



Guida per l'utente

AWS Systems Manager



AWS Systems Manager: 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

.....	xii
Cosa è AWS Systems Manager?	1
Quali sono i vantaggi di Systems Manager per l'azienda?	2
Per chi è consigliato l'utilizzo di Systems Manager?	2
Quali sono le funzionalità principali di Systems Manager?	3
Supportata Regioni AWS	3
Accesso a Systems Manager	4
Cronologia dei nomi del servizio Systems Manager	5
Sistemi operativi e tipi di macchine supportati	6
Sistemi operativi supportati per Systems Manager	6
Tipi di macchine supportati in ambienti ibridi e multicloud	12
Che cos'è la console unificata?	12
AWS Systems Manager Change Manager modifica della disponibilità	18
Valutazione di servizi alternativi	18
Configurazione dei nodi gestiti per AWS Systems Manager	19
Gestire le istanze EC2 con Systems Manager	19
Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager	20
Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager	31
Gestione dei nodi in ambienti ibridi e multicloud con Systems Manager	37
Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud	41
Crea un'attivazione ibrida per registrare i nodi con Systems Manager	49
Installa Agente SSM su nodi Linux ibridi	56
Installa Agente SSM su ibrido Windows Server nodi	62
Configurare Systems Manager per macchine virtuali Microsoft Azure	67
Configurare un Cloud Connector per Microsoft Azure in Systems Manager	71
Crea un Cloud Connector (Console di gestione AWS)	72
Prerequisiti	76
Fase 1: Creare un AWS Config connettore	84
Fase 2: Creazione di un Systems Manager Cloud Connector	85
Gestisci i connettori cloud	86
Abilita l'onboarding delle VM	87
Ruoli IAM creati dalla console di Systems Manager	90

Tag applicati alle istanze gestite	99
In che modo Systems Manager gestisce le risorse cloud	100
Gestione dei dispositivi edge con Systems Manager	101
Creazione di un ruolo di servizio IAM per dispositivi edge	102
Configura i tuoi dispositivi edge per AWS IoT Greengrass	108
Aggiorna il AWS IoT Greengrass ruolo di scambio di token e installazione Agente SSM sui tuo dispositivi periferici	108
Creare un AWS Organizations amministratore delegato per Systems Manager	109
Utilizzando un amministratore delegato con Change Manager	110
Usare un amministratore delegato con Explorer	110
Utilizzando un amministratore delegato con OpsCenter	111
Utilizzando un amministratore delegato con Configurazione rapida	111
Configurazione generale	112
Registrati per un Account AWS	112
Configurazione AWS Systems Manager	113
Configurare l'accesso alla console di Systems Manager	113
Policy di onboarding di Systems Manager	113
AWS Systems Manager politica dell'operatore della console	119
AWS Systems Manager politica di sola lettura per l'operatore della console	123
Configurazione della console unificata di Systems Manager per un'organizzazione	126
Prerequisiti	126
Risorse per console unificata	127
Configura la console unificata	129
Configurazione della console unificata di Systems Manager per singolo account e singola Regione	131
Risorse per console unificata	132
Configura la console unificata	133
Disattivazione della console unificata Systems Manager	135
Esecuzione di attività di gestione dei nodi	137
Esaminare approfondimenti nodo	137
Aggiunta o rimozione di widget	140
Riorganizzazione dei widget	141
Esplorazione dei nodi	142
Esplorazione dei nodi utilizzando i filtri della console	142
Esplorazione dei nodi utilizzando prompt di testo in Amazon Q	148
Visualizzazione dei dettagli dei singoli nodi e operazioni intraprese su un nodo	154

Effettuare il download o l'esportazione di un report sui nodi gestiti	156
Gestione del contenuto e dell'aspetto dei report dei nodi	160
Just-in-time accesso al nodo tramite Systems Manager	161
Configurazione dell'accesso just-in-time con Systems Manager	163
Avvia una sessione di accesso ai nodi just-in-time	212
Gestire le richieste di accesso just-in-time	215
Passaggio all'accesso ai nodi just-in-time da Session Manager	216
Disabilitare l'accesso just-in-time con Systems Manager	221
Domande frequenti	222
Diagnosi e correzione	224
Diagnosi e correzione delle implementazioni non riuscite	225
Diagnostica e correzione di configurazioni deviate	226
Diagnostica e correzione delle istanze Amazon EC2 non gestite	227
Tipi di impatto delle operazioni del runbook sulla correzione	240
Visualizzazione dei dettagli della cronologia di esecuzione delle correzioni	242
Regolazione delle impostazioni di Systems Manager	243
Impostazioni di configurazione dell'account	244
Impostazioni di configurazione organizzativa	244
Configurazioni delle funzionalità	244
Impostazioni di diagnosi e correzione	248
Utilizzo dei bucket Amazon S3 e delle policy dei bucket per Systems Manager	251
Utilizzo AWS Systems Manager strumenti	260
Strumenti per nodi	260
Cambia gli strumenti di gestione	262
strumenti applicativi	264
Strumenti operativi	265
Eseguire un'attività sul nodo con Systems Manager	266
Prerequisiti	266
Avvia un'istanza utilizzando un AMI con Agente SSM preinstallato	267
Connessione all'istanza gestita tramite Systems Manager	268
Pulizia dell'istanza	268
Strumenti per nodi	269
Conformità	269
Distributor	288
Fleet Manager	344
Attivazioni ibride	418

Inventory	419
Patch Manager	516
Run Command	837
Session Manager	903
State Manager	1055
Cambia gli strumenti di gestione	1157
Servizio di automazione	1157
Change Calendar	1651
Change Manager	1671
Documenti	1764
Maintenance Windows	1914
Quick Setup	2051
strumenti applicativi	264
AWS AppConfig	2105
Application Manager	2105
Parameter Store	2154
Strumenti operativi	2335
Incident Manager	2335
Explorer	2336
OpsCenter	2383
CloudWatch Dashboard	2469
Lavorare con Agente SSM	2471
Scopri i dettagli tecnici sul Agente SSM	2471
Agente SSM comportamento delle credenziali della versione 3.2.x.x	2472
Agente SSM precedenza delle credenziali	2472
Configurazione Agente SSM da utilizzare con il Federal Information Processing Standard (FIPS)	2474
Informazioni sull'account ssm-user locale	2476
Agente SSM e Servizio di metadati dell'istanza (IMDS)	2477
Mantenendo Agente SSM aggiornato	2477
Garantire che il Agente SSM la directory di installazione non venga modificata, spostata o eliminata	2478
Agente SSM aggiornamenti continui di Regioni AWS	2478
Agente SSM comunicazioni con AWS bucket S3 gestiti	2479
Agente SSM on GitHub	2488
Comprensione Agente SSM ibernazione	2488

Trova AMI con il Agente SSM preinstallato	2490
Verifica lo stato di Agente SSM	2491
Utilizzo di SSM Agent sulle istanze EC2 per Linux	2496
Verifica della firma di Agente SSM	2496
Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux	2514
Configurazione Agente SSM usare un proxy su nodi Linux	2548
Utilizzo di SSM Agent sulle istanze EC2 per macOS	2553
Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per macOS	2554
Lavorare con Agente SSM su istanze EC2 per Windows Server	2556
Installazione e disinstallazione manuali Agente SSM su istanze EC2 per Windows Server	2557
Configurazione di SSM Agent per utilizzare un proxy per le istanze Windows Server	2560
Verifica Agente SSM stato e avvio dell'agente	2564
Verifica del Agente SSM numero di versione	2566
Visualizzazione Agente SSM log	2570
Consentire Agente SSM registrazione di debug	2570
Limitare l'accesso ai comandi a livello di root tramite SSM Agent	2573
Automatizzazione degli aggiornamenti a Agente SSM	2574
Aggiornamento automatico Agente SSM	2576
Abbonarsi a Agente SSM notifiche	2577
Risoluzione dei problemi Agente SSM	2578
Agente SSM non è aggiornato	2579
Risolvi i problemi utilizzando Agente SSM file di log	2579
File watcher non riesce con troppi file aperti (Linux)	2580
I file di log dell'agente non ruotano (Windows)	2581
Impossibile connettersi agli endpoint SSM	2582
Verifica la configurazione VPC	2583
Verifica gli attributi del tuo VPC DNS-related	2584
Verifica le regole di accesso sui gruppi di sicurezza degli endpoint	2585
Usa ssm-cli per risolvere i problemi di disponibilità dei nodi gestiti	2585
Sicurezza	2586
Protezione dei dati	2587
Crittografia dei dati	2588
Riservatezza del traffico Internet	2591
Perimetri dei dati	2591
Gestione dell'identità e degli accessi	2593
Destinatari	2594

Autenticazione con identità	2594
Gestione dell'accesso tramite policy	2595
In che modo AWS Systems Manager funziona con IAM	2599
Identity-based esempi di politiche	2609
AWS politiche gestite	2621
Risoluzione dei problemi	2693
Uso di ruoli collegati ai servizi	2694
Inventario e ruolo dei dati Explorer	2696
Ruolo di individuazione account di OpsCenter e Explorer	2699
OpsData e ruolo OpsItems di creazione	2702
Ruolo di creazione di informazioni dettagliate operative	2706
Ruolo di controllo dell'integrità dell'implementazione di Quick Setup	2710
Ruolo OpsData del servizio di esportazione	2713
Just-in-time ruolo del servizio di accesso al nodo	2715
Just-in-time ruolo del servizio di notifiche di richiesta di accesso al nodo	2720
Registrazione di log e monitoraggio	2724
Convalida della conformità	2726
Resilienza	2727
Sicurezza dell'infrastruttura	2728
Analisi della configurazione e delle vulnerabilità	2728
Best practice di sicurezza	2728
Systems Manager best practice di sicurezza preventiva	2729
Agente SSM best practice di installazione	2733
Systems Manager best practice di monitoraggio e verifica	2733
Esempi di codice	2736
Nozioni di base	2740
Salve Systems Manager	2743
Informazioni di base	2747
Azioni	2799
Scenari	3146
Creazione di un servizio contenitore per istanze di macchine virtuali	3147
Guida introduttiva alle macchine virtuali	3164
Impostazione della gestione dei sistemi	3175
Registrazione di log e monitoraggio	3190
Strumenti di monitoraggio	3191
Invio dei log dei nodi a CloudWatch registri unificati (CloudWatch agente)	3191

Esegui la migrazione della raccolta di log dei nodi di Windows Server all'agente CloudWatch	3193
Memorizza le impostazioni di configurazione CloudWatch dell'agente in Parameter Store .	3204
Tornando alla raccolta dei log con Agente SSM	3205
Invio Agente SSM da log a CloudWatch Logs	3208
Monitoraggio degli eventi della richiesta di modifica	3211
Monitoraggio delle automazioni	3214
Parametri di Automazione	3215
Monitoraggio delle Run Command metriche tramite Amazon CloudWatch	3215
Parametri e dimensioni di Systems Manager Run Command	3216
Registrazione dei log AWS Systems Manager Chiamate API con AWS CloudTrail	3217
Eventi relativi ai dati di Systems Manager in CloudTrail	3219
Eventi di gestione di Systems Manager in CloudTrail	3220
Esempi di eventi Systems Manager	3221
Uscita dell'azione Logging Automation con Logs CloudWatch	3226
Configurazione di Amazon CloudWatch Logs per Run Command	3230
Specificare i CloudWatch log quando si inviano comandi	3231
Visualizzazione dell'output dei comandi nei log CloudWatch	3232
Monitoraggio con Amazon EventBridge	3233
Configurazione EventBridge per gli eventi di Systems Manager	3235
Esempi di EventBridge eventi Amazon per Systems Manager	3238
Scenari di esempio: obiettivi di Systems Manager nelle EventBridge regole di Amazon	3254
Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS	3256
Configura le notifiche Amazon SNS per AWS Systems Manager	3257
Esempi di notifiche Amazon SNS per AWS Systems Manager	3269
Utilizzo Run Command per inviare un comando che restituisce notifiche di stato	3270
Utilizzare una finestra di manutenzione per inviare un comando che restituisca notifiche di stato	3274
Integrazioni di prodotti e servizi	3280
Integrazione con Servizi AWS	3280
Calcolo	3280
Internet of Things (IoT)	3283
Archiviazione	3284
Strumenti per developer	3285
Sicurezza, identità e conformità	3286

Crittografia e PKI	3289
Gestione e governance	3290
Reti e distribuzione di contenuti	3295
Analisi	3296
Integrazione di applicazioni	3298
Console di gestione AWS	3299
Esecuzione di script da Amazon S3	3300
Referenziazione AWS Secrets Manager segreti di Parameter Store parametri	3304
AWS KMS crittografia dei Parameter Store SecureString parametri	3311
Usa AWS Secrets Manager i segreti in Amazon Elastic Kubernetes Service	3324
Utilizzo Parameter Store parametri in AWS Lambda funzioni	3344
Integrazione con altri prodotti e servizi	3369
Esecuzione di script da GitHub	3374
Utilizzo Chef InSpec profili con Systems Manager Compliance	3382
Integrazione con ServiceNow	3388
AWS Systems Manager riferimento	3389
Lavorare con gli AWS SDK	3390
Bucket Amazon S3 per operazioni di applicazione di patch	3391
Bucket contenenti documenti SSM Command per le operazioni di patching (Linux e Windows Server)	3392
Bucket contenenti documenti SSM Command per le operazioni di patching (macOS)	3395
Secchi contenenti AWS istantanee della baseline delle patch gestite	3398
EventBridge modelli e tipi di eventi per Systems Manager	3402
Tipo di evento: automazione	3403
Tipo di evento: Change Calendar	3404
Tipo di evento: Change Manager	3404
Tipo di evento: conformità di configurazione	3405
Tipo di evento: Inventario	3405
Tipo di evento: finestra di manutenzione	3406
Tipo di evento: OpsCenter	3409
Tipo di evento: Parameter Store	3409
Tipo di evento: Run Command	3410
Tipo di evento: State Manager	3411
Espressioni Cron e della frequenza	3412
Informazioni generali sulle espressioni Cron e della frequenza	3412
Espressioni Cron e della frequenza per le associazioni	3418

Espressioni Cron e della frequenza per le finestre di manutenzione	3421
ec2messages, ssmmessages e altre operazioni API	3423
Agent-related Operazioni API (endpoint ssmessages ed ec2messages)	3424
ssm: * operazioni API relative all'istanza dello spazio dei nomi	3426
ssm:* namespace per altre operazioni API	3428
Formati di stringhe di data e ora per Systems Manager	3428
Formattazione di stringhe di data e ora per Systems Manager	3429
Creazione di stringhe di data e ora personalizzate per Systems Manager	3430
Casi d'uso e best practice	3433
Eliminazione di risorse e artefatti di Systems Manager	3436
Scelta tra State Manager and Intervallo di manutenzione	3441
State Manager and Intervallo di manutenzione: Casi d'uso principali	3441
Informazioni correlate	3449
Cronologia dei documenti	3451
Aggiornamenti prima di giugno 2018	3697
Convenzioni dei documenti	3717

- La AWS Systems Manager CloudWatch dashboard non sarà più disponibile dopo il 30 aprile 2026. I clienti possono continuare a utilizzare la CloudWatch console Amazon per visualizzare, creare e gestire le proprie CloudWatch dashboard Amazon, proprio come fanno oggi. Per ulteriori informazioni, consulta la documentazione [di](#) Amazon CloudWatch Dashboard.

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.

Cosa è AWS Systems Manager?

AWS Systems Manager consente di visualizzare, gestire e utilizzare centralmente i nodi su larga scala in AWS ambienti locali e multicloud. Con il lancio di un'esperienza di console unificata, Systems Manager consolida vari strumenti per consentire all'utente di completare le attività comuni del nodo in tutti gli Account AWS e le Regioni AWS.

Per utilizzare Systems Manager, è necessario che i nodi vengano [gestiti](#), il che significa che l'SSM Agent viene installato sulla macchina per far sì che l'agente comunichi con il servizio Systems Manager. Per aiutarti a identificare il motivo per cui i nodi non vengono segnalati come gestiti, Systems Manager offre un runbook di diagnosi e risoluzione. È possibile configurare questo runbook per l'esecuzione automatica in base a una pianificazione. Questa funzionalità identifica il motivo per cui i nodi non si connettono a Systems Manager, comprese le configurazioni errate di rete. Fornisce inoltre i runbook consigliati per risolvere i problemi che impediscono la gestione dei nodi.

L'esperienza della console unificata include anche un pannello di controllo che fornisce una panoramica di alto livello dei nodi. È possibile approfondire i dettagli per ottenere informazioni più specifiche sui nodi, ad esempio su quali nodi sono in esecuzione software del sistema operativo (OS) obsoleto. Puoi anche utilizzare filtri per visualizzazioni granulari in base ai metadati delle istanze come sistemi operativi e versioni del sistema operativo,, Regioni AWS e versioni. Account AWSSSM Agent Questi filtri consentono all'utente di recuperare le informazioni pertinenti a un livello specifico di account o di applicazione nell'intera organizzazione.

Argomenti

- [Quali sono i vantaggi di Systems Manager per l'azienda?](#)
- [Per chi è consigliato l'utilizzo di Systems Manager?](#)
- [Quali sono le funzionalità principali di Systems Manager?](#)
- [Supportata Regioni AWS](#)
- [Accesso a Systems Manager](#)
- [Cronologia dei nomi del servizio Systems Manager](#)
- [Sistemi operativi e tipi di macchine supportati](#)
- [Che cos'è la console unificata?](#)

Quali sono i vantaggi di Systems Manager per l'azienda?

Alcuni vantaggi di Systems Manager sono i seguenti:

- Migliora la visibilità sull'intera infrastruttura

Systems Manager offre una visualizzazione centralizzata dei nodi negli account e nelle regioni dell'organizzazione. Accedi rapidamente alle informazioni sull'istanza come ID, nome, dettagli del sistema operativo e agenti installati. Utilizza Amazon Q Developer per interrogare i metadati delle istanze utilizzando il linguaggio naturale, identificando al meglio i problemi e agendo più rapidamente.

- Aumenta l'efficienza operativa con l'automazione

Automatizza le attività operative più comuni e riduci il tempo e l'impegno necessari per la manutenzione dei sistemi. Systems Manager offre una gestione remota sicura e protetta dei nodi su larga scala senza accedere ai server. Non è più necessario utilizzare bastion hosts, SSH o remote. PowerShell Systems Manager offre anche un metodo semplice per automatizzare attività di amministrazione comuni su gruppi di nodi, ad esempio modifiche del registro, gestione di utenti e installazione di software e patch.

- Semplifica la gestione dei nodi su larga scala in qualsiasi ambiente

Systems Manager ti aiuta a gestire i nodi in ambienti AWS locali e multicloud. Pianifica diagnosi automatiche per identificare i SSM Agent problemi e risolverli con i runbook. Dopo aver configurato i nodi come nodi gestiti, è possibile eseguire attività operative critiche come l'applicazione di patch di sicurezza, l'avvio di sessioni registrate e l'esecuzione di comandi in remoto.

Per chi è consigliato l'utilizzo di Systems Manager?

Systems Manager è utilizzato da responsabili e operatori delle operazioni IT, DevOps ingegneri, responsabili della sicurezza e della conformità, direttori IT e CIO. In generale, Systems Manager è adatto per:

- Organizzazioni che desiderano migliorare la gestione e la sicurezza dei propri nodi su larga scala.
- Organizzazioni che desiderano aumentare la visibilità e l'agilità operativa nella gestione della propria infrastruttura.
- Organizzazioni che desiderano aumentare l'efficienza operativa su larga scala.

Quali sono le funzionalità principali di Systems Manager?

Le funzionalità principali di Systems Manager sono condivise tra la console unificata e i singoli strumenti di Systems Manager per aiutarti a gestire i nodi su larga scala.

Console unificata

La console unificata offre un'esperienza centralizzata per visualizzare e gestire i nodi. Questa console utilizza diversi strumenti di Systems Manager e altro ancora per fornire quanto segue:

- Visualizzazioni centralizzate dei nodi
- Approfondimenti dettagliati sul nodo
- Diagnosi e risoluzione automatizzate dei problemi più comuni dei nodi

Per ulteriori informazioni sulla console unificata, consulta [Che cos'è la console unificata?](#).

Strumenti

Gli strumenti sono costituiti dalle capacità individuali di Systems Manager e dalle relative funzionalità come Run Command, Session Manager, Automazione e Parameter Store. Con gli strumenti di Systems Manager, puoi effettuare le seguenti operazioni:

- Just-in-time accesso al nodo di accesso
- Applicazione di patch ai nodi su larga scala
- Connettiti in modo sicuro ai nodi senza aprire le porte in entrata
- Esegui comandi in remoto sui nodi
- Archivia in modo sicuro i dati a cui fanno riferimento le applicazioni
- Automatizza le attività di amministrazione dei sistemi comuni

Per ulteriori informazioni sugli strumenti di Systems Manager, consulta [Utilizzo AWS Systems Manager strumenti](#).

Supportata Regioni AWS

Per un elenco degli strumenti Regioni AWS di supporto di [Systems Manager](#), vedere gli endpoint del servizio [Systems Manager](#) nella Riferimenti generali di Amazon Web Services.

La console unificata di Systems Manager, rilasciata il 21 novembre 2024, è disponibile nei seguenti formati: Regioni AWS

- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti orientali (Ohio)
- Regione Stati Uniti occidentali (California settentrionale)
- Stati Uniti occidentali (Oregon)
- Regione Canada (Centrale)
- Regione Sud America (San Paolo)
- Regione Asia Pacifico (Mumbai)
- Regione Asia Pacifico (Tokyo)
- Regione Asia Pacifico (Seoul)
- Regione Asia Pacifico (Singapore)
- Regione Asia Pacifico (Sydney)
- Regione Europa (Francoforte)
- Regione Europa (Stoccolma)
- Regione Europa (Irlanda)
- Regione Europa (Londra)
- Regione Europa (Parigi)

Accesso a Systems Manager

Puoi usare il servizio Systems Manager in uno dei modi seguenti:

Console di Systems Manager

La [console di Systems Manager](#) è un'interfaccia basata su browser che consente l'accesso e l'utilizzo di Systems Manager.

AWS IoT Greengrass V2 console

È possibile visualizzare e gestire i dispositivi edge configurati AWS IoT Greengrass nella console <https://console.aws.amazon.com/iot> Greengrass.

AWS strumenti da riga di comando

Utilizzando gli strumenti da riga di AWS comando, è possibile inviare comandi nella riga di comando del sistema per eseguire Systems Manager e altre AWS attività. Gli strumenti sono supportati su Linux, macOS e Windows. L'uso della AWS Command Line Interface (AWS CLI) può risultare più veloce e comodo rispetto a quello della console. Gli strumenti a riga di comando sono inoltre utili per creare script che eseguono le attività di AWS .

AWS fornisce due set di strumenti da riga di comando: the [AWS Command Line Interface](#) e the [AWS Tools for Windows PowerShell](#). Per informazioni sull'installazione e l'utilizzo di AWS CLI, consultare la Guida [AWS Command Line Interface per l'utente](#). Per informazioni sull'installazione e l'uso degli Strumenti per Windows PowerShell, consulta la Guida per [AWS Strumenti per PowerShell l'utente](#).

Note

Sulle istanze Windows Server, è necessario disporre di Windows PowerShell 3.0 o versioni successive per eseguire determinati documenti SSM (ad esempio il documento legacy AWS-ApplyPatchBaseline). Verificare che le istanze Windows Server eseguano Windows Management Framework 3.0 o versioni successive. Il framework include Windows PowerShell.

AWS SDK

AWS fornisce kit di sviluppo software (SDK) costituiti da librerie e codice di esempio per vari linguaggi e piattaforme di programmazione. I linguaggi supportati includono [Java](#), [Python](#), [Ruby](#), [.NET](#), [iOS e Android](#) e altri. <https://aws.amazon.com/tools/#sdk> Gli SDK rappresentano un sistema comodo per concedere l'accesso programmatico a Systems Manager. Per informazioni su come scaricarli e installarli, consulta [Strumenti per Amazon Web Services](#).

Cronologia dei nomi del servizio Systems Manager

AWS Systems Manager (Systems Manager) era precedentemente noto come "" e Amazon Simple Systems Manager (SSM) "». Amazon EC2 Systems Manager (SSM) Il nome abbreviato originale del servizio, "SSM«, è ancora riportato in varie AWS risorse, tra cui alcune altre console di servizio. Alcuni esempi:

- Systems Manager Agent: SSM Agent
- Parametri di Systems Manager: parametri SSM
- Endpoint del servizio Systems Manager: `ssm.region.amazonaws.com`
- AWS CloudFormation tipi di risorse: `AWS::SSM::Document`
- AWS Config identificatore della regola: `EC2_INSTANCE_MANAGED_BY_SSM`
- AWS Command Line Interface (AWS CLI) comandi: `aws ssm describe-patch-baselines`
- AWS Identity and Access Management Nomi delle policy gestite (IAM):
`AmazonSSMReadOnlyAccess`
- ARN delle risorse di Systems Manager: `arn:aws:ssm:region:account-id:patchbaseline/pb-07d8884178EXAMPLE`

Sistemi operativi e tipi di macchine supportati

Prima di utilizzare Systems Manager, verifica che il sistema operativo (OS), la versione del sistema operativo e il tipo di macchina siano supportati come nodi gestiti.

Argomenti

- [Sistemi operativi supportati per Systems Manager](#)
- [Tipi di macchine supportati in ambienti ibridi e multicloud](#)

Sistemi operativi supportati per Systems Manager

AWS Systems Manager fornisce supporto per un set definito di versioni del sistema operativo (OS) che sono supportate attivamente dal fornitore del sistema operativo e sono elencate come supportate nella AWS Systems Manager documentazione. AWS Systems Manager Il supporto del sistema operativo è in linea con i cicli di vita dei fornitori, come definito nei termini di servizio del software. Non tutti i sistemi operativi o le versioni del sistema operativo supportati da un fornitore sono supportati da AWS Systems Manager.

AWS Systems Manager il supporto per una versione del sistema operativo termina quando il fornitore del sistema operativo dichiara la fine del ciclo di vita (EOL) di tale versione. Il supporto non si estende all'Extended Long-Term Support (ELTS) a pagamento del fornitore o a programmi simili a pagamento. Sebbene i clienti possano continuare a utilizzare e installare versioni del sistema operativo che hanno superato il termine di scadenza del fornitore, il AWS supporto fornirà assistenza solo se un problema è riproducibile su una versione del sistema operativo supportata.

Le nuove versioni di AWS Systems Manager prodotto, incluse le nuove versioni principali diSSM Agent, non aggiungono il supporto per le versioni del sistema operativo il cui rilascio è previsto entro sei mesi dalla data di rilascio.

Nelle sezioni seguenti sono elencati i sistemi operativi e le versioni dei sistemi operativi supportati da Systems Manager.

Note

Se si prevede di gestire e configurare i dispositivi AWS IoT Greengrass principali utilizzando Systems Manager, tali dispositivi devono soddisfare i requisiti per [AWS IoT Greengrass Per](#) ulteriori informazioni, consulta [Configurazione dei dispositivi AWS IoT Greengrass principali](#) nella Guida per gli AWS IoT Greengrass Version 2 sviluppatori.

Se si prevede di gestire AWS IoT e configurare dispositivi non AWS periferici, tali dispositivi devono soddisfare i requisiti elencati qui ed essere configurati come nodi gestiti in locale per Systems Manager. Per ulteriori informazioni, consulta [Gestione dei dispositivi edge con Systems Manager](#).

Important

Ti consigliamo vivamente di evitare di utilizzare versioni del sistema operativo che hanno raggiunto End-of-Life (EOL). I fornitori di sistemi operativi, tra cui AWS in genere, non forniscono patch di sicurezza o altri aggiornamenti per le versioni che hanno raggiunto il termine di scadenza. Continuare a utilizzare un sistema EOL aumenta notevolmente il rischio di non poter applicare gli aggiornamenti, comprese le correzioni di sicurezza, e altri problemi operativi. AWS non verifica la funzionalità di Systems Manager sulle versioni del sistema operativo che hanno raggiunto il termine di scadenza.

Patch Manager potrebbe non supportare tutte le versioni del sistema operativo elencate in questo argomento. Per l'elenco completo delle versioni supportate da Patch Manager, consulta [Patch Manager prerequisiti](#).

Tipi di sistema operativo

- [Linux](#)
- [macOS \(solo istanze Amazon EC2\)](#)
- [Windows Server](#)

Seleziona una piattaforma di sistema operativo per visualizzare le versioni principali e secondarie supportate.

Linux

AlmaLinux

Versioni	x86	x86_64	ARM64
8.3–8.10		✓	✓
9.x		✓	✓

Amazon Linux 2

Versioni	x86	x86_64	ARM64
2.0 e tutte le versioni successive		✓	✓

Amazon Linux 2023

Versioni	x86	x86_64	ARM64
2023,0.20230315.0 e tutte le versioni successive		✓	✓

Bottlerocket

Versioni	x86_64	ARM64
1.0.0 e tutte le versioni successive	✓	✓

CentOS Stream

Versioni	x86	x86_64	ARM64
9		✓	✓

Debian Server

Versioni	x86	x86_64	ARM64
Bullseye (11)		✓	✓
Bookworm(12)		✓	✓

Oracle Linux

Versioni	x86	x86_64	ARM64
7.5 - 7.8		✓	
8.x		✓	
9.x		✓	

Red Hat Enterprise Linux (RHEL)

Versioni	x86	x86_64	ARM64
7.0 - 7.5		✓	
7.6–8.x		✓	✓
9.x		✓	✓
10.x		✓	✓

Rocky Linux

Versioni	x86	x86_64	ARM64
8.x		✓	✓
9.x		✓	✓
10.x		✓	✓

SUSE Linux Enterprise Server (SLES)

Versioni	x86	x86_64	ARM64
Versioni 15.3 e successive		✓	✓

Ubuntu Server

Versioni	x86	x86_64	ARM64
18.04 LITRI		✓	✓
20.04 LTS		✓	✓
22.04 LTS		✓	✓
24.04 LTS		✓	✓
25.04		✓	✓

macOS (solo istanze Amazon EC2)

Versione	x86	x86_64	Mac with Apple silicon
13.x (Ventura)		✓	✓
14.x (Sonoma)		✓	✓

Versione	x86	x86_64	Mac with Apple silicon
15.x (Sequoia)		✓	✓

Note

macOS non è supportato in tutto. Regioni AWS Per ulteriori informazioni sul supporto di Amazon EC2 per macOS, consulta [Istanze Amazon EC2 Mac](#) nella Guida per l'utente di Amazon EC2.

Windows Server

SSM Agent richiede Windows PowerShell 3.0 o successivamente l'esecuzione di determinati AWS Systems Manager documenti (documenti SSM) su Windows Server istanze (ad esempio, il AWS-ApplyPatchBaseline documento precedente). Verificare che le istanze Windows Server eseguano Windows Management Framework 3.0 o versioni successive. Questo framework include Windows PowerShell. Per ulteriori informazioni, consulta [Windows Management Framework 3.0](#).

Versione	x86	x86_64	ARM64
2012 e 2012 R2 ²		✓	
2016		✓	
2019		✓	
2022		✓	
2025		✓	

¹ Supporto di Windows Server 2012 e 2012 R2: Windows Server 2012 e 2012 R2 non sono più supportate a partire dal 10 ottobre 2023. Per l'utilizzo di SSM Agent con queste versioni, si consiglia di utilizzare Extended Security Updates (ESU) di Microsoft. Per ulteriori informazioni, consulta [Raggiungimento della fine del supporto di Windows Server 2012 e 2012 R2](#) sul sito Web di Microsoft.

Tipi di macchine supportati in ambienti ibridi e multicloud

Systems Manager supporta diversi tipi di computer come nodi gestiti. Un nodo gestito è un computer configurato per l'uso con Systems Manager.

Questa guida per l'utente utilizza il termine ibrido e multicloud per fare riferimento a un ambiente che contiene qualsiasi combinazione dei seguenti tipi di computer:

- Istanze Amazon Elastic Compute Cloud (Amazon EC2)
- Server presso la propria sede (server on-premises)
- AWS IoT Greengrass dispositivi principali
- AWS IoT e dispositivi non AWS periferici
- Macchine virtuali (VM), incluse le macchine virtuali in altri ambienti cloud

Per informazioni sul AWS supporto per ambienti ibridi e multicloud, vedi [AWS Soluzioni per ambienti ibridi e multicloud](#).

Che cos'è la console unificata?

La console unificata di Systems Manager è un'esperienza consolidata che combina vari strumenti per aiutarti a completare le attività dei nodi comuni in più Account AWS e Regioni AWS in un' AWS Organizations organizzazione o in un singolo account e regione. I nodi possono essere istanze EC2, server ibridi o server in esecuzione in un ambiente multicloud. Nella console unificata, ti vengono fornite informazioni utili sui tuoi nodi. Puoi generare report per i tuoi nodi, diagnosticare e risolvere problemi comuni che impediscono ai nodi di segnalare come gestito da Systems Manager, come i problemi di connettività.

Review insights about managed nodes across your organization. Hover over a graphic to access links to more detailed data.

Review insights about managed nodes across your organization. Hover over a graphic to access links to more detailed data.

+ Add widgets

+ Add widgets

Oltre ai riepiloghi sui nodi nella [pagina](#) Rivedi le informazioni sui nodi, puoi visualizzare dettagli specifici su un nodo dalla [pagina](#) Esplora i nodi.

Explore nodes (56)

Explore details about managed nodes in your organization.

Group by

None ▾

Nodes (56) Advanced instances

Find nodes

< 1 ... >

Node ID	Agent type	Agent version	Node status	Operating system name	Operating system type	Operating system version	Node type	Ac
i-00133d4e1c15e843b	amazon-ssm-agent	3.3.1230.0	Active	Ubuntu	Linux	20.04	EC2Instance	
i-00ba99a313b84a821	amazon-ssm-agent	3.3.1230.0	Active	Microsoft Windows Server 2022 Datacenter	Windows	10.0.20348	EC2Instance	
i-010e038ef4f248dbd	amazon-ssm-agent	3.3.1230.0	Active	Amazon Linux	Linux	2	EC2Instance	
i-013d9f572f5e5b6b3	amazon-ssm-agent	3.3.1230.0	Active	Microsoft Windows Server 2016 Datacenter	Windows	10.0.14393	EC2Instance	
i-018515ec864b6b34d	amazon-ssm-agent	3.3.987.0	Active	Ubuntu	Linux	24.04	EC2Instance	
i-0207b54c36e64ffac	amazon-ssm-agent	3.3.1230.0	Active	Amazon Linux	Linux	2	EC2Instance	
i-02384ada61f4a07a8	amazon-ssm-agent	3.3.1230.0	Active	Microsoft Windows Server 2019 Datacenter	Windows	10.0.17763	EC2Instance	

Schede sui dettagli del nodo

Quando selezioni un nodo nella pagina Esplora i nodi, la pagina di dettaglio del nodo fornisce una panoramica completa dei dettagli del nodo e informazioni aggiuntive su una serie di schede:



MyWindowsServer2022Instance Running

Node overview

Name MyWindowsServer2022Instance	Agent version 3.3.2746.0	IP address [REDACTED]	Instance role arn:aws:iam::[REDACTED]:instance-profile/[REDACTED]instanceProfile
Node Account [REDACTED]	Platform type Windows	Image ID ami-0eeaeaf436aca1a02	Key name [REDACTED]
Node Region us-east-2	Operating system Microsoft Windows Server 2022 Datacenter	Node state ✔ Running	Patch critical noncompliant count 0
Source type EC2 instance	Platform version 10.0.20348	Ping status ✔ Online	Patch failed count 0
Node ID i-0d55098-[REDACTED]	Architecture x86_64	Association status ✔ Success	Patch installed count 3
Activation ID -	Computer name [REDACTED]	IAM role -	Patch group -

Tags | Inventory | Associations | **Patches** | Configuration compliance

Patch summary

Patch baseline ID Updates installed

Tag

(Facoltativo) Gestisci i tag delle risorse per raggruppare e filtrare il nodo gestito con altre risorse. I tag consistono in una coppia chiave-valore che fa distinzione tra maiuscole e minuscole e vengono utilizzati per categorizzare le risorse in modi diversi, ad esempio, per scopo, proprietario o ambiente.

Inventory

Visualizza i metadati relativi al nodo gestito, che è possibile visualizzare in base a oltre 10 diversi tipi di inventario. Ad esempio, quando selezioni il tipo `AWS:Application`, i risultati del filtro di inventario forniscono dettagli sulle applicazioni installate sul nodo, come Nome, Versione, Architettura e altro. Per ulteriori informazioni sull'inventario, consulta [the section called "Inventory"](#).

Associazioni

Un'associazione è un tipo di risorsa State Manager che definisce lo stato di destinazione per un nodo gestito e mantiene tutti i nodi gestiti dell'account in uno stato coerente. L'associazione può definire i comandi, gli script o le policy da applicare a quali istanze gestite e con quale frequenza deve essere eseguita per assicurarsi che i nodi corrispondano alla configurazione definita per il

nodo. Un'associazione può favorire la creazione di report sulla conformità degli stati necessari per le risorse nell'account. Per ulteriori informazioni su State Manager e sulle associazioni, consulta [the section called “State Manager”](#).

Patch

Visualizza i metadati relativi al nodo gestito, ad esempio la baseline delle patch assegnata al nodo e il numero totale di aggiornamenti per i pacchetti che sono stati aggiornati correttamente, che hanno avuto esito negativo o che sono ancora necessari per l'installazione. La scheda Patch riporta anche i dettagli sulle patch disponibili per il nodo in base ai requisiti di configurazione nella baseline delle patch, incluso il nome del pacchetto, ad esempio `libblockdev-crypto.x86_64`; Classificazione (come Bugfix o Security); Descrizione (che mostra il titolo completo della patch, ad esempio `coreutils.x86_64:0:8.32-36.el9` e `java-11-amazon-corretto-headless-1:11.0.15+9-1.amzn2.x86_64`; e Stato della patch, ad esempio Installed, Installed_Pending_Reboot, Missing e Failed.

Note

Gli stati delle patch non indicano se un nodo gestito è conforme. La conformità delle patch non è intrinsecamente legata agli stati delle patch, né è definita dai AWS fornitori di sistemi operativi (OS) o da terze parti, come le società di consulenza sulla sicurezza. Al contrario, Il significato della conformità delle patch per i nodi gestiti dell'organizzazione o dell'account viene definito in una baseline delle patch. Per ulteriori informazioni, consulta [the section called “In cosa consiste la conformità Patch Manager?”](#) e [the section called “Baseline delle patch predefinite e personalizzate”](#).

Conformità di configurazione

Segnala la conformità delle patch e le incongruenze di configurazione sul nodo (indipendentemente dal fatto che lo stato di un pacchetto sul nodo gestito sia Compliant o in Non-compliant base alla definizione di Conforme come definita in un'associazione State Manager o in una baseline delle patch Patch Manager). È possibile filtrare i risultati di conformità della configurazione in base all'ID del pacchetto, allo stato di conformità, al tipo di conformità (Association o Patch), Severity e a diversi dettagli di esecuzione. Per le relative informazioni, consulta [the section called “Conformità”](#).

Sia che tu abbia nodi in più account e Regioni in un'organizzazione o nodi in un unico account e in un'unica Regione, ti consigliamo di utilizzare la console unificata. Per ulteriori informazioni sulle attività dei nodi che puoi eseguire ora utilizzando la console unificata, consulta [Esecuzione di attività di gestione dei nodi con AWS Systems Manager](#)

Per ulteriori informazioni sulla configurazione dei nodi per Systems Manager, consulta [Configurazione dei nodi gestiti per AWS Systems Manager](#). Dopo aver configurato i nodi, puoi configurare Systems Manager e la console unificata. Per ulteriori informazioni sulla configurazione di Systems Manager, consulta [Configurazione AWS Systems Manager](#).

Consulta anche [Sistemi operativi e tipi di macchine supportati](#).

AWS Systems Manager Change Manager modifica della disponibilità

Dopo un'attenta valutazione, abbiamo deciso di chiudere AWS Systems Manager Change Manager i battenti con nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente.

Valutazione di servizi alternativi

Per i clienti che necessitano di una soluzione di gestione delle modifiche di livello aziendale, consigliamo le soluzioni AWS Partner Network.

La [Management and Governance Cloud Environment Guide](#) consiglia di considerare le seguenti domande nella scelta di una AWS soluzione per i partner:

- Fornisce l'abilitazione dei processi ITSM?
- Consente agli utenti di mettere in relazione i processi ITSM (ovvero, collegare gli incidenti alle richieste di modifica)?
- Abilita i flussi di lavoro e le approvazioni aziendali?
- Consente la configurazione, la personalizzazione e l'integrazione con altri sistemi e piattaforme?
- Consente la possibilità di creare report e dashboard?
- Abilita il self-service per le richieste aziendali e di servizio?

Valuta attentamente i tuoi casi d'uso e i tuoi requisiti. Quindi esamina le funzionalità offerte dalle soluzioni AWS Partner Network per selezionare la migliore soluzione di gestione dei servizi per le tue esigenze.

Se hai altre domande, contattaci tramite il Centro [AWS assistenza](#) o leggi le nostre domande frequenti.

Configurazione dei nodi gestiti per AWS Systems Manager

Completa le attività in questa sezione per impostare e configurare ruoli, account utente, autorizzazioni e risorse iniziali per l'utilizzo AWS Systems Manager degli strumenti. Le attività descritte in questa sezione vengono in genere eseguite dagli amministratori Account AWS di sistema. Dopo aver completato questi passaggi, gli utenti dell'organizzazione possono utilizzare Systems Manager per configurare, gestire e accedere a nodi gestiti. Un nodo gestito è qualsiasi macchina configurata per l'uso con Systems Manager in un ambiente [ibrido e multicloud](#).

Note

Se prevedi di utilizzare sia le istanze Amazon EC2 che le risorse di calcolo in un ambiente [ibrido e multicloud](#), segui le fasi descritte in [Gestire le istanze EC2 con Systems Manager](#). Questo argomento presenta i passaggi nell'ordine più consono per completare la configurazione di Systems Manager per istanze EC2 e macchine non EC2.

Se ne utilizzi già altri Servizi AWS, hai completato alcuni di questi passaggi. Tuttavia, altri passaggi sono specifici per Systems Manager. Pertanto, ti consigliamo di consultare l'intera sezione per assicurarti di essere pronto a utilizzare tutti gli strumenti di Systems Manager.

Argomenti

- [Gestire le istanze EC2 con Systems Manager](#)
- [Gestione dei nodi in ambienti ibridi e multicloud con Systems Manager](#)
- [Configurare un Cloud Connector per Microsoft Azure in Systems Manager](#)
- [Gestione dei dispositivi edge con Systems Manager](#)
- [Creare un AWS Organizations amministratore delegato per Systems Manager](#)
- [Configurazione generale per AWS Systems Manager](#)

Gestire le istanze EC2 con Systems Manager

Completa le attività in questa sezione per impostare e configurare ruoli, autorizzazioni e risorse iniziali per AWS Systems Manager. Le attività descritte in questa sezione sono tipicamente eseguite da Account AWS e amministratori di sistema. Dopo aver completato queste fasi, gli utenti

dell'organizzazione possono utilizzare Systems Manager per configurare e gestire e accedere alle istanze di Amazon Elastic Compute Cloud (Amazon EC2).

Note

Se prevedi di utilizzare Systems Manager per gestire e configurare le macchine on-premises, segui le operazioni di configurazione descritte in [Gestione dei nodi in ambienti ibridi e multicloud con Systems Manager](#). Se prevedi di utilizzare sia le istanze Amazon EC2 che le macchine non EC2 in un ambiente [ibrido e multicloud](#), segui prima le fasi descritte in questa pagina. Questa sezione presenta, nell'ordine migliore, i passaggi per configurare i ruoli, gli utenti, le autorizzazioni e le risorse iniziali da usare nelle operazioni con Systems Manager.

Se ne usi già altri Servizi AWS, hai completato alcuni di questi passaggi. Tuttavia, altri passaggi sono specifici per Systems Manager. Pertanto, ti consigliamo di consultare l'intera sezione per assicurarti di essere pronto a utilizzare tutti gli strumenti di Systems Manager.

Indice

- [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#)
- [Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager](#)

Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager

Per impostazione predefinita, AWS Systems Manager non dispone dell'autorizzazione per eseguire azioni sulle tue istanze. Puoi fornire le autorizzazioni alle istanze a livello di account utilizzando un ruolo AWS Identity and Access Management (IAM) o a livello di istanza utilizzando un profilo di istanza. Se il caso d'uso lo consente, ti consigliamo di concedere l'accesso a livello di account utilizzando la configurazione di gestione host predefinita.

Note

È possibile saltare questo passaggio e consentire a Systems Manager di applicare le autorizzazioni richieste alle istanze durante la configurazione della console unificata. Per ulteriori informazioni, consulta [Configurazione AWS Systems Manager](#).

Configurazione consigliata per le autorizzazioni delle istanze EC2

La configurazione di gestione host predefinita consente a Systems Manager di gestire automaticamente le istanze Amazon EC2. Dopo aver attivato questa impostazione, tutte le istanze che utilizzano Instance Metadata Service versione 2 (IMDSv2) nella Regione AWS e Account AWS con la SSM Agent versione 3.2.582.0 o successiva installata diventano automaticamente istanze gestite. La configurazione di gestione host predefinita non supporta Instance Metadata Service versione 1. Per ulteriori informazioni sul passaggio a IMDSv2, consulta la pagina [Passaggio all'utilizzo del servizio di metadati dell'istanza versione 2](#) nella Guida per l'utente di Amazon EC2. Per informazioni sulla verifica della versione SSM Agent installata sull'istanza, consulta la pagina [Verifica del Agente SSM numero di versione](#). Per informazioni sull'aggiornamento dell'SSM Agent, consulta la pagina [Aggiornamento automatico Agente SSM](#). I vantaggi delle istanze gestite includono la possibilità di:

- Connettersi in modo sicuro alle istanze Linux utilizzando Session Manager.
- Eseguire scansioni automatiche delle patch utilizzando Patch Manager.
- Visualizzare informazioni dettagliate sulle istanze utilizzando Inventario di Systems Manager Inventory.
- Tenere traccia delle istanze e gestirle utilizzando Fleet Manager.
- Mantenere l'SSM Agent aggiornato automaticamente.

Fleet Manager, AWS Systems Manager Inventory e sono strumenti in. Patch Manager Session Manager

La configurazione di gestione host predefinita consente la gestione delle istanze senza l'utilizzo di profili di istanza e garantisce che Systems Manager disponga delle autorizzazioni per gestire tutte le istanze nella Regione e nell'account. Se le autorizzazioni fornite non sono sufficienti per il tuo caso d'uso, è possibile anche aggiungere policy al ruolo IAM predefinito creato dalla configurazione di gestione host predefinita. In alternativa, se non hai bisogno di autorizzazioni per tutte le funzionalità fornite dal ruolo IAM predefinito, è possibile creare ruoli e policy personalizzati. Qualsiasi modifica apportata al ruolo IAM scelto per la configurazione di gestione host predefinita si applica a tutte le istanze Amazon EC2 gestite nella Regione e nell'account. Per ulteriori informazioni sulla policy utilizzata dalla configurazione di gestione host predefinita, consulta la pagina [AWS politica gestita: AmazonSSMManagedEC2InstanceDefaultPolicy](#). Per ulteriori informazioni sulla configurazione di gestione host predefinita, consulta [Gestione automatica delle istanze EC2 con la configurazione di gestione host predefinita](#).

⚠ Important

Le istanze registrate utilizzando la configurazione di gestione host predefinita archiviano le informazioni di registrazione localmente nelle directory `/lib/amazon/ssm` o `C:\ProgramData\Amazon`. La rimozione di tali directory o dei relativi file impedirà all'istanza di acquisire le credenziali necessarie per connettersi a Systems Manager utilizzando la configurazione di gestione host predefinita. In questi casi, è necessario utilizzare un profilo dell'istanza per fornire le autorizzazioni richieste all'istanza o ricreare l'istanza.

ℹ Note

Questa procedura deve essere eseguita solo dagli amministratori. Implementa l'accesso con privilegi minimi quando consenti alle persone di configurare o modificare la configurazione di gestione host predefinita. È necessario attivare la configurazione predefinita di gestione degli host in ciascuna istanza in Regione AWS cui si desidera gestire automaticamente le istanze Amazon EC2.

Attivazione dell'impostazione di configurazione di gestione host predefinita

È possibile attivare la configurazione di gestione host predefinita dalla console Fleet Manager. Per completare correttamente questa procedura utilizzando lo Console di gestione AWS strumento a riga di comando preferito, devi disporre delle autorizzazioni per le operazioni [GetServiceSetting](#), [ResetServiceSetting](#), e [UpdateServiceSetting](#) API. Inoltre, è necessario disporre delle autorizzazioni per l'autorizzazione `iam:PassRole` per il ruolo IAM `AWSSystemsManagerDefaultEC2InstanceManagementRole`. Di seguito è riportata una policy di esempio. Sostituisci ogni *example resource placeholder* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetServiceSetting",
```

```

        "ssm:ResetServiceSetting",
        "ssm:UpdateServiceSetting"
    ],
    "Resource": "arn:aws:ssm:us-east-1:111122223333:servicesetting/ssm/managed-instance/default-ec2-instance-management-role"
},
{
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": "arn:aws:iam::111122223333:role/service-role/AWSSystemsManagerDefaultEC2InstanceManagementRole",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": [
                "ssm.amazonaws.com"
            ]
        }
    }
}
]
}

```

Prima di iniziare, se disponi di profili dell'istanza collegati alle istanze Amazon EC2, rimuovi tutte le autorizzazioni che consentono l'operazione `ssm:UpdateInstanceInformation`. L'SSM Agent tenta di utilizzare le autorizzazioni del profilo dell'istanza prima di utilizzare le autorizzazioni di configurazione di gestione host predefinita. Se consenti l'operazione `ssm:UpdateInstanceInformation` nei profili dell'istanza, l'istanza non utilizzerà le autorizzazioni di configurazione di gestione host predefinita.

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli Configura la gestione host predefinita nel menu a discesa Gestione dell'account.
4. Attiva Abilita la configurazione di gestione host predefinita.
5. Scegli il ruolo IAM utilizzato per abilitare gli strumenti di Systems Manager per le tue istanze. Ti consigliamo di utilizzare il ruolo predefinito fornito dalla configurazione di gestione host predefinita. Contiene il set minimo di autorizzazioni necessario per gestire le istanze Amazon

EC2 utilizzando Systems Manager. Se preferisci utilizzare un ruolo personalizzato, la policy di attendibilità del ruolo deve riconoscere Systems Manager come un'entità attendibile.

6. Scegli Configura per completare la configurazione.

Dopo aver attivato la configurazione di gestione host predefinita, le istanze potrebbero impiegare fino a 30 minuti per utilizzare le credenziali del ruolo scelto. È necessario attivare la configurazione di gestione host predefinita in ogni Regione nella quale desideri gestire in automatico le istanze Amazon EC2.

Configurazione alternativa per le autorizzazioni delle istanze EC2

È possibile concedere l'accesso a livello di singola istanza utilizzando un profilo dell'istanza AWS Identity and Access Management (IAM). Un profilo dell'istanza è un container che trasmette le informazioni sul ruolo IAM a un'istanza di Amazon Elastic Compute Cloud (Amazon EC2) all'avvio. È possibile creare un profilo dell'istanza per Systems Manager collegando una o più policy IAM che definiscano le autorizzazioni necessarie per un ruolo nuovo o già creato.

Note

Puoi utilizzarlo Quick Setup per configurare rapidamente un profilo di istanza su tutte le istanze del tuo Account AWS. Quick Setup crea anche un ruolo di servizio IAM (o assume il ruolo), che consente a Systems Manager di eseguire in modo sicuro i comandi sulle tue istanze per tuo conto. Utilizzando Quick Setup, è possibile ignorare questa fase (fase 3) e la fase 4. Per ulteriori informazioni, consulta [AWS Systems Manager Configurazione rapida](#).

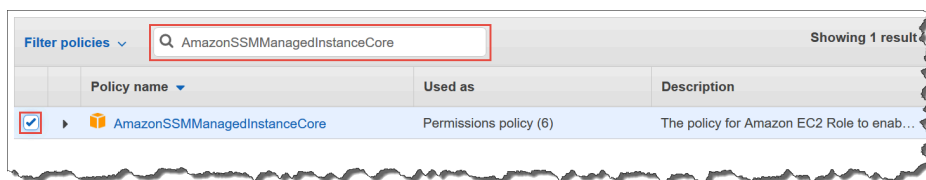
Osserva i seguenti dettagli relativi alla creazione di un profilo dell'istanza IAM:

- Se configuri macchine non EC2 in un ambiente [ibrido e multicloud](#) per Systems Manager, non devi creare il relativo profilo dell'istanza. Dovrai invece configurare i server e le macchine virtuali per l'uso di un ruolo di servizio IAM. Per ulteriori informazioni, consulta [Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud](#).
- Se modifichi il profilo dell'istanza IAM, l'aggiornamento delle credenziali dell'istanza potrebbe richiedere del tempo. Fino a quel momento, l'SSM Agent non elaborerà le richieste. Per velocizzare il processo di aggiornamento, è possibile riavviare l'SSM Agent o l'istanza.

Utilizza una delle procedure seguenti in base all'operazione da eseguire, ovvero la creazione di un nuovo ruolo per il profilo dell'istanza o l'aggiunta delle autorizzazioni necessarie a un ruolo esistente.

Creare un profilo dell'istanza per le istanze gestite (console) di Systems Manager

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, scegli Ruoli e quindi Crea ruolo.
3. Per Trusted entity type (Tipo di entità attendibile), scegli Servizio AWS.
4. In Caso d'uso, scegli EC2, quindi scegli Successivo.
5. Nella pagina Aggiungi autorizzazioni, esegui le operazioni seguenti:
 - Utilizza il campo di ricerca per individuare la `AmazonSSMManagedInstanceCore` policy. Seleziona la casella di controllo accanto al relativo nome, come illustrato nella figura seguente.



La console mantiene la selezione anche se cerchi altre policy.

- Se nella procedura precedente è stata creata una policy del bucket S3 personalizzata, [\(Facoltativo\) Creazione di una policy personalizzata per l'accesso al bucket S3](#), cercarla e selezionare la casella accanto al relativo nome file.
 - Se intendi unire le istanze a un Active Directory gestito da Directory Service, cerca `AmazonSSMDirectoryServiceAccess` e seleziona la casella di controllo accanto al nome corrispondente.
 - Se intendi utilizzare EventBridge o CloudWatch Logs per gestire o monitorare la tua istanza, cerca `CloudWatchAgentServerPolicy` e seleziona la casella di controllo accanto al nome.
6. Scegli Avanti.
 7. Per Nome ruolo, inserisci un nome per il nuovo profilo dell'istanza, ad esempio **SSMInstanceProfile**.

Note

Prendi nota del nome del ruolo. Scegli questo ruolo quando crei nuove istanze che desideri gestire utilizzando Systems Manager.

8. (Facoltativo) Per Description (Descrizione), aggiorna la descrizione di questo profilo dell'istanza.
9. (Facoltativo) Per Tags (Tag), aggiungi una o più coppie tag chiave-valore chiave per organizzare, monitorare o controllare l'accesso per questo ruolo, quindi scegli Create role (Crea ruolo). Il sistema ti riporta alla pagina Ruoli.

Aggiunta delle autorizzazioni del profilo dell'istanza per Systems Manager a un ruolo esistente (console)

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, scegli Ruoli e quindi scegli il ruolo esistente che desideri associare a un profilo dell'istanza per le operazioni di Systems Manager.
3. Nella scheda Autorizzazioni, scegli Aggiungi autorizzazioni, Collega policy.
4. Nella pagina Collega policy, esegui le operazioni seguenti:
 - Utilizza il campo di ricerca per individuare la AmazonSSMManagedInstanceCore policy. Seleziona la casella accanto al suo nome.
 - Se hai creato una policy del bucket S3 personalizzata, cercala e seleziona la casella accanto al suo nome. Per ulteriori informazioni sulle policy di bucket S3 personalizzate per un profilo dell'istanza, consulta [\(Facoltativo\) Creazione di una policy personalizzata per l'accesso al bucket S3](#).
 - Se intendi unire le istanze a un Active Directory gestito da Directory Service, cerca AmazonSSMDirectoryServiceAccess e seleziona la casella di controllo accanto al nome corrispondente.
 - Se intendi utilizzare EventBridge o CloudWatch Logs per gestire o monitorare la tua istanza, cerca CloudWatchAgentServerPolicy e seleziona la casella di controllo accanto al nome.
5. Scegli Collega policy.

Per informazioni su come aggiornare un ruolo per includere un'entità attendibile o limitare ulteriormente l'accesso, consulta [Modifica di un ruolo](#) nella Guida per l'utente di IAM.

(Facoltativo) Creazione di una policy personalizzata per l'accesso al bucket S3

La creazione di una policy personalizzata per l'accesso ad Amazon S3 è obbligatoria solo se si utilizza un endpoint VPC o un bucket S3 personale nelle operazioni di Systems Manager. È possibile collegare questa policy al ruolo IAM predefinito creato dalla configurazione di gestione host predefinita o a un profilo dell'istanza creato nella procedura precedente.

Per informazioni sui bucket S3 AWS gestiti a cui fornisci l'accesso nella seguente policy, consulta.

[Agente SSM comunicazioni con AWS bucket S3 gestiti](#)

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, seleziona Policy e quindi Crea policy.
3. Scegli la scheda JSON e sostituisci il testo predefinito con il seguente.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": [
        "arn:aws:s3:::aws-ssm-us-east-2/*",
        "arn:aws:s3:::aws-windows-downloads-us-east-2/*",
        "arn:aws:s3:::amazon-ssm-us-east-2/*",
        "arn:aws:s3:::amazon-ssm-packages-us-east-2/*",
        "arn:aws:s3:::us-east-2-birdwatcher-prod/*",
        "arn:aws:s3:::aws-ssm-distributor-file-us-east-2/*",
        "arn:aws:s3:::aws-ssm-document-attachments-us-east-2/*",
        "arn:aws:s3:::patch-baseline-snapshot-us-east-2/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetEncryptionConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    }
  ]
}
```

 Note

Il primo elemento di Statement è obbligatorio solo se si utilizza un endpoint VPC.

Il secondo elemento di Statement è obbligatorio solo se si utilizza un bucket S3 creato per l'uso nelle operazioni di Systems Manager.

L'autorizzazione della lista di controllo degli accessi PutObjectAcl è obbligatoria solo se si prevede di supportare l'accesso multi-account ai bucket S3 in altri account.

L'elemento GetEncryptionConfiguration è obbligatorio se il bucket S3 è configurato per utilizzare la crittografia.

Se il bucket S3 è configurato per utilizzare la crittografia, allora la radice del bucket S3 (ad esempio, `arn:aws:s3:::amzn-s3-demo-bucket`) deve essere elencata nella sezione Risorsa. L'utente, il gruppo o il ruolo deve essere configurato con l'accesso al bucket root.

4. Se utilizzi un endpoint VPC nelle operazioni, completa la seguente procedura:

Nel primo Statement elemento, sostituisci ogni *region* segnaposto con l'identificatore in cui verrà utilizzata Regione AWS questa policy. Ad esempio, per la Regione Stati Uniti orientali (Ohio), utilizza `us-east-2`. Per un elenco dei *region* valori supportati, vedere la colonna Regione negli endpoint [del servizio](#) Systems Manager in. Riferimenti generali di Amazon Web Services

 Important

Consigliamo di evitare l'uso di caratteri jolly (*) al posto delle Regioni specifiche in questa policy. Ad esempio, è preferibile utilizzare `arn:aws:s3:::aws-ssm-us-east-2/*` anziché `arn:aws:s3:::aws-ssm-*/*`. L'utilizzo di caratteri jolly potrebbe fornire l'accesso ai bucket S3 a cui non si intende concedere l'accesso. Se desideri utilizzare il profilo dell'istanza per più di una Regione, consigliamo di ripetere il primo elemento Statement per ciascuna Regione.

oppure

Se non si utilizza un endpoint VPC nelle operazioni, è possibile eliminare il primo elemento Statement.

5. Se si utilizza un bucket S3 personale nelle operazioni di Systems Manager, procedere nel seguente modo:

Nel secondo Statement elemento, sostituisci *amzn-s3-demo-bucket* con il nome di un bucket S3 nel tuo account. Usa questo bucket per le tue operazioni di Systems Manager. Offri l'autorizzazione per gli oggetti nel bucket, utilizzando "arn:aws:s3::my-bucket-name/*" come risorsa. Per ulteriori informazioni su come fornire le autorizzazioni per i bucket o per gli oggetti nei bucket, consulta l'argomento [Operazioni Amazon S3](#) nella Guida per l'utente di Amazon Simple Storage Service e il post del blog AWS [Policy IAM e policy di bucket e IACL! Oh, My! \(Controllo dell'accesso alle risorse S3\)](#).

 Note

Se utilizzi più di un bucket, indica l'ARN per ciascuno di essi. Guarda l'esempio che segue per le autorizzazioni sui bucket.

```
"Resource": [  
  "arn:aws:s3::amzn-s3-demo-bucket1/*",  
  "arn:aws:s3::amzn-s3-demo-bucket2/*"  
]
```

oppure

Se non utilizzi un bucket S3 personale nelle operazioni di Systems Manager, è possibile eliminare il secondo elemento Statement.

6. Scegli Successivo: Tag.
7. (Facoltativo) Aggiungi i tag scegliendo Aggiungi tag e inserendo i tag preferiti per la policy.
8. Seleziona Next: Revisione.
9. In Nome, immetti un nome per la policy, ad esempio **SSMInstanceProfileS3Policy**.
10. Scegli Crea policy.

Considerazioni aggiuntive sulle policy per le istanze gestite

Questa sezione descrive alcune delle policy che è possibile aggiungere al ruolo IAM predefinito creato dalla configurazione di gestione host predefinita o per i quali è possibile utilizzare i profili dell'istanza AWS Systems Manager. Per fornire le autorizzazioni per la comunicazione tra le istanze

e l'API di Systems Manager, consigliamo di creare policy personalizzate che riflettano le esigenze di sistema e dei requisiti di sicurezza. A seconda del piano delle operazioni, potrebbero essere necessarie le autorizzazioni rappresentate in una o più delle altre policy.

Policy: **AmazonSSMDirectoryServiceAccess**

Obbligatoria solo se prevedi di aggiungere istanze Amazon EC2 per Windows Server a una directory Microsoft AD.

Questa policy AWS gestita consente di accedere SSM Agent Servizio di directory AWS per conto dell'utente alle richieste di aggiunta al dominio da parte dell'istanza gestita. Per ulteriori informazioni, consulta [Aggiunta di un'istanza EC2 Windows](#) nella Guida di amministrazione di Servizio di directory AWS .

Policy: **CloudWatchAgentServerPolicy**

Richiesto solo se prevedi di installare ed eseguire l' CloudWatch agente sulle tue istanze per leggere i dati di metrica e log su un'istanza e scriverli su Amazon. CloudWatch Questi ti aiutano a monitorare, analizzare e rispondere rapidamente a problemi o modifiche alle tue AWS risorse.

Il ruolo IAM predefinito creato dalla configurazione di gestione host predefinita o dal profilo di istanza richiede questa policy solo se utilizzi funzionalità come Amazon EventBridge o Amazon CloudWatch Logs. (Puoi anche creare una policy più restrittiva che, ad esempio, limiti l'accesso in scrittura a uno specifico flusso di CloudWatch log di Logs).

Note

L'utilizzo CloudWatch delle funzionalità di EventBridge and Logs è facoltativo. Tuttavia, se intendi utilizzarle, è consigliabile configurare all'inizio del processo di configurazione di Systems Manager. Per ulteriori informazioni, consulta la [Amazon EventBridge User Guide](#) e la [Amazon CloudWatch Logs User Guide](#) .

Per creare policy IAM con autorizzazioni per strumenti aggiuntivi di Systems Manager, consulta le risorse seguenti:

- [Gestire l'accesso a Parameter Store parametri che utilizzano le politiche IAM](#)
- [Configurazione del servizio di automazione](#)
- [Fase 2: verifica o aggiunta di autorizzazioni dell'istanza per Session Manager](#)

Collegamento del profilo dell'istanza di Systems Manager a un'istanza (console)

La seguente procedura descrive come collegare un profilo dell'istanza IAM a un'istanza Amazon EC2 utilizzando la console Amazon EC2.

1. Accedi Console di gestione AWS e apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, in Istanze scegli Istanze.
3. Cercare e scegliere l'istanza EC2 nell'elenco.
4. Nel menu Actions (Operazioni), scegliere Security (Sicurezza), Modify IAM role (Modifica ruolo IAM).
5. Per Ruolo IAM, seleziona il profilo dell'istanza creato utilizzando la procedura descritta in [Configurazione alternativa per le autorizzazioni delle istanze EC2](#).
6. Scegli Aggiorna ruolo IAM.

Per ulteriori informazioni sul collegamento di ruoli IAM alle istanze, scegli uno dei seguenti riferimenti a seconda del tipo di sistema operativo selezionato:

- [Collegamento di un ruolo IAM a un'istanza](#) nella Guida per l'utente di Amazon EC2
- [Collegamento di un ruolo IAM a un'istanza](#) nella Guida per l'utente di Amazon EC2

Continua su [Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager](#).

Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager

Puoi migliorare il livello di sicurezza dei tuoi nodi gestiti (comprese le macchine non EC2 in un [ambiente](#) ibrido e multicloud) AWS Systems Manager configurando l'uso di un endpoint VPC di interfaccia in Amazon Virtual Private Cloud (Amazon VPC). Utilizzando un endpoint VPC di interfaccia (endpoint di interfaccia), puoi connetterti ai servizi forniti da AWS PrivateLink. AWS PrivateLink è una tecnologia che consente di accedere privatamente alle API Amazon Elastic Compute Cloud (Amazon EC2) e Systems Manager utilizzando indirizzi IP privati.

AWS PrivateLink limita tutto il traffico di rete tra le istanze gestite, Systems Manager e Amazon EC2 alla rete Amazon. Ciò vuol dire che le istanze gestite non hanno accesso a Internet. Se lo usi AWS

PrivateLink, non hai bisogno di un gateway Internet, di un dispositivo NAT o di un gateway privato virtuale.

La configurazione non è obbligatoria AWS PrivateLink, ma è consigliata. Per ulteriori informazioni sugli AWS PrivateLink endpoint VPC, consulta [AWS PrivateLink and VPC endpoint](#).

Note

L'alternativa all'utilizzo di un endpoint VPC è l'abilitazione dell'accesso a Internet in uscita sulle istanze gestite. In questo caso, le istanze gestite devono consentire anche il traffico in uscita HTTPS (porta 443) verso i seguenti endpoint:

- `ssm.region.amazonaws.com`
- `ssmmessages.region.amazonaws.com`
- `ec2messages.region.amazonaws.com`

SSM Agent avvia tutte le connessioni al servizio Systems Manager nel cloud. Per questo motivo, non è necessario configurare il firewall per consentire il traffico in ingresso verso le istanze di Systems Manager.

Per ulteriori informazioni sulle chiamate a questi endpoint, consulta [Referenza: ec2messages, ssmmessages e altre operazioni API](#).

Se si utilizza Systems Manager in un ambiente che supporta solo IPv6, è necessario consentire anche il traffico in uscita verso i seguenti endpoint:

- `ssm.region.api.aws`
- `ssmmessages.region.api.aws`
- `ec2messages.region.api.aws`

Per ulteriori informazioni sugli endpoint di servizio dual-stack, vedere gli endpoint [dual stack nella General Reference Guide](#). AWS

Devi inoltre assicurarti che i bucket per le operazioni di patch siano raggiungibili dai tuoi nodi, come descritto in [Reference: buckets Amazon S3 for patching operations](#).

Informazioni su Amazon VPC

Puoi utilizzare Amazon Virtual Private Cloud (Amazon VPC) per definire una rete virtuale nella tua area logicamente isolata all'interno di Cloud AWS, nota come cloud privato virtuale (VPC). È possibile avviare le risorse AWS, ad esempio le istanze, nel 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. È possibile 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 nel VPC a Internet. Puoi connettere il tuo VPC al tuo data center aziendale, rendendolo Cloud AWS un'estensione del tuo data center. Per proteggere le risorse in ciascuna sottorete, è possibile usare diversi livelli di sicurezza, compresi gruppi di sicurezza e liste di controllo accessi alla rete. Per ulteriori informazioni, consulta la [Guida utente Amazon VPC](#).

Argomenti

- [Restrizioni e limitazioni degli endpoint VPC](#)
- [Creazione degli endpoint VPC per Systems Manager](#)
- [Creazione di una policy degli endpoint VPC d'interfaccia](#)
- [Considerazioni sulle politiche degli endpoint VPC per i nodi ibridi](#)

Restrizioni e limitazioni degli endpoint VPC

Prima di configurare gli endpoint VPC di Systems Manager, occorre considerare le seguenti limitazioni e restrizioni.

Connessioni peering di VPC

Gli endpoint di interfaccia del VPC sono accessibili tramite connessioni peering VPC all'interno di una regione e tra regioni. Per ulteriori informazioni sulle richieste di connessione con peering VPC per gli endpoint dell'interfaccia VPC, consulta [Connessioni peering VPC \(quote\)](#) nella Guida per l'utente di Amazon Virtual Private Cloud.

Le connessioni endpoint del gateway VPC non possono essere estese all'esterno di un VPC. Le risorse sul lato opposto di una connessione peering VPC nel VPC non possono utilizzare l'endpoint del gateway per comunicare con le risorse del servizio endpoint gateway. Per ulteriori informazioni sulle richieste di connessione peering VPC per gli endpoint del gateway VPC, consulta [Connessioni peering VPC \(quote\)](#) nella Guida per l'utente di Amazon Virtual Private Cloud.

Connessioni in entrata

Il gruppo di sicurezza collegato all'endpoint VPC deve consentire le connessioni in entrata sulla porta 443 dalla sottorete privata dell'istanza gestita. Se le connessioni in entrata non sono consentite, l'istanza gestita non è in grado di connettersi agli endpoint SSM ed EC2.

Risoluzione DNS

Se utilizzi un server DNS personalizzato, devi aggiungere un server d'inoltro condizionale per eventuali query al dominio `amazonaws.com` al server Amazon DNS per il tuo VPC.

Bucket S3

È necessario che la policy dell'endpoint VPC consenta l'accesso almeno ai bucket Amazon S3 elencati su [Agente SSM comunicazioni con AWS bucket S3 gestiti](#).

Note

Se si usa un firewall on-premises e si intende utilizzare Patch Manager, il firewall deve consentire anche l'accesso all'endpoint della baseline delle patch appropriato.

Amazon Logs CloudWatch

Se non consenti alle tue istanze di accedere a Internet, crea un endpoint VPC per consentire a Logs di utilizzare le funzionalità che inviano CloudWatch i log a Logs. CloudWatch Per ulteriori informazioni sulla creazione di un endpoint per CloudWatch i log, consulta [Creating a VPC endpoint for CloudWatch Logs](#) nella Amazon Logs User Guide. CloudWatch

DNS in ambiente ibrido e multicloud

Per informazioni sulla configurazione del DNS per funzionare con gli AWS PrivateLink endpoint in [ambienti](#) ibridi e multicloud, consulta [Private DNS for interface endpoint nella Amazon VPC User Guide](#). Se si desidera utilizzare il proprio DNS, è possibile utilizzare il Resolver Route 53. Per ulteriori informazioni, consulta [Risoluzione delle query DNS tra i VPC e la propria rete](#) nella Guida per gli sviluppatori di Amazon Route 53.

Creazione degli endpoint VPC per Systems Manager

Utilizza le seguenti informazioni per creare endpoint di interfaccia VPC per AWS Systems Manager. Questo argomento si collega alle procedure descritte nella Guida utente Amazon VPC.

 Note

region rappresenta l'identificatore di una regione AWS supportata da AWS Systems Manager, ad esempio `us-east-2` per la regione Stati Uniti orientali (Ohio). Per un elenco dei **region** valori supportati, vedere la colonna Regione negli endpoint [del servizio Systems Manager](#) in Riferimenti generali di Amazon Web Services

Seguire la procedura in [Creazione di un endpoint di interfaccia](#) per creare i seguenti endpoint di interfaccia:

- **com.amazonaws.region.ssm**: l'endpoint per il servizio Systems Manager.
- **com.amazonaws.region.ec2messages**: Systems Manager utilizza questo endpoint per effettuare chiamate da SSM Agent al servizio Systems Manager. A partire dalla versione 3.3.40.0 dell'SSM Agent, Systems Manager ha iniziato a utilizzare endpoint `ssmmessages:*` (Amazon Message Gateway Service) ogni volta che era disponibile, al posto dell'endpoint `ec2messages:*` (Amazon Message Delivery Service).
- **com.amazonaws.region.ec2**— Se utilizzi Systems Manager per creare VSS-enabled istantanee, devi assicurarti di avere un endpoint per il servizio EC2. Se non è definito l'endpoint EC2, la chiamata per enumerare i volumi Amazon EBS collegati ha esito negativo e causa un errore del comando di Systems Manager.
- **com.amazonaws.region.s3**: Systems Manager utilizza questo endpoint per l'aggiornamento dell'SSM Agent. Systems Manager utilizza questo endpoint anche quando, facoltativamente, si sceglie di recuperare script o altri file archiviati in bucket o caricare log di output nel bucket. Se il gruppo di sicurezza associato alle istanze in uso limita il traffico in uscita, occorre aggiungere una regola per consentire al traffico di utilizzare l'elenco di prefissi per Amazon S3. Per ulteriori informazioni, consulta [Modifica del gruppo di sicurezza](#) nella Guida di AWS PrivateLink .
- **com.amazonaws.region.smmessages**: questo endpoint è necessario per far sì che l'SSM Agent comunichi con il servizio Systems Manager, per Run Command, e se ci si connette alle istanze tramite un canale dati sicuro utilizzando Session Manager. Per ulteriori informazioni, consulta [AWS Systems Manager Session Manager](#) e [Referenza: ec2messages, ssmmessages e altre operazioni API](#).
- (Facoltativo) **com.amazonaws.region.kms**: crea questo endpoint se desideri utilizzare la crittografia AWS Key Management Service (AWS KMS) per i parametri. Session Manager Parameter Store

- (Facoltativo) **com.amazonaws.*region*.logs**: crea questo endpoint se desideri utilizzare Amazon CloudWatch Logs (CloudWatch Logs) per Session ManagerRun Command, o SSM Agent logs.

Per informazioni sui bucket S3 AWS gestiti a cui SSM Agent deve essere possibile accedere, consulta [Agente SSM comunicazioni con AWS bucket S3 gestiti](#). Se si utilizza un endpoint VPC nelle operazioni di Systems Manager, è necessario fornire un'autorizzazione esplicita in un profilo di istanza EC2 o in un ruolo di servizio per i nodi gestiti non EC2.

Creazione di una policy degli endpoint VPC d'interfaccia

È possibile creare policy per gli endpoint dell'interfaccia VPC in cui è possibile specificare: AWS Systems Manager

- Il principale che può eseguire operazioni.
- Le operazioni che possono essere eseguite
- Le risorse su cui è possibile eseguire le operazioni

Per ulteriori informazioni, consulta [Controllo degli accessi ai servizi con endpoint VPC](#) nella Guida utente Amazon VPC.

Considerazioni sulle politiche degli endpoint VPC per i nodi ibridi

I nodi ibridi non appartengono nativamente a un, ma Account AWS ne sono registrati. Per questo motivo, le `ssm:UpdateManagedInstancePublicKey` API `ssm:RegisterManagedInstance` `ssm:RequestManagedInstanceRoleToken`, e non utilizzano AWS Signature Version 4 (Sigv4) per l'autenticazione dei nodi ibridi. Di conseguenza, la valutazione delle policy non può accedere a un'identità AWS principale o a chiavi di contesto globali come, e. `aws:PrincipalOrgId` `aws:PrincipalAccount` `aws:SourceAccount`. Le restrizioni delle policy sugli endpoint VPC che si basano su queste chiavi globali o sull'identità AWS principale potrebbero bloccare l'accesso a queste tre API.

Per risolvere questo problema, puoi utilizzare due chiavi di condizione fornite. AWS Systems Manager Queste chiavi funzionano in modo coerente sia in Amazon EC2 che in scenari ibridi:

- `ssm:NodeAccountId`— Si risolve nell'account in cui esiste un'istanza Amazon EC2 o nell'account in cui è registrato un nodo ibrido.

- `ssm:NodeOrgId`— Si riferisce all'organizzazione proprietaria dell'account dell'istanza Amazon EC2 o all'organizzazione dell'account in cui è registrato un nodo ibrido.

Gestione dei nodi in ambienti ibridi e multicloud con Systems Manager

Puoi utilizzarle AWS Systems Manager per gestire istanze Amazon Elastic Compute Cloud (Amazon EC2) insieme a macchine non EC2 in ambienti ibridi e multicloud. Systems Manager supporta server locali, dispositivi edge e macchine virtuali in esecuzione in altri ambienti cloud, incluso Microsoft Azure.

Questa sezione descrive le attività di configurazione eseguite dagli amministratori di account e di sistema per configurare macchine non EC2 da utilizzare con Systems Manager in un [ambiente ibrido e multicloud](#). Una volta completata questa procedura, gli utenti che hanno ricevuto le autorizzazioni dall'amministratore dell' Account AWS potranno utilizzare Systems Manager per configurare e gestire le macchine non EC2 dell'organizzazione.

Qualsiasi macchina che è stata configurata per l'uso con Systems Manager è chiamata nodo gestito.

Systems Manager fornisce due metodi per l'onboarding di macchine non EC2:

- Cloud Connectors: integra e gestisci automaticamente le macchine virtuali di Azure su larga scala da. Console di gestione AWS I Cloud Connectors gestiscono la federazione delle identità, l'installazione degli agenti e la registrazione delle macchine virtuali senza richiedere l'accesso diretto alle macchine virtuali di Azure. Per ulteriori informazioni, consulta [Configurare un Cloud Connector per Microsoft Azure in Systems Manager](#).
- Attivazioni ibride: registra singoli server locali, dispositivi edge e macchine virtuali da qualsiasi ambiente installando e attivando manualmente ogni macchina. SSM Agent Per ulteriori informazioni, consulta [Crea un'attivazione ibrida per registrare i nodi con Systems Manager](#).

Note

- È possibile registrare i dispositivi edge come nodi gestiti utilizzando gli stessi passaggi di attivazione ibrida utilizzati per altre macchine non EC2. Questi tipi di dispositivi periferici includono sia dispositivi che AWS IoT dispositivi diversi dai dispositivi. AWS IoT Systems Manager supporta anche i dispositivi edge che utilizzano il software AWS IoT Greengrass

Core. Il processo di configurazione e i requisiti per i dispositivi AWS IoT Greengrass principali sono diversi. Per informazioni sulla registrazione AWS IoT Greengrass dei dispositivi da utilizzare con Systems Manager, vedere [Gestione dei dispositivi edge con Systems Manager](#).

- Non-EC2 macOS le macchine non sono supportate per gli ambienti ibridi e multicloud di Systems Manager.

Note

Importante: a partire dal 30 giugno 2026, il livello di istanze avanzate è stato rimosso. Non esiste più un limite di 1.000 istanze per i nodi gestiti ibridi e non è più necessario abilitare un livello a pagamento da utilizzare su macchine non EC2. Session Manager Invece, a partire dal 30 settembre 2026, utilizza i prezzi Session Manager pay-as-you-go se Run Command utilizzati su nodi gestiti ibridi.

Per ulteriori informazioni sui prezzi, consulta [Prezzi di AWS Systems Manager](#).

Se prevedi di utilizzare Systems Manager per gestire le istanze Amazon Elastic Compute Cloud (Amazon EC2) o di utilizzare sia le istanze Amazon EC2 che le macchine non EC2 in un ambiente ibrido e multicloud, segui prima la procedura riportata in [Gestire le istanze EC2 con Systems Manager](#).

Dopo aver configurato l'ambiente ibrido e multicloud per Systems Manager, potrai eseguire le seguenti operazioni:

- Creare un modo coerente e sicuro per gestire in remoto carichi di lavoro ibridi e multicloud da una posizione utilizzando gli stessi strumenti o script.
- Centralizza il controllo degli accessi per le azioni che possono essere eseguite sui tuoi computer utilizzando (IAM). AWS Identity and Access Management
- Centralizza il controllo e la registrazione delle operazioni eseguite sui tuoi computer visualizzando l'attività API registrata in. AWS CloudTrail

Per informazioni sull'utilizzo per monitorare le azioni CloudTrail di Systems Manager, vedere. [Registrazione dei log AWS Systems Manager Chiamate API con AWS CloudTrail](#)

- Centralizza il monitoraggio configurando Amazon EventBridge e Amazon Simple Notification Service (Amazon SNS) per inviare notifiche sul successo dell'esecuzione del servizio.

Per informazioni sull'utilizzo per monitorare EventBridge gli eventi di Systems Manager, consulta [Monitoraggio degli eventi di Systems Manager con Amazon EventBridge](#)

Onboarding con Cloud Connectors

Un Cloud Connector è una risorsa di Systems Manager che stabilisce una relazione di fiducia tra l'utente Account AWS e un fornitore di servizi cloud di terze parti. Con Cloud Connectors, puoi integrare e gestire macchine virtuali da altri ambienti cloud su larga scala. Non è necessario accedere a singole VM, eseguire script o installare manualmente gli agenti.

Quando si crea un Cloud Connector, Systems Manager rileva le VM associate e le installa SSM Agent su ciascuna macchina virtuale. Le nuove VM online vengono registrate automaticamente. Dopo l'onboarding, le VM vengono visualizzate come nodi gestiti nella console unificata di Systems Manager insieme alle istanze Amazon EC2 e puoi gestirle utilizzando le stesse funzionalità di Systems Manager che usi per Amazon EC2.

I Cloud Connectors attualmente supportano Microsoft Azure. Per ulteriori informazioni, consulta [Configurare un Cloud Connector per Microsoft Azure in Systems Manager](#).

Onboarding con attivazioni ibride

Un'attivazione ibrida consente di registrare singoli server locali, dispositivi periferici e VM da qualsiasi ambiente come nodi gestiti. Con le attivazioni ibride, è possibile creare un'attivazione nella console di Systems Manager, installarla manualmente SSM Agent su ogni computer e registrarla utilizzando il codice di attivazione e l'ID.

Le attivazioni ibride offrono la flessibilità necessaria per l'integrazione di macchine da qualsiasi ambiente, inclusi data center locali, edge location e provider cloud che non sono ancora supportati da Cloud Connectors. Dopo la registrazione, le macchine appaiono come nodi gestiti e supportano le stesse funzionalità di Systems Manager delle istanze Amazon EC2.

Per ulteriori informazioni, consulta [Crea un'attivazione ibrida per registrare i nodi con Systems Manager](#).

Informazioni sui nodi gestiti

Dopo aver completato la configurazione delle macchine non EC2 per Systems Manager come descritto in questa sezione, le macchine attivate in modalità ibrida vengono elencate e descritte come

nodi gestiti. Console di gestione AWS Nella console, gli ID dei nodi gestiti attivati da sistemi ibridi sono distinti dalle istanze Amazon EC2 tramite il prefisso "mi-". Gli ID delle istanze Amazon EC2 utilizzano il prefisso "i-".

Un nodo gestito è un computer configurato per l'uso con Systems Manager. In precedenza, i nodi gestiti erano tutti indicati come istanze gestite. Il termine istanza ora si riferisce solo alle istanze EC2. Il comando [deregister-managed-instance](#) è stato denominato prima di questa modifica terminologica.

Per ulteriori informazioni, consulta [Utilizzo dei nodi gestiti](#).

Important

Si consiglia vivamente di evitare di utilizzare versioni del sistema operativo che hanno raggiunto (EOL). End-of-Life I fornitori di sistemi operativi, tra cui AWS in genere, non forniscono patch di sicurezza o altri aggiornamenti per le versioni che hanno raggiunto il termine di scadenza. Continuare a utilizzare un sistema EOL aumenta notevolmente il rischio di non poter applicare gli aggiornamenti, comprese le correzioni di sicurezza, e altri problemi operativi. AWS non verifica la funzionalità di Systems Manager sulle versioni del sistema operativo che hanno raggiunto il termine di scadenza.

Informazioni sui livelli di istanza

A partire dal 30 giugno 2026, il livello Advanced Instances è stato rimosso. Non esiste più un limite di 1.000 istanze per i nodi gestiti ibridi e non è più necessario abilitare un livello a pagamento per utilizzare Session Manager su macchine non EC2. Invece, Session Manager, Run Command e Patch Manager utilizzano prezzi pay-as-you-go se utilizzati su nodi gestiti ibridi.

Per ulteriori informazioni sui prezzi, consulta [Prezzi di AWS Systems Manager](#).

Argomenti

- [Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud](#)
- [Crea un'attivazione ibrida per registrare i nodi con Systems Manager](#)
- [Installa Agente SSM su nodi Linux ibridi](#)
- [Installa Agente SSM su ibrido Windows Server nodi](#)
- [Configurare Systems Manager per macchine virtuali Microsoft Azure](#)

Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud

Non-EC2 Le macchine (Amazon Elastic Compute Cloud) in un [ambiente](#) ibrido e multicloud richiedono un ruolo di servizio AWS Identity and Access Management (IAM) per comunicare con il servizio. AWS Systems Manager Il ruolo concede Servizio di token di sicurezza AWS (AWS STS) [AssumeRole](#) attendibile al servizio Systems Manager. Il ruolo di servizio per un ambiente ibrido e multicloud deve essere creato una sola volta per ogni Account AWS. Tuttavia, è possibile scegliere di creare più ruoli di servizio per diverse attivazioni ibride se le macchine dell'ambiente ibrido e multicloud richiedono autorizzazioni diverse.

Le procedure seguenti descrivono come creare il ruolo di servizio necessario utilizzando la console di Systems Manager o lo strumento a riga di comando preferito.

Utilizzo di Console di gestione AWS per creare un ruolo di servizio IAM per le attivazioni ibride di Systems Manager

La seguente procedura consente di creare un ruolo di servizio per un'attivazione ibrida. Questa procedura utilizza la policy AmazonSSMManagedInstanceCore per la funzionalità di base di Systems Manager. A seconda del caso d'uso, potrebbe essere necessario aggiungere ulteriori policy al ruolo di servizio per le macchine on-premises, in modo che tu possa accedere ad altri strumenti di Systems Manager o ai Servizi AWS. Ad esempio, senza l'accesso ai bucket AWS gestiti di Amazon Simple Storage Service (Amazon S3) richiesti, le operazioni di Patch Manager patching falliscono.

Per creare un ruolo di servizio (console)

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, scegli Ruoli e quindi Crea ruolo.
3. Per Seleziona un'entità attendibile, effettua le seguenti selezioni:
 1. Per Tipo di entità attendibile, seleziona Servizio AWS.
 2. Per altri casi d'uso Servizi AWS, scegli Systems Manager.
 3. Scegli Systems Manager.

L'immagine seguente evidenzia la posizione dell'opzione Systems Manager.

Service or use case

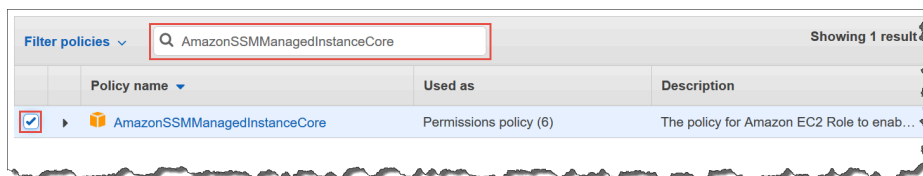
Systems Manager

Choose a use case for the specified service.

Use case

- ☒ **Systems Manager**
Allows SSM to call AWS services on your behalf
- ☐ **Systems Manager - Inventory and Maintenance Windows**
Allow AWS Systems Manager to call AWS resources on your behalf.

4. Scegli Successivo.
5. Nella pagina Add permissions (Aggiungi autorizzazioni), esegui le operazioni seguenti:
 - Usa il campo di ricerca per individuare la `AmazonSSMManagedInstanceCore` policy. Seleziona la casella di controllo accanto al relativo nome, come illustrato nella figura seguente.

**Note**

La console mantiene la selezione anche se cerchi altre policy.

- Se nella procedura [\(Facoltativo\) Creazione di una policy personalizzata per l'accesso al bucket S3](#) hai creato una policy di bucket S3 personalizzata, cercala e seleziona la casella accanto al suo nome.
 - Se prevedi di unire macchine non EC2 a un Active Directory gestito da Directory Service, cerca `AmazonSSMDirectoryServiceAccess` e seleziona la casella di controllo accanto al suo nome.
 - Se intendi utilizzare EventBridge o CloudWatch Logs per gestire o monitorare il tuo nodo gestito, cerca `CloudWatchAgentServerPolicy` e seleziona la casella di controllo accanto al suo nome.
6. Scegli Avanti.
 7. Per Nome ruolo, inserisci un nome per il nuovo ruolo del server IAM, ad esempio **SSMServerRole**.

 Note

Prendi nota del nome del ruolo. Scegli questo ruolo quando registri nuove macchine che desideri gestire utilizzando Systems Manager.

8. (Facoltativo) Per Descrizione ruolo, aggiorna la descrizione di questo ruolo del server IAM.
9. (Facoltativo) In Tag, aggiungi una o più coppie tag chiave-valore per organizzare, monitorare o controllare l'accesso per questo ruolo.
10. Scegliere Crea ruolo. Il sistema visualizza di nuovo la pagina Ruoli.

Utilizzo di AWS CLI per creare un ruolo di servizio IAM per le attivazioni ibride di Systems Manager

La seguente procedura consente di creare un ruolo di servizio per un'attivazione ibrida. Questa procedura utilizza la policy AmazonSSMManagedInstanceCore per la funzionalità di base di Systems Manager. A seconda del caso d'uso, potrebbe essere necessario aggiungere altre policy al ruolo di servizio in modo che le macchine non EC2 possano accedervi ad altre. Servizi AWS

Requisito delle policy di bucket S3

Se uno dei seguenti casi è true, è necessario creare una policy di autorizzazione IAM personalizzata per i bucket Amazon Simple Storage Service (Amazon S3) prima di completare questa procedura:

- Caso 1: stai utilizzando un endpoint VPC per connettere privatamente il tuo VPC ai servizi di endpoint VPC supportati Servizi AWS e forniti da. AWS PrivateLink
- Caso 2: prevedi di utilizzare un bucket Amazon S3 che hai creato durante le operazioni di Systems Manager, ad esempio per archiviare l'output per i comandi Run Command o le sessioni Session Manager in un bucket S3. Prima di procedere, segui i passaggi descritti in [Creare una policy di bucket S3 personalizzata per un profilo dell'istanza](#). Le informazioni sulle policy dei bucket S3 fornite in quell'argomento sono valide anche per il ruolo di servizio.

AWS CLI

Per creare un ruolo di servizio IAM per un ambiente ibrido e multicloud (AWS CLI)

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Creare un file di testo con un nome, ad esempio `SSMService-Trust.json` con la seguente policy di attendibilità. Salvare il file con l'estensione `.json`. Assicurati di specificare i tuoi Account AWS e i valori Regione AWS nell'ARN in cui hai creato l'attivazione ibrida. Sostituisci *placeholder values* l'ID dell'account e la regione con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:ssm:us-east-1:111122223333:*"
        }
      }
    }
  ]
}
```

3. Apri e AWS CLI, nella directory in cui hai creato il file JSON, esegui il [comando](#) `create-role` per creare il ruolo del servizio. Questo esempio crea un ruolo denominato `SSMServiceRole`. È possibile scegliere un nome diverso.

Linux & macOS

```
aws iam create-role \
  --role-name SSMServiceRole \
```

```
--assume-role-policy-document file://SSMSERVICE-Trust.json
```

Windows

```
aws iam create-role ^  
  --role-name SSMSERVICERole ^  
  --assume-role-policy-document file://SSMSERVICE-Trust.json
```

4. Esegui il comando [attach-role-policy](#) come segue per abilitare il ruolo di servizio appena creato per la creazione di un token di sessione. Il token della sessione concede al nodo gestito l'autorizzazione di eseguire comandi utilizzando Systems Manager.

Note

Le policy aggiunte per un profilo del servizio per i nodi gestiti in un ambiente ibrido e multicloud sono le stesse policy utilizzate per la creazione di un profilo dell'istanza per Amazon Elastic Compute Cloud (Amazon EC2). Per ulteriori informazioni sulle policy AWS utilizzate nei seguenti comandi, consulta [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#).

(Obbligatorio) Esegui il comando seguente per consentire a un nodo gestito di utilizzare le funzionalità di base del AWS Systems Manager servizio.

Linux & macOS

```
aws iam attach-role-policy \  
  --role-name SSMSERVICERole \  
  --policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

Windows

```
aws iam attach-role-policy ^  
  --role-name SSMSERVICERole ^  
  --policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

Se hai creato una policy bucket S3 personalizzata per il tuo ruolo di servizio, esegui il comando seguente per consentire ad AWS Systems Manager Agent (SSM Agent) di

accedere ai bucket specificati nella policy. Sostituisci *account-id* and *amzn-s3-demo-bucket* con il tuo Account AWS ID e il nome del bucket.

Linux & macOS

```
aws iam attach-role-policy \  
  --role-name SSMSERVICE_ROLE \  
  --policy-arn arn:aws:iam::account-id:policy/amzn-s3-demo-bucket
```

Windows

```
aws iam attach-role-policy ^  
  --role-name SSMSERVICE_ROLE ^  
  --policy-arn arn:aws:iam::account-id:policy/amzn-s3-demo-bucket
```

(Facoltativo) Esegui il comando seguente SSM Agent per consentire l'accesso per tuo Directory Service conto alle richieste di aggiunta al dominio da parte del nodo gestito. Il ruolo di servizio necessita di questa policy solo se aggiungi i nodi a una directory Microsoft AD.

Linux & macOS

```
aws iam attach-role-policy \  
  --role-name SSMSERVICE_ROLE \  
  --policy-arn arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess
```

Windows

```
aws iam attach-role-policy ^  
  --role-name SSMSERVICE_ROLE ^  
  --policy-arn arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess
```

(Facoltativo) Esegui il comando seguente per consentire l'esecuzione CloudWatch dell'agente sui tuoi nodi gestiti. Questo comando consente di leggere le informazioni su un nodo e di scriverle su CloudWatch. Il tuo profilo di servizio necessita di questa politica solo se utilizzi servizi come Amazon EventBridge o Amazon CloudWatch Logs.

```
aws iam attach-role-policy \  
  --role-name SSMSERVICE_ROLE \  
  --policy-arn arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
```

```
--policy-arn arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
```

Tools for PowerShell

Per creare un ruolo di servizio IAM per un ambiente ibrido e multicloud (AWS Tools for Windows PowerShell)

1. Installa e configura AWS Strumenti per PowerShell (Strumenti per Windows PowerShell), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione di AWS Strumenti per PowerShell](#).

2. Creare un file di testo con un nome, ad esempio `SSMService-Trust.json` con la seguente policy di attendibilità. Salvare il file con l'estensione `.json`. Assicurati di specificare il nome Account AWS e l'indirizzo Regione AWS nell'ARN in cui hai creato l'attivazione ibrida.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:ssm:us-east-1:123456789012:*"
        }
      }
    }
  ]
}
```

3. Apri PowerShell in modalità amministrativa e nella directory in cui hai creato il file JSON, esegui [New-IAMRole](#) quanto segue per creare un ruolo di servizio. Questo esempio crea un ruolo denominato `SSMSERVICE_ROLE`. È possibile scegliere un nome diverso.

```
New-IAMRole `
  -RoleName SSMSERVICE_ROLE `
  -AssumeRolePolicyDocument (Get-Content -raw SSMSERVICE_ROLE-Trust.json)
```

4. Usa [Register-IAMRolePolicy](#) quanto segue per consentire al ruolo di servizio che hai creato di creare un token di sessione. Il token della sessione concede al nodo gestito l'autorizzazione di eseguire comandi utilizzando Systems Manager.

 Note

Le policy aggiunte per un profilo del servizio per i nodi gestiti in un ambiente ibrido e multicloud sono le stesse policy utilizzate per la creazione di un profilo dell'istanza per EC2. Per ulteriori informazioni sulle AWS politiche utilizzate nei seguenti comandi, vedere [Configurazione delle autorizzazioni di istanza richieste per Systems Manager](#).

(Obbligatorio) Esegui il comando seguente per consentire a un nodo gestito di utilizzare le funzionalità AWS Systems Manager di base del servizio.

```
Register-IAMRolePolicy `
  -RoleName SSMSERVICE_ROLE `
  -PolicyArn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

Se è stata creata una policy di bucket S3 personalizzata per il ruolo di servizio, esegui il comando seguente per abilitare SSM Agent per l'accesso al bucket specificato nella policy. Sostituisci *account-id* and *my-bucket-policy-name* con il tuo Account AWS ID e il nome del bucket.

```
Register-IAMRolePolicy `
  -RoleName SSMSERVICE_ROLE `
  -PolicyArn arn:aws:iam::account-id:policy/my-bucket-policy-name
```


(Facoltativo) Esegui il comando seguente SSM Agent per consentire l'accesso per tuo Directory Service conto alle richieste di aggiunta al dominio da parte del nodo gestito. Il ruolo del server necessita di questa policy solo se aggiungi i nodi a una directory Microsoft AD.

```
Register-IAMRolePolicy `
  -RoleName SSMSERVICERole `
  -PolicyArn arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess
```

(Facoltativo) Esegui il comando seguente per consentire l'esecuzione CloudWatch dell'agente sui tuoi nodi gestiti. Questo comando consente di leggere le informazioni su un nodo e di scriverle su CloudWatch. Il tuo profilo di servizio necessita di questa politica solo se utilizzi servizi come Amazon EventBridge o Amazon CloudWatch Logs.

```
Register-IAMRolePolicy `
  -RoleName SSMSERVICERole `
  -PolicyArn arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
```

Continua su [Crea un'attivazione ibrida per registrare i nodi con Systems Manager](#).

Crea un'attivazione ibrida per registrare i nodi con Systems Manager

Per configurare macchine diverse dalle istanze Amazon Elastic Compute Cloud (EC2) come nodi gestiti per un ambiente [ibrido e multicloud](#), devi creare e applicare un'attivazione ibrida. Una volta completata l'attivazione, ricevi immediatamente un codice e un ID di attivazione nella parte superiore della pagina della console. Specificate questa combinazione di codice e ID quando installate AWS Systems Manager SSM Agent su macchine non EC2 per il vostro ambiente ibrido e multicloud. Il codice e l'ID forniscono accesso sicuro al servizio Systems Manager dai nodi gestiti.

Important

Systems Manager restituisce immediatamente il codice e l'ID di attivazione alla console o finestra di comando, a seconda di come è stata creata l'attivazione. Copia queste informazioni e archiviale in un luogo sicuro. Se esci dalla console o chiudi la finestra di comando, potresti perdere queste informazioni. Se le smarrisci, devi creare una nuova attivazione.

Informazioni sulle scadenze dell'attivazione

Una scadenza dell'attivazione è una finestra temporale durante la quale è possibile registrare macchine on-premises su Systems Manager. Un'attivazione scaduta non ha alcun impatto su server o macchine virtuali (VM) registrate in precedenza su Systems Manager. Se un'attivazione scade allora non è possibile registrare altri server o macchine virtuali su Systems Manager utilizzando tale specifica attivazione. È necessario crearne una nuova.

Ogni server e macchina virtuale (VM) on-premises registrata in precedenza rimane registrata come nodo gestito di Systems Manager, fino a quando annulli la registrazione esplicitamente. Puoi annullare la registrazione di un nodo gestito non EC2 nei seguenti modi:

- Utilizza la scheda Nodi gestiti in Fleet Manager nella console Systems Manager
- Usa il comando AWS CLI [deregister-managed-instance](#)
- Utilizza l'azione API [DeregisterManagedInstance](#).

Per ulteriori informazioni, consulta i seguenti argomenti

- [Annullamento della registrazione e nuova registrazione di un nodo gestito \(Linux\)](#)
- [Annullare la registrazione e ri-registrare un nodo gestito \(Windows Server\)](#)

Informazioni sui nodi gestiti

Un nodo gestito è qualsiasi macchina configurata per AWS Systems Manager. AWS Systems Manager supporta istanze Amazon Elastic Compute Cloud (Amazon EC2), dispositivi edge e server o VM locali, incluse le VM in altri ambienti cloud. In precedenza, i nodi gestiti erano tutti indicati come istanze gestite. Il termine istanza ora si riferisce solo alle istanze EC2. Il comando [deregister-managed-instance](#) è stato denominato prima di questa modifica terminologica.

Informazioni sui tag di attivazione

Se crei un'attivazione utilizzando AWS Command Line Interface (AWS CLI) o AWS Tools for Windows PowerShell, puoi specificare i tag. I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Di seguito è AWS CLI riportato un comando di esempio da eseguire nella regione Stati Uniti orientali (Ohio) su un computer Linux locale che include tag opzionali.

```
aws ssm create-activation \
```

```
--default-instance-name MyWebServers \  
--description "Activation for Finance department webserver" \  
--iam-role service-role/AmazonEC2RunCommandRoleForManagedInstances \  
--registration-limit 10 \  
--region us-east-2 \  
--tags "Key=Department,Value=Finance"
```

Se specifichi i tag durante la creazione di un'attivazione, tali tag vengono automaticamente assegnati ai nodi gestiti al momento della loro attivazione.

Non puoi aggiungere o eliminare tag da un'attivazione esistente. Se non desideri assegnare automaticamente tag ai server e alle macchine virtuali on-premises tramite un'attivazione, puoi aggiungerli in un secondo momento. In particolare, puoi applicare tag ai server e alle macchine virtuali on-premises dopo che si connettono a Systems Manager per la prima volta. Dopo la connessione, gli viene assegnato un ID nodo gestito elencato nella console Systems Manager con un ID preceduto da "mi-".

Note

Non puoi assegnare tag a un'attivazione se questa viene creata utilizzando la console Systems Manager. È necessario crearlo utilizzando AWS CLI o Tools for Windows PowerShell.

Se non desideri più gestire un server on-premises o una macchina virtuale (VM) con Systems Manager puoi annullare la registrazione. Per informazioni, consulta [Annullamento della registrazione dei nodi gestiti in un ambiente ibrido e multicloud](#).

Argomenti

- [Utilizzo Console di gestione AWS di per creare un'attivazione per la registrazione dei nodi gestiti con Systems Manager](#)
- [Utilizzo della riga di comando per creare un'attivazione per la registrazione dei nodi gestiti con Systems Manager](#)

Utilizzo Console di gestione AWS di per creare un'attivazione per la registrazione dei nodi gestiti con Systems Manager

Per creare un'attivazione di un nodo gestito

1. Aprire la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel riquadro di navigazione, selezionare Attivazioni ibride.
3. Scegli Create activation (Crea attivazione).

oppure

Se accedi ad Hybrid Activations per la prima volta nella versione corrente Regione AWS, scegli Crea un'attivazione.

4. (Facoltativo) Per Activation description (Descrizione attivazione), inserisci una descrizione per questa attivazione. Ti consigliamo di inserire una descrizione se prevedi di attivare un numero elevato di server e VM.
5. Ad esempio, limite, specifica il numero totale di nodi con cui desideri registrarti AWS come parte di questa attivazione. Il valore predefinito è una istanza.
6. Per il ruolo IAM, scegli un'opzione di ruolo di servizio che consenta ai server e alle macchine virtuali di comunicare AWS Systems Manager nel cloud:
 - Opzione 1: scegli Use the default role created by the system (Usa il ruolo predefinito creato dal sistema) per utilizzare un ruolo e una policy gestita fornita da AWS.
 - Opzione 2: scegli Seleziona un ruolo IAM personalizzato esistente con le autorizzazioni necessarie per utilizzare il ruolo personalizzato facoltativo che hai creato in precedenza. A tale ruolo deve essere associato una policy di relazione di trust che specifichi "Service": "ssm.amazonaws.com". Se il ruolo IAM non specifica questo principio in una policy di relazione di trust, viene visualizzato il seguente errore:

```
An error occurred (ValidationException) when calling the CreateActivation
operation: Not existing role:
arn:aws:iam::<accountid>:role/SSMRole
```

Per ulteriori informazioni sulla creazione di questo ruolo, consultare [Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud](#).

7. Per Activation expiry date (Data di scadenza dell'attivazione), specifica una data di scadenza per l'attivazione. La data di scadenza deve essere in futuro e non più di 30 giorni in futuro. Il valore predefinito è 24 ore.

 Note

Se vuoi registrare nodi gestiti aggiuntivi dopo la scadenza, devi creare una nuova attivazione. La data di scadenza non ha alcun impatto sui nodi registrati e in esecuzione.

8. (Facoltativo) Nel campo Default instance name (Nome predefinito dell'istanza), specifica un valore di nome identificativo da visualizzare per tutti i nodi gestiti associati a questa attivazione.
9. Scegli Create activation (Crea attivazione). Systems Manager restituisce immediatamente il codice di attivazione e l'ID alla console.

Utilizzo della riga di comando per creare un'attivazione per la registrazione dei nodi gestiti con Systems Manager

La procedura seguente descrive come utilizzare AWS Command Line Interface (AWS CLI) (su Linux o Windows Server) o AWS Strumenti per PowerShell creare un'attivazione gestita del nodo.

Per creare un'attivazione

1. Installa e configura il AWS CLI o il AWS Strumenti per PowerShell, se non l'hai già fatto.

Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

2. Eseguire il comando seguente per creare un'attivazione.

 Note

- Nel comando seguente, sostituiscilo *region* con le tue informazioni. Per un elenco dei *region* valori supportati, vedere la colonna Regione negli [endpoint del servizio Systems Manager](#) in. Riferimenti generali di Amazon Web Services
- Il ruolo specificato per il *iam-role* parametro deve avere una politica di relazione di fiducia che specifichi "Service": "ssm.amazonaws.com". Se il tuo ruolo AWS Identity and Access Management (IAM) non specifica questo principio in una politica di relazione di fiducia, ricevi il seguente errore:

An error occurred (ValidationException) when calling the CreateActivation operation: Not existing role:
arn:aws:iam::<accountid>:role/SSMRole

Per ulteriori informazioni sulla creazione di questo ruolo, consultare [Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud](#).

- Per `--expiration-date`, fornire una data in formato timestamp, ad esempio `"2021-07-07T00:00:00"`, per quando scade il codice di attivazione. È possibile specificare una data fino a 30 giorni di anticipo. Se non fornisci una data di scadenza, il codice di attivazione scade tra 24 ore.

Linux & macOS

```
aws ssm create-activation \
  --default-instance-name name \
  --iam-role iam-service-role-name \
  --registration-limit number-of-managed-instances \
  --region region \
  --expiration-date "timestamp" \
  --tags "Key=key-name-1,Value=key-value-1" "Key=key-name-2,Value=key-value-2"
```

Windows

```
aws ssm create-activation ^
  --default-instance-name name ^
  --iam-role iam-service-role-name ^
  --registration-limit number-of-managed-instances ^
  --region region ^
  --expiration-date "timestamp" ^
  --tags "Key=key-name-1,Value=key-value-1" "Key=key-name-2,Value=key-value-2"
```

PowerShell

```
New-SSMActivation -DefaultInstanceName name `
  -IamRole iam-service-role-name `
  -RegistrationLimit number-of-managed-instances `
  -Region region `
  -ExpirationDate "timestamp" `
```

```
-Tag @{"Key"="key-name-1";"Value"="key-value-1"},@{"Key"="key-name-2";"Value"="key-value-2"}
```

Ecco un esempio.

Linux & macOS

```
aws ssm create-activation \  
  --default-instance-name MyWebServers \  
  --iam-role service-role/AmazonEC2RunCommandRoleForManagedInstances \  
  --registration-limit 10 \  
  --region us-east-2 \  
  --expiration-date "2021-07-07T00:00:00" \  
  --tags "Key=Environment,Value=Production" "Key=Department,Value=Finance"
```

Windows

```
aws ssm create-activation ^  
  --default-instance-name MyWebServers ^  
  --iam-role service-role/AmazonEC2RunCommandRoleForManagedInstances ^  
  --registration-limit 10 ^  
  --region us-east-2 ^  
  --expiration-date "2021-07-07T00:00:00" ^  
  --tags "Key=Environment,Value=Production" "Key=Department,Value=Finance"
```

PowerShell

```
New-SSMActivation -DefaultInstanceName MyWebServers `   
  -IamRole service-role/AmazonEC2RunCommandRoleForManagedInstances `   
  -RegistrationLimit 10 `   
  -Region us-east-2 `   
  -ExpirationDate "2021-07-07T00:00:00" `   
  -Tag   
  @{"Key"="Environment";"Value"="Production"},@{"Key"="Department";"Value"="Finance"}
```

Se l'attivazione viene creata correttamente, il sistema restituisce immediatamente un codice e un ID di attivazione.

Installa Agente SSM su nodi Linux ibridi

Questo argomento descrive come installare AWS Systems Manager SSM Agent su macchine Linux non EC2 (Amazon Elastic Compute Cloud) in un ambiente [ibrido e multicloud](#). Per informazioni sull'installazione di SSM Agent su istanze EC2 per Linux, consulta [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#).

Prima di iniziare, individua il codice e l'ID di attivazione generati durante il processo di attivazione ibrida, come descritto in [Crea un'attivazione ibrida per registrare i nodi con Systems Manager](#). È possibile specificare il codice e l'ID nella procedura seguente.

Per installare Agente SSM su macchine non EC2 in un ambiente ibrido e multicloud

1. Accedi a un server o una macchina virtuale all'interno dell'ambiente ibrido e multicloud.
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 utilizzi un proxy, questa fase può essere ignorata.

Per un server proxy HTTP, immettere i comandi seguenti nella riga di comando:

```
export http_proxy=http://hostname:port  
export https_proxy=http://hostname:port
```

Per un server proxy HTTPS, immettere i comandi seguenti nella riga di comando:

```
export http_proxy=http://hostname:port  
export https_proxy=https://hostname:port
```

3. Copia e incolla uno dei seguenti blocchi di comandi in SSH. Sostituisci i valori segnaposto con il codice di attivazione e l'ID di attivazione generati durante il processo di attivazione ibrido e con l'identificatore del file da Regione AWS cui desideri eseguire il download, quindi premi. SSM Agent Enter

Important

Tieni presenti queste importanti informazioni relative a questo processo:

- L'utilizzo di `ssm-setup-cli` per installazioni non EC2 massimizza la sicurezza dell'installazione e della configurazione di Systems Manager.

- `sudo` non è necessario se sei un utente `root`.
- Effettua il download `ssm-setup-cli` dallo stesso sito Regione AWS in cui è stata creata l'attivazione ibrida.
- La `ssm-setup-cli` supporta un'opzione `manifest-url` che determina l'origine da cui viene scaricato l'agente. Non specificare un valore per questa opzione a meno che non sia richiesto dall'organizzazione.
- Durante la registrazione delle istanze, utilizza solo il link per il download fornito per la `ssm-setup-cli`. La `ssm-setup-cli` non deve essere conservata separatamente per usi futuri.
- È possibile utilizzare lo [script](#) `setupcli_data_integrity_linux.sh` per convalidare la firma di `ssm-setup-cli`.

region rappresenta l'identificatore di una regione Regione AWS supportata da AWS Systems Manager, ad esempio `us-east-2` per la regione Stati Uniti orientali (Ohio). Per un elenco dei **region** valori supportati, vedere la colonna Regione negli endpoint [del servizio](#) Systems Manager in. Riferimenti generali di Amazon Web Services

Inoltre, la `ssm-setup-cli` include le seguenti opzioni:

- `version`: i valori validi sono `latest` e `stable`.
- `downgrade`: consente il downgrade di SSM Agent a una versione precedente. Specifica `true` per installare una versione precedente dell'agente.
- `skip-signature-validation`: ignora la convalida della firma durante il download e l'installazione dell'agente.
- `provider` (Facoltativo): specifica il provider cloud della macchina da registrare. I valori validi sono `Azure` e `EC2`. Quando specificato, SSM Agent legge i metadati dell'istanza dall'Instance Metadata Service (IMDS) del provider cloud e associa il nodo gestito all'istanza di calcolo di origine. Se omesso, il comportamento predefinito rimane invariato e non vengono raccolti metadati del provider cloud.

Amazon Linux 2, RHEL 7.x e Oracle Linux

```
mkdir /tmp/ssm
curl https://amazon-ssm-region.s3.region.amazonaws.com/latest/linux_amd64/ssm-setup-cli
-o /tmp/ssm/ssm-setup-cli
```

```
sudo chmod +x /tmp/ssm/ssm-setup-cli
sudo /tmp/ssm/ssm-setup-cli -register -activation-code "activation-code" -activation-id "activation-id" -region "region"
```

RHEL 8.x

```
mkdir /tmp/ssm
curl https://amazon-ssm-region.s3.region.amazonaws.com/latest/linux_amd64/ssm-setup-cli -o /tmp/ssm/ssm-setup-cli
sudo chmod +x /tmp/ssm/ssm-setup-cli
sudo /tmp/ssm/ssm-setup-cli -register -activation-code "activation-code" -activation-id "activation-id" -region "region"
```

Debian Server

```
mkdir /tmp/ssm
curl https://amazon-ssm-region.s3.region.amazonaws.com/latest/debian_amd64/ssm-setup-cli -o /tmp/ssm/ssm-setup-cli
sudo chmod +x /tmp/ssm/ssm-setup-cli
sudo /tmp/ssm/ssm-setup-cli -register -activation-code "activation-code" -activation-id "activation-id" -region "region"
```

Ubuntu Server

- Utilizzo dei pacchetti .deb

```
mkdir /tmp/ssm
curl https://amazon-ssm-region.s3.region.amazonaws.com/latest/debian_amd64/ssm-setup-cli -o /tmp/ssm/ssm-setup-cli
sudo chmod +x /tmp/ssm/ssm-setup-cli
sudo /tmp/ssm/ssm-setup-cli -register -activation-code "activation-code" -activation-id "activation-id" -region "region"
```

- Utilizzo dei pacchetti Snap

Non è necessario specificare un URL per il download, poiché il snap comando scarica automaticamente l'agente dall'app store di [Snap](https://snapcraft.io) all'indirizzo <https://snapcraft.io>.

Su LTS Ubuntu Server 20.04 e 18.04, i file di SSM Agent installazione, inclusi i file binari dell'agente e i file di configurazione, sono archiviati nella seguente directory: `/snap/amazon-ssm-agent/current/` Se apporti modifiche ai file di configurazione in questa directory, devi

copiare questi file dalla cartella `/snap` nella cartella `/etc/amazon/ssm/`. I file di log e della libreria non sono cambiati (`/var/lib/amazon/ssm`, `/var/log/amazon/ssm`).

```
sudo snap install amazon-ssm-agent --classic
sudo systemctl stop snap.amazon-ssm-agent.amazon-ssm-agent.service
sudo /snap/amazon-ssm-agent/current/amazon-ssm-agent -register -code "activation-code" -id "activation-id" -region "region"
sudo systemctl start snap.amazon-ssm-agent.amazon-ssm-agent.service
```

Important

La candidatura nell'archivio Snap contiene l'ultima versione di SSM Agent; non il canale stabile. Se desideri tenere traccia delle informazioni sulla SSM Agent versione sul canale candidato, esegui il seguente comando sui nodi gestiti 18.04 LTS a 64 bit. Ubuntu Server

```
sudo snap switch --channel=candidate amazon-ssm-agent
```

Il comando scarica e installa SSM Agent sulla macchina attivata da sistemi ibridi nell'ambiente ibrido e multicloud. Il comando interrompe SSM Agent e quindi registra la macchina con il servizio Systems Manager. La macchina è ora un nodo gestito. Le istanze Amazon EC2 configurate per Systems Manager sono anche nodi gestiti. Nella console di Systems Manager, tuttavia, i nodi attivati da sistemi ibridi si distinguono dalle istanze Amazon EC2 tramite il prefisso "mi-".

Continua su [Installa Agente SSM su ibrido Windows Server nodi](#).

Impostazione della rotazione automatica della chiave privata

Per rafforzare il tuo livello di sicurezza, puoi configurare AWS Systems Manager Agent (SSM Agent) per ruotare automaticamente la chiave privata per il tuo ambiente ibrido e multicloud. È possibile accedere a questa funzionalità utilizzando SSM Agent 3.0.1031.0 o versioni successive. Attivare questa funzionalità seguendo la procedura seguente.

Per configurare Agente SSM per ruotare la chiave privata per un ambiente ibrido e multicloud

1. Accedi a `/etc/amazon/ssm/` su una macchina Linux o `C:\Program Files\Amazon\SSM` per una macchina Windows.

2. Copiare il contenuto `amazon-ssm-agent.json.template` in un nuovo file denominato `amazon-ssm-agent.json`. Salvare (Salva) `amazon-ssm-agent.json` nella stessa directory dove `amazon-ssm-agent.json.template` si trova.
3. Trova `Profile`, `KeyAutoRotateDays`. Immettere il numero di giorni desiderato tra le rotazioni automatiche della chiave privata.
4. Riavviare SSM Agent.

Ogni volta che si modifica la configurazione, riavviare SSM Agent.

È possibile personalizzare altre funzionalità di SSM Agent utilizzando la stessa procedura. Per l'elenco aggiornato delle proprietà di configurazione disponibili e dei relativi valori predefiniti, vedi [Definizioni delle proprietà](#).

Annullamento della registrazione e nuova registrazione di un nodo gestito (Linux)

È possibile annullare la registrazione di un nodo gestito attivato da un sistema ibrido richiamando l'operazione [DeregisterManagedInstance](#) API da Tools for Windows o da Tools for Windows. AWS CLI PowerShell Di seguito è illustrato un esempio di comando CLI:

```
aws ssm deregister-managed-instance --instance-id "mi-1234567890"
```

Per rimuovere le informazioni di registrazione rimanenti per l'agente, rimuovi la chiave `IdentityConsumptionOrder` dal file `amazon-ssm-agent.json`. Quindi, a seconda del tipo di installazione, esegui uno dei seguenti comandi.

Sui nodi Ubuntu Server in cui è stato installato SSM Agent utilizzando i pacchetti Snap:

```
sudo /snap/amazon-ssm-agent/current/amazon-ssm-agent -register -clear
```

Su tutte le altre installazioni Linux:

```
amazon-ssm-agent -register -clear
```

Note

Puoi registrare nuovamente un server on-premises, un dispositivo edge o una macchina virtuale locale utilizzando lo stesso codice di attivazione e lo stesso ID, purché non sia stato raggiunto il limite di istanze per il codice di attivazione e l'ID designati. Puoi

verificare il limite di istanza per un codice e un ID di attivazione chiamando l'API [describe-activations](#) utilizzando il AWS CLI. Dopo aver eseguito il comando, verifica che il valore di `RegistrationCount` non sia superiore a `RegistrationLimit`. Se è maggiore, è necessario utilizzare un codice e un ID di attivazione diversi.

Per registrare nuovamente un nodo gestito su una macchina Linux non EC2

1. Connettiti alla macchina.
2. Eseguire il seguente comando seguente. Assicurati di sostituire i valori segnaposto con il codice e l'ID di attivazione generati quando hai creato un'attivazione del nodo gestito e con l'identificativo della Regione da cui desideri scaricare l'SSM Agent.

```
echo "yes" | sudo /tmp/ssm/ssm-setup-cli -register -activation-code "activation-code" -activation-id "activation-id" -region "region"
```

Risoluzione dei problemi Agente SSM installazione su macchine Linux non EC2

Usa le informazioni seguenti per risolvere i problemi relativi all'installazione di SSM Agent su macchine Linux attivate da sistemi ibridi in un ambiente [ibrido e multicloud](#).

Riceverai un errore `DeliveryTimedOut`

Problema: durante la configurazione di un computer in uno Account AWS come nodo gestito per un altro Account AWS, `DeliveryTimedOut` dopo l'esecuzione, si ricevono i comandi da installare SSM Agent sul computer di destinazione.

Soluzione: `DeliveryTimedOut` è il codice di risposta previsto per questo scenario. Il comando per installare SSM Agent sul nodo target modifica l'ID del nodo di origine. Poiché l'ID del nodo è cambiato, il nodo sorgente non può rispondere al nodo di destinazione dicendo che il comando non è riuscito, completato o è scaduto durante l'esecuzione.

Impossibile caricare le associazioni del nodo

Problema: dopo aver eseguito i comandi di installazione, viene visualizzato il seguente errore nei log di errore dell'SSM Agent:

```
Unable to load instance associations, unable to retrieve  
associations unable to retrieve associations error occurred in
```

RequestManagedInstanceRoleToken: MachineFingerprintDoesNotMatch:
Fingerprint doesn't match

Questo errore viene visualizzato quando l'ID macchina non persiste dopo un riavvio.

Soluzione: Per risolvere questo problema, eseguire il comando seguente. Questo comando costringe l'ID macchina a mantenere l'aspetto persistente dopo un riavvio.

```
umount /etc/machine-id  
systemd-machine-id-setup
```

Installa Agente SSM su ibrido Windows Server nodi

Questo argomento descrive come eseguire l'installazione AWS Systems Manager SSM Agent su Windows Server macchine in un ambiente [ibrido e multicloud](#). Per informazioni sull'installazione di SSM Agent su istanze EC2 per Windows Server consultare [Installazione e disinstallazione manuali Agente SSM su istanze EC2 per Windows Server](#).

Prima di iniziare, individua il codice e l'ID di attivazione generati durante il processo di attivazione ibrida, come descritto in [Crea un'attivazione ibrida per registrare i nodi con Systems Manager](#). È possibile specificare il codice e l'ID nella procedura seguente.

Per installare Agente SSM su sistemi non EC2 Windows Server macchine in un ambiente ibrido e multicloud

1. Accedi a un server o una macchina virtuale all'interno dell'ambiente ibrido e multicloud.
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 utilizzi un proxy, questa fase può essere ignorata.

Per un server proxy HTTP, impostare la variabile seguente:

```
http_proxy=http://hostname:port  
https_proxy=http://hostname:port
```

Per un server proxy HTTPS, impostare questa variabile:

```
http_proxy=http://hostname:port  
https_proxy=https://hostname:port
```

Per PowerShell, configurare le impostazioni del proxy WinInet:

```
[System.Net.WebRequest]::DefaultWebProxy

$proxyServer = "http://hostname:port"
$proxyBypass = "169.254.169.254"
$WebProxy = New-Object System.Net.WebProxy($proxyServer,$true,$proxyBypass)

[System.Net.WebRequest]::DefaultWebProxy = $WebProxy
```

 Note

La configurazione del proxy WinInet è necessaria per le operazioni. PowerShell Per ulteriori informazioni, consulta [the section called “Impostazioni del proxy di SSM Agent e servizi di Systems Manager”](#).

3. Apri Windows PowerShell come amministratore.
4. Copia e incolla il seguente blocco di comandi in Windows PowerShell. Sostituisci ogni *example resource placeholder* con le tue informazioni. Ad esempio, il codice di attivazione e l'ID di attivazione generati quando si crea un'attivazione ibrida e con l'identificatore da Regione AWS cui si desidera effettuare il download. SSM Agent

 Important

Tieni presenti queste importanti informazioni relative a questo processo:

- L'utilizzo di `ssm-setup-cli` per installazioni non EC2 massimizza la sicurezza dell'installazione e della configurazione di Systems Manager.
- La `ssm-setup-cli` supporta un'opzione `manifest-url` che determina l'origine da cui viene scaricato l'agente. Non specificare un valore per questa opzione a meno che non sia richiesto dall'organizzazione.
- È possibile utilizzare lo script [setupcli_data_integrity_windows.ps1](#) per convalidare la firma di `ssm-setup-cli`

- Durante la registrazione delle istanze, utilizza solo il link per il download fornito per la `ssm-setup-cli`. La `ssm-setup-cli` non deve essere conservata separatamente per usi futuri.

region rappresenta l'identificatore di una regione supportata da, ad esempio per la regione Stati Uniti orientali (Ohio). Regione AWS `us-east-2` Per un elenco dei *region* valori supportati, vedere la colonna Regione negli endpoint [del servizio](#) Systems Manager in. Riferimenti generali di Amazon Web Services

Inoltre, la `ssm-setup-cli` include le seguenti opzioni:

- `version`: i valori validi sono `latest` e `stable`.
- `downgrade`: riporta l'agente a una versione precedente.
- `skip-signature-validation`: ignora la convalida della firma durante il download e l'installazione dell'agente.
- `provider`(Facoltativo): specifica il provider cloud della macchina da registrare. I valori validi sono `Azure` e `EC2`. Quando specificato, SSM Agent legge i metadati dell'istanza dall'Instance Metadata Service (IMDS) del provider cloud e associa il nodo gestito all'istanza di calcolo di origine. Se omesso, il comportamento predefinito rimane invariato e non vengono raccolti metadati del provider cloud.

64-bit

```
[System.Net.ServicePointManager]::SecurityProtocol = 'TLS12'
$code = "activation-code"
$id = "activation-id"
$region = "us-east-1"
$dir = $env:TEMP + "\ssm"
New-Item -ItemType directory -Path $dir -Force
cd $dir
(New-Object System.Net.WebClient).DownloadFile("https://amazon-ssm-$region.s3.
$region.amazonaws.com/latest/windows_amd64/ssm-setup-cli.exe", $dir + "\ssm-
setup-cli.exe")
./ssm-setup-cli.exe -register -activation-code="$code" -activation-id="$id" -
region="$region"
Get-Content ($env:ProgramData + "\Amazon\SSM\InstanceData\registration")
Get-Service -Name "AmazonSSMAgent"
```


5. Premi Enter.

Note

Se il comando ha esito negativo, verificare che sia in esecuzione la versione più recente di AWS Strumenti per PowerShell.

Il comando esegue quanto segue:

- Scarica e installa SSM Agent sulla macchina.
- Registra la macchina con il servizio Systems Manager.
- Restituisce una risposta alla richiesta simile a quella riportata di seguito:

```
Directory: C:\Users\ADMINI~1\AppData\Local\Temp\2
```

Mode	LastWriteTime	Length	Name
d-----	07/07/2018 8:07 PM		ssm
{ "ManagedInstanceID": "mi-008d36be46EXAMPLE", "Region": "us-east-2" }			
Status	: Running		
Name	: AmazonSSMAgent		
DisplayName	: Amazon SSM Agent		

La macchina è ora un nodo gestito. Questi nodi gestiti ora vengono identificati con il prefisso "mi-". È possibile visualizzare i nodi gestiti nella pagina [Nodo Fleet Manager gestito](#) in utilizzando il AWS CLI comando o utilizzando [describe-instance-information](#) il comando API. [DescribeInstanceInformation](#)

Impostazione della rotazione automatica della chiave privata

Per rafforzare il tuo livello di sicurezza, puoi configurare AWS Systems Manager Agent (SSM Agent) per ruotare automaticamente la chiave privata per un ambiente ibrido e multicloud. È possibile accedere a questa funzionalità utilizzando SSM Agent 3.0.1031.0 o versioni successive. Attivare questa funzionalità seguendo la procedura seguente.

Per configurare Agente SSM per ruotare la chiave privata per un ambiente ibrido e multicloud

1. Accedi a `/etc/amazon/ssm/` su una macchina Linux o `C:\Program Files\Amazon\SSM` per una macchina Windows Server.
2. Copiare il contenuto `amazon-ssm-agent.json.template` in un nuovo file denominato `amazon-ssm-agent.json`. Salvare (Salva) `amazon-ssm-agent.json` nella stessa directory dove `amazon-ssm-agent.json.template` si trova.
3. Trova `Profile`, `KeyAutoRotateDays`. Immettere il numero di giorni desiderato tra le rotazioni automatiche della chiave privata.
4. Riavviare SSM Agent.

Ogni volta che si modifica la configurazione, riavviare SSM Agent.

È possibile personalizzare altre funzionalità di SSM Agent utilizzando la stessa procedura. Per l'elenco aggiornato delle proprietà di configurazione disponibili e dei relativi valori predefiniti, vedi [Definizioni delle proprietà](#).

Annullare la registrazione e ri-registrare un nodo gestito (Windows Server)

È possibile annullare la registrazione di un nodo gestito richiamando l'operazione [DeregisterManagedInstance](#) API da Tools for Windows o da Tools for Windows. AWS CLI PowerShell Di seguito è illustrato un esempio di comando CLI:

```
aws ssm deregister-managed-instance --instance-id "mi-1234567890"
```

Per rimuovere le informazioni di registrazione rimanenti per l'agente, rimuovi la chiave `IdentityConsumptionOrder` dal file `amazon-ssm-agent.json`. Quindi, esegui il comando riportato di seguito:

```
amazon-ssm-agent -register -clear
```

Note

Puoi registrare nuovamente un server on-premises, un dispositivo edge o una macchina virtuale locale utilizzando lo stesso codice di attivazione e lo stesso ID, purché non sia stato raggiunto il limite di istanze per il codice di attivazione e l'ID designati. Puoi verificare il limite di istanza per un codice e un ID di attivazione chiamando l'API [describe-activations](#) utilizzando il AWS CLI. Dopo aver eseguito il comando, verifica che il valore

di `RegistrationCount` non sia superiore a `RegistrationLimit`. Se è maggiore, è necessario utilizzare un codice e un ID di attivazione diversi.

Per registrare nuovamente un nodo gestito su un Windows Server macchina ibrida

1. Connettiti alla macchina.
2. Eseguire il seguente comando seguente. Assicurati di sostituire i valori segnaposto con il codice e l'ID di attivazione generati, quando hai creato un'attivazione ibrida e con l'identificativo della Regione da cui desideri scaricare l'SSM Agent.

```
$dir = $env:TEMP + "\ssm"
cd $dir
Start-Process ./ssm-setup-cli.exe -ArgumentList @(
    "-register",
    "-activation-code=$code",
    "-activation-id=$id",
    "-region=$region"
) -Wait -NoNewWindow
```

Configurare Systems Manager per macchine virtuali Microsoft Azure

Puoi registrare le macchine virtuali (VM) di Azure come nodi gestiti di Systems Manager usando il processo di attivazione ibrido con l'integrazione nativa di Azure Instance Metadata Service (IMDS). Quando si specifica il `-provider Azure` parametro durante la registrazione, SSM Agent legge i dati di identità delle macchine virtuali di Azure direttamente dall'endpoint IMDS di Azure e associa il nodo gestito alla macchina virtuale di Azure di origine.

Questa integrazione offre i seguenti vantaggi:

- Associazione dell'identità dell'istanza: il nodo gestito SSM (mi-) viene automaticamente collegato all'ID VM di Azure, consentendo il monitoraggio coerente delle risorse tra i cloud.
- Ricca raccolta di metadati: le proprietà delle macchine virtuali di Azure, come l'ID di sottoscrizione, il gruppo di risorse, la posizione e la zona di disponibilità, vengono acquisite e visualizzate come attributi del nodo gestito.
- Sicurezza avanzata: la designazione esplicita del provider previene gli attacchi di impersonificazione IMDS e garantisce che le credenziali siano assegnate al provider cloud corretto.

 Note

Prima di iniziare, completa i passaggi preliminari per creare un ruolo di servizio IAM e un'attivazione ibrida, come descritto in e. [Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud](#) [Crea un'attivazione ibrida per registrare i nodi con Systems Manager](#)

Installa SSM Agent su macchine virtuali Linux di Azure

Usa la procedura seguente per installare e registrare SSM Agent su una macchina virtuale Linux di Azure.

Per l'installazione SSM Agent su una macchina virtuale Linux di Azure

1. Connect alla tua macchina virtuale di Azure.
2. Esegui i comandi seguenti. Sostituisci i valori segnaposto con il codice di attivazione e l'ID di attivazione generati durante il processo di attivazione ibrida e con l'identificatore che desideri utilizzare. Regione AWS

 Note

Il comando seguente utilizza il file binario. `linux_amd64` Se la tua macchina virtuale di Azure usa un processore ARM64 (ad esempio, serie Dpsv5 o Epsv5), sostituiscilo con. `linux_amd64 linux_arm64`

```
mkdir /tmp/ssm
curl https://amazon-ssm-region.s3.region.amazonaws.com/latest/linux_amd64/ssm-
setup-cli -o /tmp/ssm/ssm-setup-cli
sudo chmod +x /tmp/ssm/ssm-setup-cli
sudo /tmp/ssm/ssm-setup-cli -register \
    -activation-code "activation-code" \
    -activation-id "activation-id" \
    -region "region" \
    -provider Azure
```

3. Verifica che sia in esecuzione e che i SSM Agent dati di registrazione siano stati scritti correttamente:

```
sudo systemctl status amazon-ssm-agent  
cat /var/lib/amazon/ssm/registration
```

Installazione SSM Agent su macchine virtuali di Azure Windows Server

Usa la seguente procedura per installare e registrare SSM Agent su una macchina virtuale di AzureWindows Server.

Per installare SSM Agent su una macchina virtuale di Azure Windows Server

1. Connect alla tua macchina virtuale di Azure.
2. Apri Windows PowerShell come amministratore.
3. Copia e incolla il seguente blocco di comandi in Windows PowerShell. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Note

Il comando seguente usa il file binario. windows_amd64 Se la tua macchina virtuale di Azure usa un processore ARM64, sostituiscilo con. windows_amd64 windows_arm64

```
[System.Net.ServicePointManager]::SecurityProtocol = 'TLS12'  
$code = "activation-code"  
$id = "activation-id"  
$region = "us-east-1"  
$dir = $env:TEMP + "\ssm"  
New-Item -ItemType directory -Path $dir -Force  
cd $dir  
(New-Object System.Net.WebClient).DownloadFile("https://amazon-ssm-$region.s3.  
$region.amazonaws.com/latest/windows_amd64/ssm-setup-cli.exe", $dir + "\ssm-setup-  
cli.exe")  
Start-Process ./ssm-setup-cli.exe -ArgumentList @(  
    "-register",  
    "-activation-code=$code",  
    "-activation-id=$id",  
    "-region=$region",  
    "-provider=Azure"  
) -Wait -NoNewWindow
```

```
Get-Content ($env:ProgramData + "\Amazon\SSM\InstanceData\registration")
Get-Service -Name "AmazonSSMAgent"
```

Mappatura dei metadati delle macchine virtuali di Azure

Quando registri una macchina virtuale di Azure usando il `-provider Azure` parametro, SSM Agent legge le seguenti proprietà dall'endpoint Azure IMDS (<http://169.254.169.254/metadata/instance>) e le mappa agli attributi del nodo gestito di Systems Manager corrispondenti.

Proprietà del nodo gestito	Campo Azure IMDS	Valore di esempio
ComputerName	{compute.subscriptionId}:{compute.resourceGroupName}:{compute.name}	14724fea-7bad-4c32-8af0-ebde38f42a46:MyRG:my-azure-vm
SourceType	Hardcoded	Microsoft.Compute/virtualMachines
SourceID	{compute.vmId}	1724afd8-9092-429e-8b04-0708130c38f7
SourceLocation	{compute.location}	centralus
AvailabilityZone	{compute.zone}	1
AvailabilityZoneId	Zone{compute.zone}	Zone1

Verifica la registrazione del nodo gestito utilizzando `DescribeInstanceInformation`

Dopo la registrazione, usa il [describe-instance-information](#) comando per confermare che i metadati delle macchine virtuali di Azure sono stati acquisiti correttamente. L'esempio seguente filtra `SourceId` utilizzando l'ID di macchina virtuale di Azure:

```
aws ssm describe-instance-information \
  --filters "Key=SourceIds,Values=1724afd8-9092-429e-8b04-0708130c38f7" \
  --region us-east-1
```

La risposta include l'ID del nodo gestito (con il prefisso `mi-`) e i campi di metadati popolati come, e:

ComputerName	SourceId	SourceType
--------------	----------	------------

```
{
  "InstanceInformationList": [
    {
      "InstanceId": "mi-008d36be46EXAMPLE",
      "ComputerName": "14724fea-7bad-4c32-8af0-ebde38f42a46:MyRG:my-azure-vm",
      "SourceId": "1724afd8-9092-429e-8b04-0708130c38f7",
      "SourceType": "Microsoft.Compute/virtualMachines",
      "SourceLocation": "centralus",
      "AvailabilityZone": "1",
      "AvailabilityZoneId": "Zone1",
      "PingStatus": "Online",
      "PlatformType": "Linux",
      "PlatformName": "Ubuntu",
      "PlatformVersion": "24.04"
    }
  ]
}
```

Configurare un Cloud Connector per Microsoft Azure in Systems Manager

Un Systems Manager Cloud Connector è una risorsa che stabilisce una connessione tra Systems Manager e macchine virtuali (VM) in un provider cloud esterno come Microsoft Azure. Dopo aver creato un Cloud Connector, i servizi di Systems Manager come Automation e State Manager possono indirizzare e gestire le VM di Azure come se fossero nodi gestiti nativi.

Questa sezione contiene gli argomenti seguenti.

- [Crea un Cloud Connector \(Console di gestione AWS\)](#)
- [Prerequisiti](#)
- [Fase 1: Creare un AWS Config connettore](#)
- [Fase 2: Creazione di un Systems Manager Cloud Connector](#)
- [Gestisci i connettori cloud](#)
- [Abilita l'onboarding delle VM](#)
- [Ruoli IAM creati dalla console di Systems Manager](#)

- [Tag applicati alle istanze gestite](#)
- [In che modo Systems Manager gestisce le risorse cloud](#)

Le VM di Azure integrate tramite Cloud Connector si comportano come istanze gestite standard di Systems Manager attivate in modo ibrido. Puoi usare gli stessi strumenti e flussi di lavoro, come Run Command, Patch Manager e State Manager, per gestirli insieme ai tuoi nodi locali e EC2.

La creazione di un Cloud Connector per Azure prevede due passaggi principali:

1. Crea un AWS Config connettore, che imposta lo scambio di credenziali tra AWS e Azure e consente di registrare lo stato delle risorse AWS Config di Azure.
2. Crea un Systems Manager Cloud Connector, che registri il tenant di Azure e gli obiettivi di sottoscrizione con Systems Manager.

È possibile creare un Cloud Connector in due modi. Ti consigliamo di utilizzare Console di gestione AWS (la procedura guidata genera uno script di installazione che configura il lato Azure per te). Puoi anche usare AWS CLI, dove esegui tu stesso i comandi di configurazione di Azure e i comandi di creazione.

Note

- I Cloud Connectors supportano Microsoft Azure al momento del lancio. Il supporto di Google Cloud Platform è previsto per una versione futura.
- Systems Manager supporta fino a 10 Cloud Connector per Account AWS. Ogni Cloud Connector supporta fino a 75 destinazioni di sottoscrizione di Azure. Tutti i Cloud Connector in un singolo cloud Account AWS devono essere indirizzati allo stesso tenant di Azure.

Per informazioni dettagliate sui ruoli IAM che Systems Manager crea per tuo conto durante la procedura guidata di configurazione del connettore, incluse le relative politiche di attendibilità e autorizzazioni, consulta. [Ruoli IAM creati dalla console di Systems Manager](#)

Crea un Cloud Connector (Console di gestione AWS)

Ti consigliamo di utilizzare il Console di gestione AWS per creare un Cloud Connector. La procedura guidata della console raccoglie i dettagli del tenant e della sottoscrizione di Azure, quindi genera

uno script di configurazione che configura il lato Azure per te. Lo script generato crea o riutilizza le registrazioni delle applicazioni Microsoft Entra ID e i principi di servizio. Inoltre, configura le credenziali federate OIDC, assegna i ruoli di Azure con privilegi minimi e crea le risorse e le impostazioni diagnostiche dell'Event Hub per lo streaming del registro delle attività.

Poiché la procedura guidata genera questo script, non è necessario eseguire i singoli comandi all'interno dell'utente. az [Prerequisiti di Azure](#) Questi passaggi manuali si applicano solo al AWS CLI percorso.

Prima di iniziare, completa il prerequisito AWS unilaterale: devi abilitare la federazione delle identità web in uscita in IAM. Per istruzioni, consulta l'argomento [AWS prerequisiti](#).

Per creare un Cloud Connector per Azure nella console

1. Aprire la console Systems Manager. Nel riquadro di navigazione, scegli i nodi ibridi e multicloud. Questa pagina mostra i connettori Cloud e le attivazioni ibride esistenti in schede separate.
2. Scegli i nodi ibridi integrati.
3. Per il metodo di onboarding, scegli Azure Cloud Connector, quindi scegli Configura con script. Questo metodo utilizza la federazione basata su script con Microsoft Entra ID. Lo consigliamo per la gestione di macchine virtuali di Azure su larga scala.
4. Nella pagina Create Cloud Connector, fornisci i seguenti dettagli:

Nome del connettore

Inserisci un nome per il Cloud Connector.

Descrizione

(Facoltativo) Inserisci una descrizione per Cloud Connector.

Ruolo federativo di Azure

Scegli il ruolo di servizio creato automaticamente consigliato o scegli un ruolo esistente che fornisci. Per informazioni dettagliate sui ruoli creati dalla console, consulta [Ruoli IAM creati dalla console di Systems Manager](#).

ID del tenant

Inserisci l'UUID del tenant del tuo ID Microsoft Entra.

Nome del tenant

(Facoltativo) Inserisci un nome descrittivo per l'inquilino.

Sottoscrizioni Azure

Scegli se selezionare l'intero tenant (consigliato) o selezionare sottoscrizioni specifiche. Un Cloud Connector supporta fino a 75 obiettivi di sottoscrizione di Azure.

ID della sottoscrizione di hosting

Inserisci la sottoscrizione di Azure in cui vengono create le risorse dell'Event Hub per lo streaming del registro delle attività.

Note

Puoi verificare i dettagli del tenant e della sottoscrizione nel portale di Azure. Inserisci l'ID tenant e gli ID della sottoscrizione di Azure nel modulo. Console di gestione AWS

5. Se hai scelto di selezionare sottoscrizioni specifiche, inserisci gli ID delle sottoscrizioni, uno per riga o separati da virgole. Il modulo convalida il formato UUID e mostra un errore per qualsiasi immissione non valida. L'ID dell'abbonamento all'hosting si compila automaticamente.
6. Controlla le impostazioni del AWS Config connettore e dell'Event Hub. Se il modulo rileva un AWS Config connettore esistente per il tenant, mostra un banner informativo. I seguenti campi sono facoltativi:

Connettore di configurazione ARN

Auto-populates se viene rilevato un AWS Config connettore esistente. Lascia vuoto questo campo per far sì che il connettore venga creato automaticamente.

Namespace Event Hub

L'impostazione predefinita è `awsconfig-{accountId}-{region}`.

Nome dell'Event Hub

L'impostazione predefinita è `activitylog`.

7. La console genera uno script bash con i tuoi valori incorporati. Scegli **Copia** per copiare lo script. Lo script viene eseguito nella procedura seguente.

Lo script generato esegue la Azure-side configurazione al posto tuo. Eseguilo una volta, come descritto nella procedura seguente, quindi torna alla console per completare la creazione del connettore.

Per eseguire lo script di configurazione generato

1. Apri Azure Cloud Shell o qualsiasi terminale su cui è installata l'interfaccia della riga di comando di Azure ed esegui lo script che hai copiato.
2. Quando lo script viene eseguito, si apre una finestra del browser per l'autenticazione di Azure. Accedi ad Azure. Dopo l'accesso, lo script conferma che hai effettuato l'accesso a Microsoft Azure e continua.
3. Lo script viene eseguito fino al completamento. Durante l'esecuzione, esegue le seguenti operazioni nel tenant di Azure:
 - Si autentica nel tenant e seleziona la sottoscrizione configurata.
 - Crea la registrazione dell'applicazione AWS Config Microsoft Entra ID e l'entità del servizio.
 - Crea lo spazio dei nomi Event Hub e l'activitylogEvent Hub, contrassegna lo spazio dei nomi per il AWS Config rilevamento, assegna all' AWS Config applicazione il ruolo di ricevitore dati di Event Hub e configura le impostazioni di diagnostica del registro delle attività per lo streaming all'Event Hub.
 - Crea l'applicazione Microsoft Entra ID e l'entità del servizio Systems Manager, configura la credenziale federata OIDC e crea e assegna un ruolo personalizzato con privilegi minimi nell'ambito dell'abbonamento.

Al termine, lo script emette l'ID dell'app SSM e l'ID dell'app di configurazione.

4. Copia i valori SSM App ID e Config App ID dall'output dello script.
5. Torna alla sezione Azure Resource ID Console di gestione AWS e inserisci i valori copiati.
6. Scegli Create connector (Crea connettore). Quando si sceglie Create connector, la console crea il ruolo di federazione IAM, registra il AWS Config connettore e registra il Systems Manager Cloud Connector.

Dopo che il connettore è stato creato correttamente, la pagina Installa e configura SSM Agent viene visualizzata con un banner di successo. In questa pagina, abilita la gestione dei nodi: selezioni le regioni di Azure per gestire e configurare i tre ruoli IAM creati da Systems Manager. Per istruzioni, consulta l'argomento [Abilita l'onboarding della VM \(Console di gestione AWS\)](#). Per dettagli sui tre ruoli IAM creati dalla console, consulta [Ruoli IAM creati dalla console di Systems Manager](#).

La pagina dei dettagli del connettore mostra quanto segue:

- Una panoramica del connettore (nome, ID, provider e ID tenant).

- Controlli di convalida automatici con indicatori di esito positivo o negativo per federazione, autorizzazioni e connettività.
- Gli abbonamenti inclusi con il relativo stato di gestione.
- Tag modificabili.
- Azioni come Modifica dettagli, Modifica sottoscrizioni con script , Elimina e Test connector.

Il nuovo connettore viene visualizzato nella scheda Connettori cloud della pagina dei nodi ibridi e multicloud. Da questa pagina, puoi creare più connettori, modificare o eliminare un connettore esistente o passare alla scheda Attivazioni ibride.

Prerequisiti

Prima di creare un Cloud Connector, completa i seguenti prerequisiti sia sul lato laterale che sul AWS lato Azure. Questi passaggi stabiliscono l'autenticazione OIDC-based federata tra Microsoft Azure AWS e Microsoft Azure.

Note

I prerequisiti manuali di Azure si [Prerequisiti di Azure](#) applicano solo al percorso. AWS CLI Se crei un Cloud Connector in Console di gestione AWS, la procedura guidata genera uno script di configurazione che esegue questa Azure-side configurazione per te. Per ulteriori informazioni, consulta [Crea un Cloud Connector \(Console di gestione AWS\)](#).

Important

Assicurati che non Account AWS sia inclusa alcuna politica di controllo del servizio (SCP) che limiti l'azione. `sts:GetWebIdentityToken`

Argomenti

- [AWS prerequisiti](#)
- [Prerequisiti di Azure](#)

AWS prerequisiti

Completa i seguenti passaggi nel tuo Account AWS.

Per configurare il AWS lato della federazione

1. Abilita la federazione delle identità web in uscita

Abilita la federazione delle identità web in uscita nelle impostazioni Account AWS IAM. Ciò consente di AWS emettere token OIDC che Azure può verificare.

Nella console IAM, vai alle impostazioni dell'account e abilita la federazione delle identità web in uscita. In alternativa, usa: AWS CLI

```
aws iam enable-outbound-web-identity-federation
```

2. Annota l'URL dell'emittente OIDC

Dopo aver abilitato la federazione delle identità web in uscita, annota l'URL dell'emittente AWS OIDC del tuo account. L'URL ha il seguente formato:

```
https://UNIQUE_ID.tokens.sts.global.api.aws
```

Questo URL è necessario per configurare le credenziali di identità federate in Azure.

Prerequisiti di Azure

Completa i passaggi seguenti nel tuo ambiente Azure. Tra i AWS prerequisiti sono necessari i seguenti valori:

- URL dell'emittente: l'URL dell'emittente AWS OIDC della sezione precedente.
- Oggetto: l'ARN del ruolo federativo di Systems Manager Azure, ad esempio:
`arn:aws:iam::ACCOUNT_ID:role/service-role/SSM-AzureRole-connector-name`

Per configurare il lato Azure della federazione

1. Crea un'applicazione Azure Entra ID

Crea una registrazione dell'applicazione in Microsoft Entra ID (in precedenza Azure Active Directory). Annota l'ID dell'applicazione (client) nell'output.

```
az ad app create --display-name "AWSSMAzureIntegration" --query appId
```

2. Crea un'entità di servizio per l'applicazione

Creare un service principal associato all'applicazione. L'output del comando include un `id` campo, che è l'ID oggetto dell'entità del servizio. Nota questo valore `id` (ID oggetto). È **SERVICE_PRINCIPAL_ID** quello che utilizzerai `--assignee` in seguito come fase di assegnazione dei ruoli (Fase 5).

```
az ad sp create --id APPLICATION_ID
```

3. Aggiungi una credenziale di identità federata

Aggiungi una credenziale di identità federata all'applicazione che considera attendibile l'emittente OIDC. AWS Ciò consente ad Azure di accettare i token emessi da AWS per conto del ruolo federativo di Systems Manager Azure (vedi). [Ruolo di federazione di Azure](#)

```
az ad app federated-credential create \
  --id APPLICATION_ID \
  --parameters "{
    \"name\": \"aws-ssm-federation\",
    \"issuer\": \"AWS_OIDC_ISSUER_URL\",
    \"subject\": \"arn:aws:iam::ACCOUNT_ID:role/service-role/SSM-
AzureRole-CONNECTOR_NAME\",
    \"audiences\": [\"api://AzureADTokenExchange\"]
  }"
```

Sostituire:

- **APPLICATION_ID**— L'ID dell'applicazione (client) del passaggio 1.
- **AWS_OIDC_ISSUER_URL**— L'URL dell'emittente AWS OIDC (ad esempio,). `https://a1667813-695b-5415-b0f7-d473d62bb123.tokens.sts.global.api.aws`
- **ACCOUNT_ID**— Il tuo ID. Account AWS

- **CONNECTOR_NAME**— Il componente del nome del ruolo federativo di Systems Manager Azure. Nel percorso AWS CLI o API, crei tu stesso questo ruolo prima di creare Cloud Connector, quindi scegli il nome. A tale subject scopo, utilizza lo stesso ruolo ARN utilizzato `--role-arn` nella [Fase 2: Creazione di un Systems Manager Cloud Connector](#) fase. Per le politiche di fiducia e autorizzazioni del ruolo, consulta. [Ruolo di federazione di Azure](#)

4. Crea il ruolo personalizzato VM Run Command

Crea un ruolo personalizzato che conceda le autorizzazioni minime richieste a Systems Manager per eseguire comandi sulle macchine virtuali di Azure. Sostituiscilo **SUBSCRIPTION_ID** con l'ID della sottoscrizione di Azure che desideri gestire.

```
az role definition create --role-definition '{
  "Name": "AWSSSMVMExtensionRole-SUBSCRIPTION_ID",
  "Description": "Allows AWS Systems Manager to run commands on Azure VMs",
  "Actions": [
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/runCommand/action",
    "Microsoft.Compute/virtualMachines/runCommands/*"
  ],
  "AssignableScopes": [
    "/subscriptions/SUBSCRIPTION_ID"
  ]
}'
```

Per l'ambito a livello di tenant (tutte le sottoscrizioni del tenant), usa invece un ambito di gruppo di gestione:

```
az role definition create --role-definition '{
  "Name": "AWSSSMVMExtensionRole-TENANT_ID",
  "Description": "Allows AWS Systems Manager to run commands on Azure VMs",
  "Actions": [
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/runCommand/action",
    "Microsoft.Compute/virtualMachines/runCommands/*"
  ],
  "AssignableScopes": [
    "/providers/Microsoft.Management/managementGroups/TENANT_ID"
  ]
}'
```

Per verificare che il ruolo sia stato creato:

```
az role definition list --name "AWSSSMVMEExtensionRole-SUBSCRIPTION_ID" --output table
```

5. Assegna il ruolo VM Run Command al responsabile del servizio

Assegna il ruolo personalizzato all'entità del servizio che hai creato nel passaggio 2. L'ambito determina quali risorse di Azure Systems Manager può gestire.

Per l'ambito a livello di sottoscrizione (ripetere per ogni sottoscrizione):

```
az role assignment create \  
  --assignee SERVICE_PRINCIPAL_ID \  
  --role "AWSSSMVMEExtensionRole-SUBSCRIPTION_ID" \  
  --scope "/subscriptions/SUBSCRIPTION_ID"
```

Per l'ambito a livello di gruppo di gestione:

```
az role assignment create \  
  --assignee SERVICE_PRINCIPAL_ID \  
  --role "AWSSSMVMEExtensionRole-TENANT_ID" \  
  --scope "/providers/Microsoft.Management/managementGroups/TENANT_ID"
```

6. Crea un'applicazione Azure Entra ID per AWS Config

Crea una registrazione dell'applicazione separata AWS Config da utilizzare durante la registrazione dello stato delle risorse di Azure. Annota l'ID dell'applicazione (client) nell'output.

```
az ad app create \  
  --display-name "AWSConfigAzureIntegration-ACCOUNT_ID-TENANT_ID_PREFIX" \  
  --query appId
```

Sostituire:

- *ACCOUNT_ID*— Il tuo Account AWS ID.
- *TENANT_ID_PREFIX*— I personaggi principali del tuo ID tenant di Azure. Questo prefisso esiste solo per rendere univoco il nome visualizzato dell'applicazione. È possibile utilizzare qualsiasi parte breve e riconoscibile dell'ID del tenant.

Crea un'entità di servizio per l'applicazione. AWS Config `CONFIG_APPLICATION_ID` È il appId valore restituito dal `az ad app create` comando precedente in questo passaggio.

```
az ad sp create --id CONFIG_APPLICATION_ID
```

L'`az ad sp create` output include un campo `id` (ID oggetto), che è il `CONFIG_SERVICE_PRINCIPAL_ID` valore utilizzato nelle fasi successive Reader-role e di assegnazione dei ruoli di Event Hub.

7. Aggiungi una credenziale di identità federata per AWS Config

Aggiungi una credenziale di identità federata all'applicazione. AWS Config L'oggetto è il ruolo ARN AWS Config collegato al servizio (creato automaticamente quando si crea il connettore Config in una fase successiva).

```
az ad app federated-credential create \
  --id CONFIG_APPLICATION_ID \
  --parameters "{
    \"name\": \"aws-config-federation\",
    \"issuer\": \"AWS_OIDC_ISSUER_URL\",
    \"subject\": \"arn:aws:iam:ACCOUNT_ID:role/aws-service-role/
thirdparty.config.amazonaws.com/AWSServiceRoleForConfigThirdParty\",
    \"audiences\": [\"api://AzureADTokenExchange\"]
  }"
```

8. Assegna il ruolo Reader al AWS Config responsabile del servizio

Assegna il ruolo Reader integrato di Azure al responsabile del AWS Config servizio a livello di tenant (gruppo di gestione). Ciò consente di scoprire AWS Config le risorse di Azure.

```
az role assignment create \
  --assignee CONFIG_SERVICE_PRINCIPAL_ID \
  --role "acdd72a7-3385-48ef-bd42-f606fba81ae7" \
  --scope "/providers/Microsoft.Management/managementGroups/TENANT_ID"
```

9. Crea un Event Hub per lo streaming di Azure Activity Log

AWS Config utilizza un Azure Event Hub per ricevere eventi di Activity Log che indicano le modifiche alle risorse. Crea uno spazio dei nomi, un hub e un gruppo di consumatori di Event Hub in una delle tue sottoscrizioni di Azure.

```
# Create a resource group for the Event Hub
az group create \
  --subscription "HOSTING_SUBSCRIPTION_ID" \
  --name "AWSConfigAzureResources" \
  --location eastus

# Create an Event Hub namespace with a discovery tag
az eventhubs namespace create \
  --subscription "HOSTING_SUBSCRIPTION_ID" \
  --resource-group "AWSConfigAzureResources" \
  --name "EVENT_HUB_NAMESPACE" \
  --location eastus \
  --sku Standard \
  --tags "AWSConfig-ACCOUNT_ID-AWS_REGION=activitylog"

# Create the Event Hub
az eventhubs eventhub create \
  --subscription "HOSTING_SUBSCRIPTION_ID" \
  --resource-group "AWSConfigAzureResources" \
  --namespace-name "EVENT_HUB_NAMESPACE" \
  --name "activitylog" \
  --partition-count 4

# Create the consumer group for AWS Config
az eventhubs eventhub consumer-group create \
  --subscription "HOSTING_SUBSCRIPTION_ID" \
  --resource-group "AWSConfigAzureResources" \
  --namespace-name "EVENT_HUB_NAMESPACE" \
  --eventhub-name "activitylog" \
  --name "AWSConfig"
```

Sostituiscilo *EVENT_HUB_NAMESPACE* con un nome univoco globale (ad esempio *awsconfig-ACCOUNT_ID-REGION*) e *HOSTING_SUBSCRIPTION_ID* con la sottoscrizione di Azure che ospiterà le risorse di Event Hub.

10. Assegna il ruolo di ricevitore dati di Event Hub a AWS Config responsabile del servizio

Consenti al responsabile del AWS Config servizio di leggere dall'Event Hub:

```
EVENT_HUB_ID=$(az eventhubs eventhub show \
  --subscription "HOSTING_SUBSCRIPTION_ID" \
  --resource-group "AWSConfigAzureResources" \
```

```
--namespace-name "EVENT_HUB_NAMESPACE" \
--name "activitylog" \
--query id \
-o tsv)

az role assignment create \
  --assignee CONFIG_SERVICE_PRINCIPAL_ID \
  --role "a638d3c7-ab3a-418d-83e6-5f17a39d4fde" \
  --scope "$EVENT_HUB_ID"
```

11. Configurare l'esportazione del registro delle attività nell'Event Hub

Per ogni sottoscrizione di Azure che desideri AWS Config monitorare, crea un'impostazione diagnostica che esporti gli eventi del registro delle attività nell'Event Hub:

```
az provider register \
  --namespace Microsoft.Insights \
  --subscription "SUBSCRIPTION_ID"

az rest --method PUT \
  --url "https://management.azure.com/subscriptions/SUBSCRIPTION_ID/providers/
Microsoft.Insights/diagnosticSettings/EVENT_HUB_NAMESPACE?api-version=2021-05-01-
preview" \
  --body "{
    \"properties\": {
      \"eventHubAuthorizationRuleId\": \"\"/
subscriptions/HOSTING_SUBSCRIPTION_ID/resourceGroups/AWSConfigAzureResources/
providers/Microsoft.EventHub/namespaces/EVENT_HUB_NAMESPACE/authorizationRules/
RootManageSharedAccessKey\",
      \"eventHubName\": \"activitylog\",
      \"logs\": [{\"category\": \"Administrative\", \"enabled\": true}]
    }
  }"
```

Ripeti questo passaggio per ogni sottoscrizione che desideri monitorare.

Dopo aver completato la configurazione di Azure, prendi nota dei seguenti valori. Ti servono quando crei il Cloud Connector:

- ID tenant: l'ID della tua directory (tenant) di Azure AD.

- ID applicazione SSM (client): l'ID dell'applicazione dell'app Systems Manager Azure AD (passaggio 1).
- ID applicazione (client) di configurazione: l'ID dell'applicazione dell'app AWS Config Azure AD (passaggio 6).
- ID di sottoscrizione: le sottoscrizioni di Azure che desideri gestire.
- Nome host dello spazio dei nomi Event Hub: il nome host completo dello spazio dei nomi Event Hub (ad esempio,). `EVENT_HUB_NAMESPACE.servicebus.windows.net`

Fase 1: Creare un AWS Config connettore

Il AWS Config connettore imposta lo scambio di credenziali tra AWS e Azure e consente di registrare lo stato delle AWS Config risorse di Azure. È necessario crearlo prima di creare Systems Manager Cloud Connector.

Note

Il AWS Config connettore crea automaticamente un ruolo collegato al servizio per la federazione. Non è necessario creare un ruolo IAM separato per questo passaggio.

Per creare un AWS Config connettore per Azure

1. Crea il AWS Config connettore. Sostituiscilo `TENANT_ID` con il tuo ID tenant di Azure e `CLIENT_ID` con l'ID dell'applicazione di configurazione (client), l'ID dell'applicazione (client) dell'app AWS Config Azure AD che hai annotato nei prerequisiti di Azure (passaggio 6).

```
aws configservice put-connector \  
  --connector-configuration '{  
    "azure": {  
      "tenantIdentifier": "TENANT_ID",  
      "clientIdentifier": "CLIENT_ID"  
    }  
  }'
```

Annota l'informazione `Arn` contenuta nella risposta: ti servirà nel passaggio successivo.

2. Conferma che il connettore è stato creato:

```
aws configservice list-connectors
```

Fase 2: Creazione di un Systems Manager Cloud Connector

Dopo aver configurato il AWS Config connettore, crea Systems Manager Cloud Connector. Systems Manager Cloud Connector archivia la configurazione del tenant e della sottoscrizione di Azure e la collega al AWS Config connettore.

Per creare un Systems Manager Cloud Connector

1. Eseguire il seguente comando seguente. Sostituisci i valori segnaposto con l'ID del tenant di Azure, l'ID dell'applicazione Systems Manager (client), gli ID delle sottoscrizioni, l'ARN del ruolo federativo di Systems Manager Azure e l'ARN del connettore del AWS Config passaggio 1.

 Crea il ruolo federativo prima di eseguire questo comando

Prima di eseguire questo comando, il ruolo federativo di Systems Manager Azure che `--role-arn` identifica deve già esistere. La sua politica di fiducia deve inoltre consentire al responsabile del servizio Systems Manager (`ssm.amazonaws.com`) di assumerla. L'API AWS CLI and non crea questo ruolo per te. Se uno dei due requisiti non viene soddisfatto, il comando ha esito negativo. Il messaggio di errore è `ValidationException: Nonexistent role or missing ssm service principal in trust policy`. Crea prima il ruolo inserendo i criteri di fiducia e autorizzazioni. [Ruolo di federazione di Azure](#) Usa lo stesso nome di ruolo e lo stesso ARN che hai usato per l'oggetto della credenziale di identità federata in. [Prerequisiti di Azure](#)

```
aws ssm create-cloud-connector \
  --display-name "MyAzureConnector" \
  --configuration '{
    "AzureConfiguration": {
      "TenantId": "TENANT_ID",
      "ApplicationId": "SSM_APP_CLIENT_ID",
      "Targets": {
        "Subscriptions": [
          {"Id": "SUBSCRIPTION_ID"}
        ]
      }
    }
  }
```

```

    ]
  }
}
}' \
--role-arn "arn:aws:iam::ACCOUNT_ID:role/service-role/SSM-
AzureRole-CONNECTOR_NAME" \
--config-connector-arn CONFIG_CONNECTOR_ARN

```

Per indirizzare tutti gli abbonamenti nel tenant (configurazione a livello di tenant), ometti il campo dalla configurazione. Targets

La risposta restituisce il CloudConnectorId. Nota questo valore per le operazioni future.

2. Verifica che il Cloud Connector sia stato creato correttamente:

```

aws ssm get-cloud-connector \
--cloud-connector-id CLOUD_CONNECTOR_ID

```

Gestisci i connettori cloud

Usa i seguenti AWS CLI comandi per gestire i tuoi Cloud Connector.

Elenca tutti i Cloud Connector

```

aws ssm list-cloud-connectors \
--region us-east-1

```

Aggiorna un Cloud Connector

È possibile aggiornare il nome visualizzato o gli obiettivi di abbonamento di un Cloud Connector esistente.

```

aws ssm update-cloud-connector \
--cloud-connector-id CLOUD_CONNECTOR_ID \
--display-name "UpdatedName" \
--region us-east-1

```

Eliminare un Cloud Connector

L'eliminazione dell'ultimo Cloud Connector in un comporta Account AWS anche l'eliminazione del registratore collegato al AWS Config servizio associato.

```
aws ssm delete-cloud-connector \  
  --cloud-connector-id CLOUD_CONNECTOR_ID \  
  --region us-east-1
```

Abilita l'onboarding delle VM

Dopo aver creato un Cloud Connector, devi abilitare l'onboarding delle VM in modo che Systems Manager possa scoprire e registrare le VM di Azure destinate al connettore. L'attivazione dell'onboarding delle VM crea un'associazione denominata `AWSSMAzureConnector-CONNECTOR_ID` che utilizza il documento di automazione `AWS-InstallSSMAgentOnAzure`. L'associazione si rivolge alle VM tramite Cloud Connector.

Systems Manager integra le macchine virtuali di Azure tramite un processo basato sugli eventi. Quando viene creata una nuova macchina virtuale in Azure, il AWS Config connettore riceve l'evento di modifica tramite Azure Event Hub e lo inoltra a Systems Manager. L'associazione invia quindi un'esecuzione di automazione per l'onboard della macchina virtuale appena scoperta.

L'associazione opera inoltre con un programma periodico di 48 ore come rete di sicurezza. Ciò garantisce che tutte le VM mancate a causa di eventi di perdita o guasti transitori vengano infine scoperte e integrate.

Per ogni macchina virtuale di Azure da integrare, l'automazione esegue i seguenti passaggi:

1. Crea un'attivazione ibrida di Systems Manager per la macchina virtuale.
2. Installa l'agente SSM sulla macchina virtuale utilizzando un'estensione della macchina virtuale di Azure.
3. Registra la macchina virtuale come istanza gestita in Systems Manager utilizzando le credenziali di attivazione ibride.
4. Contrassegna l'istanza gestita con il `CloudConnector` tag (vedi). [Tag applicati alle istanze gestite](#)
5. Elimina l'attivazione ibrida, che non è più necessaria una volta completata la registrazione.

L'onboarding delle VM richiede due ruoli IAM. Il ruolo di invio dell'automazione viene assunto dall'avvio del flusso State Manager di lavoro di automazione. Il ruolo di assunzione dell'automazione viene utilizzato dal flusso di lavoro per creare attivazioni ed autenticarsi con Azure. Se abiliti l'onboarding tramite Console di gestione AWS, Systems Manager può creare questi ruoli

automaticamente. Per dettagli sulle politiche e le autorizzazioni di fiducia richieste, vedere. [Ruoli IAM creati dalla console di Systems Manager](#)

Abilita l'onboarding della VM (Console di gestione AWS)

Per abilitare l'onboarding delle VM in: Console di gestione AWS

1. Apri la console di Systems Manager e accedi a Hybrid Cloud.
2. Scegli il Cloud Connector per il quale desideri abilitare l'onboarding delle VM.
3. Scegli Installa e configura SSM Agent.
4. Configura le impostazioni seguenti:

Selezione della regione di Azure

Scegli se abilitare tutte le regioni di Azure (consigliato) o selezionare le regioni specifiche in cui si trovano le tue macchine virtuali.

Ruolo di associazione State Manager (ruolo di invio dell'automazione)

Il ruolo IAM che State Manager assume per inviare le esecuzioni di automazione. Questo ruolo passa il ruolo di esecuzione dell'automazione ad Automation all'avvio del flusso di lavoro di onboarding. Per la politica di fiducia e le autorizzazioni richieste da questo ruolo, consulta. [Ruolo di invio dell'automazione](#)

Ruolo di esecuzione dell'automazione (l'automazione assume il ruolo)

Il ruolo IAM che Automation assume per eseguire il runbook di installazione dell'agente. Questo ruolo assume il ruolo federativo di Azure per l'autenticazione con Azure tramite OIDC, crea attivazioni ibride e gestisce le istanze gestite. Per la politica di fiducia e le autorizzazioni richieste da questo ruolo, consulta. [Ruolo di assunzione dell'automazione](#)

Ruolo dell'istanza di attivazione ibrida

Il ruolo IAM assegnato alle macchine virtuali di Azure quando si registrano come istanze gestite. Questo ruolo deve essere affidabile `ssm.amazonaws.com` e avere la policy allegata `AmazonSSMManagedInstanceCore`. Per ulteriori informazioni, consulta [Ruolo dell'istanza gestita](#).

Tag VM

Facoltativamente, aggiungi tag che verranno applicati alle istanze gestite durante l'onboarding. Il `CloudConnector` tag viene applicato automaticamente (vedi). [Tag applicati](#)

[alle istanze gestite](#) Puoi aggiungere tag aggiuntivi per organizzare ulteriormente la tua flotta gestita.

5. Scegli Connetti.

Systems Manager crea l'associazione e inizia l'onboarding delle macchine virtuali di Azure. È possibile monitorare l'avanzamento nella pagina dei dettagli del connettore.

Abilita l'onboarding delle macchine virtuali (AWS CLI)

Per abilitare l'onboarding delle macchine virtuali utilizzando AWS CLI, crea un'associazione State Manager che abbia come target il Cloud Connector. Il comando richiede i seguenti ruoli:

- **AutomationAssumeRole**— Il ruolo di esecuzione dell'automazione che il runbook assume per creare attivazioni e autenticarsi con Azure. Per informazioni, consulta [Ruolo di assunzione dell'automazione](#).
- **ManagedInstanceIamRole**— Il ruolo dell'istanza di attivazione ibrida assegnato alle macchine virtuali quando si registrano come istanze gestite. Per informazioni, consulta [Ruolo dell'istanza gestita](#).
- **--association-dispatch-assume-role**— Il ruolo di State Manager invio che avvia l'automazione. Per informazioni, consulta [Ruolo di invio dell'automazione](#).

```
aws ssm create-association \
  --association-name "AWSSMAzureConnector-CLLOUD_CONNECTOR_ID" \
  --name "AWS-InstallSSMAgentOnAzure" \
  --automation-target-parameter-name "AzureVmResourceId" \
  --association-dispatch-assume-role "arn:aws:iam::ACCOUNT_ID:role/service-
role/DISPATCH_ROLE_NAME" \
  --parameters '{
    "AutomationAssumeRole": ["arn:aws:iam::ACCOUNT_ID:role/service-
role/ASSUME_ROLE_NAME"],
    "ManagedInstanceIamRole": ["service-role/
AmazonEC2RunCommandRoleForManagedInstances"],
    "CloudConnector": [CLLOUD_CONNECTOR_ID]
  }' \
  --targets 'Key=CloudConnector,Values=["{"CloudConnectorId\":"
\CLLOUD_CONNECTOR_ID\","SsmManagedNodeFilter\":"UNMANAGED\"}"]' \
  --schedule-expression "rate(48 hours)" \
  --max-concurrency "50"
```

Per indirizzare aree di Azure specifiche, aggiungi il `CloudProviderRegions` campo al valore `target`:

```
--targets 'Key=CloudConnector,Values=["{\"CloudConnectorId\":\"CLLOUD_CONNECTOR_ID\",
\"SsmManagedNodeFilter\":\"UNMANAGED\", \"CloudProviderRegions\":[\"eastus\",
\"westus2\"]}"]'
```

Per aggiungere tag personalizzati alle istanze gestite durante l'onboarding, includi il parametro: `ManagedInstanceTags`

```
--parameters '{
  "AutomationAssumeRole": ["arn:aws:iam::ACCOUNT_ID:role/service-
role/ASSUME_ROLE_NAME"],
  "ManagedInstanceIamRole": ["service-role/
AmazonEC2RunCommandRoleForManagedInstances"],
  "CloudConnector": [CLLOUD_CONNECTOR_ID],
  "ManagedInstanceTags": [{"\"Key\": \"Environment\", \"Value\": \"Production
\"}], [{"\"Key\": \"Team\", \"Value\": \"DevOps\"}]}'
```

Ruoli IAM creati dalla console di Systems Manager

Quando crei un Cloud Connector in Systems Manager Console di gestione AWS, Systems Manager crea e configura tre ruoli IAM per tuo Account AWS conto. Assegna inoltre un ruolo di istanza gestita alle macchine virtuali di Azure registrate tramite il connettore. I ruoli stabiliscono la catena di fiducia tra Systems Manager State Manager, Automation e Azure tramite la federazione OpenID Connect (OIDC). Questa catena di fiducia consente a Systems Manager di eseguire i runbook di Automation sulle tue macchine virtuali di Azure senza segreti di lunga durata.

Ogni nome di ruolo utilizza lo schema `SSM-AzureType-connector-name`, dove *connector-name* è il nome visualizzato che hai fornito (ripulito con caratteri alfanumerici, trattini e trattini bassi, quindi troncato per adattarsi al limite di 64 caratteri dei nomi di ruolo di IAM). Console di gestione AWS Aggiunge un suffisso univoco a ogni nome di ruolo per mantenerlo unico. I ruoli vengono creati nel percorso `/service-role/` IAM.

La console crea i ruoli nel seguente ordine:

1. Ruolo federativo di Azure, con una politica di fiducia che inizialmente nomina solo il principale del servizio Systems Manager come entità attendibile.

2. L'automazione assume il ruolo e il ruolo di invio dell'automazione.
3. La console aggiorna quindi la politica di fiducia del ruolo federativo di Azure per aggiungere il ruolo di assunzione dell'automazione e il ruolo di invio dell'automazione come responsabili attendibili. Dopo questo aggiornamento, la politica di fiducia è quella mostrata in [Ruolo di federazione di Azure](#)

Note

La console di Systems Manager crea questi ruoli solo durante la procedura guidata di configurazione di Cloud Connector. Se crei un Cloud Connector con AWS CLI (come descritto in [Fase 2: Creazione di un Systems Manager Cloud Connector](#)), devi creare i ruoli tu stesso. Le politiche di attendibilità e autorizzazioni in questa sezione mostrano il JSON che puoi utilizzare per ricrearle. Se ricreate i ruoli, effettuate le seguenti operazioni:

- Crea tutti e tre i ruoli (federazione di Azure, automation assume e automation dispatch) nel `/service-role/` percorso IAM. Le politiche di autorizzazione e la politica di fiducia del ruolo federativo di Azure fanno riferimento ai ruoli degli ARN che includono questo percorso.
- Contrassegna il ruolo di assunzione dell'automazione e il ruolo di invio dell'automazione con il tag principale. `caller=SSM` La politica di fiducia del ruolo federativo di Azure richiede questo tag.

Ruolo di federazione di Azure

Il ruolo federativo di Azure consente a Systems Manager di ottenere un token di identità Web da Servizio di token di sicurezza AWS (AWS STS) e di scambiarlo con credenziali di Azure tramite la federazione OIDC. L'automazione assume questo ruolo durante l'esecuzione del runbook per l'autenticazione nel tenant di Azure. Il servizio Systems Manager assume inoltre questo ruolo direttamente per convalidare il Cloud Connector prima che esista qualsiasi associazione. State Manager

Modello di nome del ruolo: `SSM-AzureRole-connector-name`

La politica di fiducia include due dichiarazioni:

- La prima dichiarazione consente al cliente di Account AWS assumere il ruolo, ma solo quando il principale chiamante è il ruolo di assunzione dell'automazione o il ruolo di invio dell'automazione

(corrispondente alla `aws:PrincipalArn` condizione) e tale principale è contrassegnato `concaller=SSM`. La corrispondenza tra principale e ARN richiede che il ruolo di `assuma` e il ruolo di `invio` siano inseriti nel percorso IAM. `/service-role/`

- La seconda dichiarazione consente al responsabile del servizio di Systems Manager di assumere direttamente il ruolo. Le `aws:SourceArn` condizioni `aws:SourceAccount` e forniscono una protezione in caso di confusione limitando la fiducia all'ARN di Cloud Connector Account AWS e a quello dell'ARN di Cloud Connector.

Sostituiscilo con il tuo ID. 123456789012 Account AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      },
      "Condition": {
        "StringEquals": {
          "aws:PrincipalTag/caller": "SSM"
        },
        "ArnLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::123456789012:role/service-role/SSM-
AzureAssumeRole*",
            "arn:aws:iam::123456789012:role/service-role/SSM-
AzureDispatchRole*"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Condition": {
        "StringEquals": {
```

```

        "aws:SourceAccount": "123456789012"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ssm:*:123456789012:cloud-connector/*"
      }
    }
  ]
}

```

La politica delle autorizzazioni consente al ruolo di ottenere un token di identità Web il cui pubblico è limitato a `api://AzureADTokenExchange`, ovvero il pubblico richiesto da Microsoft Entra ID per la federazione OIDC.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `sts:GetWebIdentityToken`— Consente al ruolo di ottenere un token di identità web da AWS STS presentare a Microsoft Entra ID per scambiare le credenziali di Azure.
- `sts:TagGetWebIdentityToken`— Consente a Systems Manager di aggiungere tag di identità (come l'ID del connettore) al token di identità web emesso. Ciò consente di applicare le regole di federazione dell'ID Microsoft Entra a uno specifico Cloud Connector.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sts:GetWebIdentityToken",
        "sts:TagGetWebIdentityToken"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "sts:IdentityTokenAudience": [
            "api://AzureADTokenExchange"
          ]
        }
      }
    }
  ]
}

```

```

    }
  ]
}
```

Ruolo di assunzione dell'automazione

Il ruolo assunto dall'automazione è il ruolo che assume l'automazione quando esegue il runbook che integra una macchina virtuale di Azure come nodo gestito. Il ruolo può richiamare le API principali di Systems Manager necessarie per l'attivazione ibrida. Può anche passare un ruolo di servizio a Systems Manager e assumere il ruolo di federazione di Azure per ottenere le credenziali di Azure.

Schema di denominazione del ruolo: SSM-AzureAssumeRole-*connector-name*

La politica di fiducia consente al responsabile del servizio di Systems Manager di assumere il ruolo, limitato al tuo Account AWS. Sostituisci 123456789012 con l'ID dell' Account AWS .

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        }
      }
    }
  ]
}
```

La politica delle autorizzazioni concede le azioni necessarie ad Automation per eseguire i runbook di onboarding. Sostituiscila 123456789012 con il tuo Account AWS ID, us-east-1 con Regione AWS quello in cui è stato creato Cloud Connector, SSM-AzureRole-MyConnector con il nome del ruolo federativo di Azure, AmazonEC2RunCommandRoleForManagedInstances con il nome del ruolo dell'istanza gestita collegato a Cloud Connector e connector-id con l'ID del Cloud Connector.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **ssm**— Consente ad Automation di creare, eliminare e descrivere le attivazioni ibride (`CreateActivation`, `DeleteActivation`, `DescribeActivations`); di registrare le macchine virtuali di Azure come nodi gestiti e leggerne lo stato (`DescribeInstanceInformation`); di etichettare le attivazioni e le istanze gestite (`AddTagsToResource`); di leggere il runbook di installazione (`GetDocumentativoAWS-InstallSSMAgentOnAzure`); e di leggere la configurazione di Cloud Connector (`GetCloudConnector`).
- **iam:PassRole**— Consente ad Automation di passare il ruolo di istanza gestita a Systems Manager durante la registrazione di una macchina virtuale di Azure. La `iam:PassedToService` condizione limita il passaggio a `ssm.amazonaws.com`
- **iam:ListRoleTags**— Consente ad Automation di leggere i tag sul ruolo federativo di Azure per confermare che appartiene allo stesso Cloud Connector prima di assumerlo.
- **sts:AssumeRole**— Consente ad Automation di assumere il ruolo federativo di Azure per ottenere le credenziali di Azure.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::123456789012:role/service-role/SSM-AzureRole-MyConnector"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/service-role/AmazonEC2RunCommandRoleForManagedInstances",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
```

```

        "ssm:CreateActivation",
        "ssm:DeleteActivation",
        "ssm:DescribeActivations",
        "ssm:DescribeInstanceInformation",
        "iam:ListRoleTags",
        "ssm:AddTagsToResource"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "ssm:GetDocument",
    "Resource": [
      "arn:aws:ssm:us-east-1:*:document/AWS-InstallSSMAgentOnAzure"
    ]
  },
  {
    "Effect": "Allow",
    "Action": "ssm:GetCloudConnector",
    "Resource": "arn:aws:ssm:us-east-1:123456789012:cloud-connector/connector-
id"
  }
]
}

```

Ruolo di invio dell'automazione

Il ruolo di invio dell'automazione è il ruolo State Manager utilizzato quando avvia un'esecuzione di automazione su un Cloud Connector. State Manager passa il ruolo di assunzione dell'automazione ad Automation attraverso questo ruolo. Il ruolo di dispatch assume anche direttamente il ruolo di federazione di Azure, quindi State Manager può determinare quali macchine virtuali di Azure corrispondono agli obiettivi di un Cloud Connector quando viene eseguita un'associazione.

Schema di denominazione del ruolo: SSM-AzureDispatchRole-*connector-name*

La politica di fiducia consente al responsabile del servizio di Systems Manager di assumere il ruolo, limitato al tuo Account AWS. Sostituisci 123456789012 con l'ID dell' Account AWS .

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",

```



```

        "Action": "sts:AssumeRole",
        "Principal": {
            "Service": "ssm.amazonaws.com"
        },
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "123456789012"
            }
        }
    }
}
]
}

```

La politica delle autorizzazioni garantisce le azioni State Manager necessarie per inviare le esecuzioni di automazione agli obiettivi di un Cloud Connector. Sostituisci `123456789012` con il tuo Account AWS ID, `us-east-1` con Regione AWS quello in cui è stato creato Cloud Connector, `SSM-AzureAssumeRole-MyConnector` con il nome del ruolo di assunzione dell'automazione, `SSM-AzureRole-MyConnector` con il nome del ruolo federativo di Azure e `connector-id` con l'ID di Cloud Connector.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `iam:PassRole`— Consente di State Manager passare il ruolo di assunzione dell'automazione ad Automation all'avvio di un'esecuzione di un runbook. La `iam:PassedToService` condizione limita il passaggio e lo limita alle `ssm.amazonaws.com` esecuzioni del `AWS-InstallSSMAgentOnAzure` runbook e dell'automazione nei connettori.
`iam:AssociatedResourceARN` Regione AWS
- `iam:ListRoleTags`— Consente di State Manager leggere i tag sui ruoli per confermare che appartengono allo stesso Cloud Connector prima di passarli o assumerli.
- `ssm:GetCloudConnector`— Consente di State Manager leggere la configurazione di Cloud Connector durante la risoluzione del target.
- `ssm:ListCloudConnectors`— Consente di State Manager enumerare Cloud Connectors durante la risoluzione degli obiettivi delle associazioni.
- `ssm:DescribeInstanceInformation`— Consente di State Manager leggere lo stato dei nodi gestiti registrati tramite il connettore per determinare quali obiettivi sono idonei.
- `ssm:StartAutomationExecution`— Consente di State Manager avviare un'esecuzione automatica del `AWS-InstallSSMAgentOnAzure` runbook rispetto agli obiettivi del connettore.

- **sts:AssumeRole**— Consente di State Manager assumere il ruolo di federazione di Azure in modo che possa autenticarsi su Azure durante la risoluzione degli obiettivi del connettore.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/service-role/SSM-
AzureAssumeRole-MyConnector",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "ssm.amazonaws.com"
        },
        "ArnLike": {
          "iam:AssociatedResourceARN": [
            "arn:aws:ssm:us-east-1:*:document/AWS-InstallSSMAgentOnAzure",
            "arn:aws:ssm:us-east-1:*:automation-definition/AWS-
InstallSSMAgentOnAzure:1",
            "arn:aws:ssm:us-east-1:123456789012:automation-execution/*"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ssm:GetCloudConnector",
      "Resource": "arn:aws:ssm:us-east-1:123456789012:cloud-connector/connector-
id"
    },
    {
      "Effect": "Allow",
      "Action": "ssm:StartAutomationExecution",
      "Resource": [
        "arn:aws:ssm:us-east-1:*:document/AWS-InstallSSMAgentOnAzure",
        "arn:aws:ssm:us-east-1:*:automation-definition/AWS-
InstallSSMAgentOnAzure:1",
        "arn:aws:ssm:us-east-1:123456789012:automation-execution/*"
      ]
    }
  ],
  {
```

```

        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": "arn:aws:iam::123456789012:role/service-role/SSM-AzureRole-MyConnector"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ssm:DescribeInstanceInformation",
            "ssm:ListCloudConnectors",
            "iam:ListRoleTags"
        ],
        "Resource": "*"
    }
]
}

```

Ruolo dell'istanza gestita

Il ruolo dell'istanza gestita è il ruolo IAM che viene SSM Agent assunto in ogni macchina virtuale di Azure dopo l'installazione e la registrazione. Il ruolo concede all'agente le autorizzazioni necessarie per chiamare il servizio Systems Manager dalla macchina virtuale. A differenza degli altri tre ruoli, questo non viene creato per conto dell'utente. Si seleziona un ruolo esistente durante la procedura guidata di configurazione del connettore o si lascia che sia la procedura guidata a creare il ruolo consigliato `AmazonEC2RunCommandRoleForManagedInstances` con la policy `AmazonSSMManagedInstanceCore` AWS gestita allegata.

Per informazioni sulla creazione di questo ruolo e sulle politiche che è possibile allegare ad esso, vedere. [Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud](#) Le attivazioni di Cloud Connector utilizzano lo stesso schema di ruolo delle attivazioni ibride.

Tutte le chiamate API effettuate da questi ruoli vengono registrate su AWS CloudTrail ()CloudTrail. Per informazioni sull'accesso a Systems Manager CloudTrail, vedere. [Registrazione dei log AWS Systems Manager Chiamate API con AWS CloudTrail](#)

Tag applicati alle istanze gestite

Quando Systems Manager esegue l'onboard di una macchina virtuale di Azure tramite un Cloud Connector, applica automaticamente il seguente tag all'istanza gestita risultante. Questo tag identifica

quale Cloud Connector è stato usato per integrare la macchina virtuale e può essere usato per filtrare, organizzare e applicare policy alle istanze gestite in base al connettore di origine.

Chiave tag	Valore di tag	Description
CloudConnector	L'ID Cloud Connector come GUID (ad esempio,) a1b2c3d4-5678-90ab-cdef-EXAMPLE11111	Identifica il Systems Manager Cloud Connector utilizzato per effettuare l'onboard della macchina virtuale di Azure come istanza gestita. Questo tag viene applicato automaticamente durante il processo di onboarding. È possibile utilizzare questo tag per filtrare le istanze gestite per connettore nella console di Systems Manager o per operazioni API che supportano il filtraggio basato su tag. AWS CLI

Ad esempio, per elencare tutte le istanze gestite registrate tramite uno specifico Cloud Connector, utilizzate il seguente comando: AWS CLI

```
aws ssm describe-instance-information \
  --filters "Key=tag:CloudConnector,Values=CLoudConnectorID"
```

In che modo Systems Manager gestisce le risorse cloud

Abilitando le integrazioni multicloud per AWS Systems Manager, gli identificatori delle macchine virtuali di altri provider cloud vengono archiviati in Systems Manager e in altri, se necessario. Servizi AWS Questi metadati si riferiscono alla gestione delle risorse corrispondenti raccolte da altri fornitori di servizi cloud. Tali identificatori non costituiscono i Contenuti dell'utente. Ti consigliamo di non includere in essi informazioni sensibili, riservate o di identificazione personale.

Abilitando le integrazioni multicloud, i seguenti identificatori dell'ambiente cloud connesso vengono archiviati e utilizzati per fornire funzionalità di sicurezza multicloud: AWS

- Identificatori di risorsa: ID tenant di Azure, ID sottoscrizione, posizione (area), ID risorsa (ID o nomi dei gruppi di risorse)

Gestione dei dispositivi edge con Systems Manager

Questa sezione descrive le attività di configurazione eseguite dagli amministratori di account e di sistema per abilitare la configurazione e la gestione dei dispositivi AWS IoT Greengrass principali. Dopo aver completato queste attività, gli utenti a cui sono state concesse le autorizzazioni dall'Account AWS amministratore possono utilizzare AWS Systems Manager per configurare e gestire i dispositivi AWS IoT Greengrass principali della propria organizzazione.

Note

- SSM Agent for AWS IoT Greengrass non è supportato su macOS e Windows 10. Non è possibile utilizzare gli strumenti di Systems Manager per gestire e configurare i dispositivi edge che utilizzano questi sistemi operativi.
- Systems Manager supporta anche i dispositivi edge che non sono configurati come dispositivi AWS IoT Greengrass principali. Per utilizzare Systems Manager per gestire i dispositivi AWS IoT Core e i dispositivi non AWS edge, è necessario configurarli utilizzando un'attivazione ibrida. Per ulteriori informazioni, consulta [Gestione dei nodi in ambienti ibridi e multicloud con Systems Manager](#).

Prima di iniziare

Verifica che i dispositivi Edge soddisfino i seguenti requisiti.

- I dispositivi periferici devono soddisfare i requisiti per essere configurati come dispositivi AWS IoT Greengrass principali. Per ulteriori informazioni, consulta [Configurazione dei dispositivi AWS IoT Greengrass principali](#) nella Guida per gli AWS IoT Greengrass Version 2 sviluppatori.
- I dispositivi edge devono essere compatibili con AWS Systems Manager Agent (SSM Agent). Per ulteriori informazioni, consulta [Sistemi operativi supportati per Systems Manager](#).
- I dispositivi Edge devono essere in grado di comunicare con il servizio Systems Manager nel cloud. Systems Manager non supporta dispositivi edge scollegati.

Informazioni sulla configurazione di dispositivi edge

La configurazione AWS IoT Greengrass dei dispositivi per Systems Manager prevede i seguenti processi.

 Note

Per informazioni sulla disinstallazione SSM Agent da un dispositivo edge, vedere [Disinstallare l' AWS Systems Manager agente](#) nella Guida per gli AWS IoT Greengrass Version 2 sviluppatori.

Creazione di un ruolo di servizio IAM per dispositivi edge

AWS IoT Greengrass i dispositivi principali richiedono un ruolo di servizio AWS Identity and Access Management (IAM) con cui comunicare AWS Systems Manager. Il ruolo concede Servizio di token di sicurezza AWS (AWS STS) la [AssumeRole](#) fiducia al servizio Systems Manager. È necessario creare il ruolo di servizio una sola volta per ogni Account AWS. Specificate questo ruolo per il `RegistrationRole` parametro quando configurate e distribuite il SSM Agent componente sui vostri AWS IoT Greengrass dispositivi. Se è già stato creato questo ruolo durante la configurazione di nodi non EC2 per un ambiente [ibrido e multicloud](#), è possibile ignorare questo passaggio.

 Note

È necessario fornire agli utenti dell'azienda o dell'organizzazione che usano Systems Manager sui tuoi dispositivi edge l'autorizzazione in IAM per richiamare l'API Systems Manager.

Requisito delle policy del bucket S3

Se uno dei seguenti casi è true, è necessario creare una policy di autorizzazione IAM personalizzata per i bucket Amazon Simple Storage Service (Amazon S3) prima di completare questa procedura:

- Caso 1: stai utilizzando un endpoint VPC per connettere privatamente il tuo VPC ai servizi di endpoint VPC supportati Servizi AWS e forniti da. AWS PrivateLink
- Caso 2: Prevedi di utilizzare un bucket S3 per archiviare l'output dei comandi o i log delle sessioni. Run Command Session Manager Prima di procedere, segui i passaggi descritti in [Creare una policy di bucket S3 personalizzata per un profilo dell'istanza](#). Le informazioni sulla policy del bucket S3 contenute in quell'argomento si applicano anche al tuo ruolo di servizio.

 Note

Se i tuoi dispositivi sono protetti da un firewall e prevedi di utilizzare Patch Manager, il firewall deve permettere l'accesso all'endpoint di baseline delle patch `arn:aws:s3:::patch-baseline-snapshot-region/*`. *region* rappresenta l'identificatore di una regione AWS supportata da AWS Systems Manager, ad esempio, `us-east-2` per la regione Stati Uniti orientali (Ohio). Per un elenco dei *region* valori supportati, vedere la colonna Regione negli endpoint [del servizio](#) Systems Manager in. Riferimenti generali di Amazon Web Services

AWS CLI

Per creare un ruolo del servizio IAM per un AWS IoT Greengrass ambiente (AWS CLI)

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Creare un file di testo con un nome, ad esempio `SSMService-Trust.json` con la seguente policy di attendibilità. Salvare il file con l'estensione `.json`.

 Note

Prendere nota del nome. Specificarlo quando esegui la distribuzione SSM Agent sui tuoi dispositivi AWS IoT Greengrass principali.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "Service": "ssm.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }
}
```

```
}  
}
```

3. Apri e AWS CLI, nella directory in cui hai creato il file JSON, esegui il [comando](#) `create-role` per creare il ruolo del servizio. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux e macOS

```
aws iam create-role \  
  --role-name SSMSERVICERole \  
  --assume-role-policy-document file://SSMSERVICE-Trust.json
```

Windows

```
aws iam create-role ^  
  --role-name SSMSERVICERole ^  
  --assume-role-policy-document file://SSMSERVICE-Trust.json
```

4. Usare [attach-role-policy](#) come segue per abilitare il ruolo di servizio appena creato per la creazione di un token di sessione. Il token della sessione fornisce ai tuoi dispositivi edge l'autorizzazione di eseguire comandi utilizzando Systems Manager.

Note

Le policy aggiunte per un profilo del servizio per i dispositivi edge sono le stesse policy utilizzate per la creazione di un profilo dell'istanza Amazon Elastic Compute Cloud (Amazon EC2). Per ulteriori informazioni sulle policy IAM utilizzate nei seguenti comandi, consulta [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#).

(Obbligatorio) Esegui il comando seguente per consentire a un dispositivo edge di utilizzare le funzionalità di base del AWS Systems Manager servizio.

Linux e macOS

```
aws iam attach-role-policy \  
  --role-name SSMSERVICERole \  
  --policy-name SSMSERVICEManagedPolicy
```



```
--policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

Windows

```
aws iam attach-role-policy ^  
  --role-name SSMSERVICE_ROLE ^  
  --policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

Se hai creato una policy bucket S3 personalizzata per il tuo ruolo di servizio, esegui il comando seguente per consentire ad AWS Systems Manager Agent (SSM Agent) di accedere ai bucket specificati nella policy. Sostituisci *account_ID* and *my_bucket_policy_name* con il tuo Account AWS ID e il nome del bucket.

Linux e macOS

```
aws iam attach-role-policy \  
  --role-name SSMSERVICE_ROLE \  
  --policy-arn arn:aws:iam::account_ID:policy/my_bucket_policy_name
```

Windows

```
aws iam attach-role-policy ^  
  --role-name SSMSERVICE_ROLE ^  
  --policy-arn arn:aws:iam::account_id:policy/my_bucket_policy_name
```

(Facoltativo) Esegui il comando seguente per permettere a SSM Agent di accedere a Directory Service per tuo conto per unirti al dominio da dispositivi edge. Il ruolo di servizio necessita di questa policy solo se i dispositivi Edge vengono aggiunti a una directory Microsoft AD.

Linux e macOS

```
aws iam attach-role-policy \  
  --role-name SSMSERVICE_ROLE \  
  --policy-arn arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess
```

Windows

```
aws iam attach-role-policy ^
```

```
--role-name SSMSERVICE_ROLE ^  
--policy-arn arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess
```

(Facoltativo) Esegui il comando seguente per consentire all' CloudWatch agente di funzionare sui tuoi dispositivi edge. Questo comando consente di leggere le informazioni su un dispositivo e di scriverle su CloudWatch. Il tuo ruolo di servizio richiede questa politica solo se utilizzi servizi come Amazon EventBridge o Amazon CloudWatch Logs.

```
aws iam attach-role-policy \  
  --role-name SSMSERVICE_ROLE \  
  --policy-arn arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
```

Tools for PowerShell

Per creare un ruolo di servizio IAM per un AWS IoT Greengrass ambiente (AWS Tools for Windows PowerShell)

1. Installa e configura AWS Strumenti per PowerShell (Strumenti per Windows PowerShell), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione di AWS Strumenti per PowerShell](#).

2. Creare un file di testo con un nome, ad esempio `SSMSERVICE-Trust.json` con la seguente policy di attendibilità. Salvare il file con l'estensione `.json`.

Note

Prendere nota del nome. Specificalo quando esegui la distribuzione SSM Agent sui tuoi dispositivi AWS IoT Greengrass principali.

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": {  
    "Effect": "Allow",  
    "Principal": {  
      "Service": "ssm.amazonaws.com"    }  
  }  
}
```

```
    },  
    "Action": "sts:AssumeRole"  
  }  
}
```

3. Apri PowerShell in modalità amministrativa e nella directory in cui hai creato il file JSON, esegui [New-IAMRole](#) quanto segue per creare un ruolo di servizio.

```
New-IAMRole `  
-RoleName SSMSERVICERole `  
-AssumeRolePolicyDocument (Get-Content -raw SSMSERVICE-Trust.json)
```

4. Usa [Register-IAMRolePolicy](#) quanto segue per consentire al ruolo di servizio che hai creato di creare un token di sessione. Il token della sessione fornisce ai tuoi dispositivi edge l'autorizzazione di eseguire comandi utilizzando Systems Manager.

Note

Le policy aggiunte per un ruolo di servizio per i dispositivi edge in un ambiente AWS IoT Greengrass sono le stesse policy utilizzate per la creazione di un profilo dell'istanza per le istanze EC2. Per ulteriori informazioni sulle AWS politiche utilizzate nei seguenti comandi, vedere [Configurazione delle autorizzazioni di istanza richieste per Systems Manager](#).

(Obbligatorio) Esegui il comando seguente per consentire a un dispositivo perimetrale di utilizzare le funzionalità AWS Systems Manager di base del servizio.

```
Register-IAMRolePolicy `  
-RoleName SSMSERVICERole `  
-PolicyArn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

Se è stata creata una policy di bucket S3 personalizzata per il ruolo di servizio, esegui il comando seguente per abilitare SSM Agent per l'accesso al bucket specificato nella policy. Sostituisci *account_ID* and *my_bucket_policy_name* con il tuo Account AWS ID e il nome del bucket.

```
Register-IAMRolePolicy `  
-RoleName SSMSERVICERole `  
-PolicyArn arn:aws:iam::account_ID:policy/my_bucket_policy_name
```

```
-PolicyArn arn:aws:iam::account_ID:policy/my_bucket_policy_name
```

(Facoltativo) Esegui il comando seguente per permettere a SSM Agent di accedere a Directory Service per tuo conto per unirti al dominio da dispositivi edge. Il ruolo di servizio necessita di questa policy solo se i dispositivi Edge vengono aggiunti a una directory Microsoft AD.

```
Register-IAMRolePolicy `
  -RoleName SSMSERVICERole `
  -PolicyArn arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess
```

(Facoltativo) Esegui il comando seguente per consentire all' CloudWatch agente di funzionare sui tuoi dispositivi edge. Questo comando consente di leggere le informazioni su un dispositivo e di scriverle su CloudWatch. Il tuo ruolo di servizio richiede questa politica solo se utilizzi servizi come Amazon EventBridge o Amazon CloudWatch Logs.

```
Register-IAMRolePolicy `
  -RoleName SSMSERVICERole `
  -PolicyArn arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
```

Configura i tuoi dispositivi edge per AWS IoT Greengrass

Configura i tuoi dispositivi edge come dispositivi AWS IoT Greengrass principali. Il processo di configurazione prevede la verifica dei sistemi operativi e dei requisiti di sistema supportati e l'installazione e la configurazione del software AWS IoT Greengrass Core sui dispositivi. Per ulteriori informazioni, consulta [Configurazione di altri dispositivi AWS IoT Greengrass](#) nella Guida per sviluppatori AWS IoT Greengrass Version 2 .

Aggiorna il AWS IoT Greengrass ruolo di scambio di token e installazione Agente SSM sui tuoi dispositivi periferici

Il passaggio finale richiede l'aggiornamento del ruolo del servizio del dispositivo AWS IoT Greengrass AWS Identity and Access Management (IAM) (il ruolo di scambio di token) e l'implementazione SSM Agent sui AWS IoT Greengrass dispositivi. Per informazioni, consulta [Install the AWS Systems Manager Agent](#) nella AWS IoT Greengrass Version 2 Developer Guide.

Dopo la distribuzione SSM Agent sui dispositivi, registra AWS IoT Greengrass automaticamente i dispositivi con Systems Manager. Non è necessaria alcuna registrazione aggiuntiva. È possibile iniziare a utilizzare gli strumenti di Systems Manager per accedere, gestire e configurare i AWS IoT Greengrass dispositivi.

Note

I dispositivi Edge devono essere in grado di comunicare con il servizio Systems Manager nel cloud. Systems Manager non supporta dispositivi edge scollegati.

Creare un AWS Organizations amministratore delegato per Systems Manager

Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

Quando si configura un'organizzazione in AWS Organizations, si assegna un account di gestione per eseguire tutte le attività amministrative per tutti Servizi AWS. L'utente dell'account di gestione può assegnare un account amministratore delegato solo a Systems Manager per eseguire attività amministrative per Change Manager Explorer, eOpsCenter. AWS Organizations è un servizio di gestione degli account che è possibile utilizzare per creare un'organizzazione e Account AWS assegnare la gestione centralizzata di questi account. Per informazioni su AWS Organizations, consulta [AWS Organizations](#) la Guida AWS Organizations per l'utente.

Change Manager Explorer, eOpsCenter, tools in AWS Systems Manager, consente di AWS Organizations eseguire attività su tutti gli account membri dell'organizzazione. È possibile assegnare un solo amministratore delegato per tutti gli strumenti di Systems Manager. È necessario che l'account di amministratore delegato sia un membro dell'organizzazione a cui è assegnato.

Argomenti

- [Utilizzando un amministratore delegato con Change Manager](#)

- [Usare un amministratore delegato con Explorer](#)
- [Utilizzando un amministratore delegato con OpsCenter](#)
- [Utilizzando un amministratore delegato con Configurazione rapida](#)

Utilizzando un amministratore delegato con Change Manager

Change Manager è un framework di gestione delle modifiche enterprise per la richiesta, l'approvazione, l'implementazione e la creazione di report sulle modifiche operative alla configurazione e all'infrastruttura delle applicazioni.

Se utilizzi Change Manager in un'organizzazione, assegna un account di amministratore delegato per gestire modelli di modifica, approvazioni e report per tutti gli account membri. Utilizzando Quick Setup, è possibile configurare Change Manager per l'utilizzo con un'organizzazione e selezionare l'account di amministratore delegato. Se si utilizza Change Manager con un singolo utente Account AWS, l'account amministratore delegato non è richiesto.

Per impostazione predefinita, Change Manager visualizza tutte le attività relative alle modifiche nell'account di amministratore delegato. Per istruzioni sulla configurazione di un amministratore delegato durante la configurazione di Change Manager per un'organizzazione, consulta [Configurazione Change Manager per un'organizzazione \(account di gestione\)](#).

Important

Se utilizzi Change Manager in un'organizzazione, si consiglia di apportare sempre modifiche dall'account amministratore delegato. Sebbene sia possibile apportare modifiche da altri account dell'organizzazione, tali modifiche non verranno segnalate o visualizzate dall'account amministratore delegato.

Usare un amministratore delegato con Explorer

Explorer è una dashboard operativa personalizzabile che riporta la visualizzazione aggregata dei dati operativi (OpsData) per te Account AWS, attraverso. Regioni AWS

È possibile configurare un account amministratore delegato per Systems Manager per aggregare Explorer i dati provenienti da più regioni e account utilizzando la sincronizzazione dei dati delle risorse con. AWS Organizations Un amministratore delegato può cercare, filtrare e aggregare

Explorer i dati utilizzando Console di gestione AWS, the AWS Command Line Interface (AWS CLI) o. AWS Tools for Windows PowerShell

Quando utilizzi un account di amministratore delegato per Explorer, limiti il numero di amministratori che possono creare o eliminare le sincronizzazioni dei dati delle risorse di più account e regioni a un solo Account AWS.

È possibile sincronizzare i dati operativi Account AWS in tutta l'organizzazione utilizzando.

Explorer Per informazioni su come assegnare un amministratore delegato da Explorer, consulta [Configurazione di un amministratore delegato per Explorer](#).

Utilizzando un amministratore delegato con OpsCenter

OpsCenter fornisce una posizione centrale in cui gli ingegneri operativi e i professionisti IT possono gestire gli elementi di lavoro operativi (OpsItems) relativi alle AWS risorse. Se desideri utilizzare OpsCenter per la gestione centralizzata di OpsItems su più account, devi configurare l'organizzazione in AWS Organizations.

Utilizzando Quick Setup per OpsCenter, è possibile assegnare un account di amministratore delegato e configurare OpsCenter per la gestione centralizzata di OpsItems. Per ulteriori informazioni, consulta [\(Facoltativo\) Configura OpsCenter da gestire OpsItems tra gli account utilizzando Configurazione rapida](#).

Utilizzando un amministratore delegato con Configurazione rapida

Quick Setup consente di configurare rapidamente i AWS servizi e le funzionalità utilizzati di frequente con le best practice consigliate. Puoi configurare un account amministratore delegato per aiutarti Quick Setup a distribuire e gestire le configurazioni tra account e regioni utilizzando. AWS Organizations Un amministratore delegato per Quick Setup crea, aggiorna, visualizza ed elimina le risorse del gestore della configurazione nell'organizzazione. Systems Manager registra un amministratore delegato per Quick Setup come parte del processo di configurazione per l'esperienza di console integrata. Per ulteriori informazioni, consulta [Configurazione della console unificata di Systems Manager per un'organizzazione](#).

Configurazione generale per AWS Systems Manager

Registrati per un Account AWS

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

Configurazione AWS Systems Manager

I seguenti argomenti descrivono come configurare la AWS Systems Manager console unificata per AWS Organizations organizzazioni e single Account AWS.

Configurare l'accesso alla console di Systems Manager

Per AWS Systems Manager utilizzarlo Console di gestione AWS, è necessario che siano configurate le autorizzazioni corrette.

Questa sezione contiene gli argomenti seguenti.

- [Configurazione della console unificata di Systems Manager per singolo account e singola Regione](#)

Per ulteriori informazioni su come creare AWS Identity and Access Management policy e collegarle alle identità IAM, consulta [Create IAM policies](#) nella IAM User Guide

Policy di onboarding di Systems Manager

È possibile creare una policy IAM come quella mostrata nell'esempio seguente e allegarla alle identità IAM. Questa policy concede l'accesso completo ad onboard e alla configurazione di Systems Manager.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ssm-quicksetup`: consente alle entità principali di accedere a tutte le operazioni di AWS Configurazione rapida di Systems Manager .
- `ssm`: consente alle entità principali l'accesso a Systems Manager Automation e Resource Explorer.
- `organizations`— Consente ai responsabili di leggere la struttura di un'organizzazione e di AWS Organizations gestirne gli amministratori delegati durante l'onboarding a Systems Manager come organizzazione.
- `cloudformation`: consente alle entità principali di creare e gestire stack Quick Setup.
- `iam`: consente alle entità principali di gestire i ruoli e le policy IAM necessarie per l'onboarding di Systems Manager.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "QuickSetupActions",
      "Effect": "Allow",
      "Action": [
        "ssm-quicksetup:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SsmReadOnly",
      "Effect": "Allow",
      "Action": [
        "ssm:DescribeAutomationExecutions",
        "ssm:GetAutomationExecution",
        "ssm:ListAssociations",
        "ssm:DescribeAssociation",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "ssm:DescribePatchBaselines",
        "ssm:GetPatchBaseline",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeMaintenanceWindowTasks"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SsmDocument",
      "Effect": "Allow",
      "Action": [
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource": [
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-*",
        "arn:aws:ssm:*:*:document/AWS-EnableExplorer"
      ]
    }
  ],
}
```

```

{
  "Sid": "SsmEnableExplorer",
  "Effect": "Allow",
  "Action": "ssm:StartAutomationExecution",
  "Resource": [
    "arn:aws:ssm:*:*:document/AWS-EnableExplorer",
    "arn:aws:ssm:*:*:automation-execution/*"
  ]
},
{
  "Sid": "SsmExplorerRds",
  "Effect": "Allow",
  "Action": [
    "ssm:GetOpsSummary",
    "ssm:CreateResourceDataSync",
    "ssm:UpdateResourceDataSync"
  ],
  "Resource": "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*"
},
{
  "Sid": "OrgsReadOnly",
  "Effect": "Allow",
  "Action": [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListRoots",
    "organizations:ListParents",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:DescribeOrganizationalUnit",
    "organizations:ListAWSServiceAccessForOrganization"
  ],
  "Resource": "*"
},
{
  "Sid": "OrgsAdministration",
  "Effect": "Allow",
  "Action": [
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
  ],
  "Resource": "*",
  "Condition": {

```

```

    "StringEquals": {
      "organizations:ServicePrincipal": [
        "ssm.amazonaws.com",
        "ssm-quicksetup.amazonaws.com",
        "member.org.stacksets.cloudformation.amazonaws.com",
        "resource-explorer-2.amazonaws.com"
      ]
    }
  },
  {
    "Sid": "CfnReadOnly",
    "Effect": "Allow",
    "Action": [
      "cloudformation:ListStacks",
      "cloudformation:DescribeStacks",
      "cloudformation:ListStackSets",
      "cloudformation:DescribeOrganizationsAccess"
    ],
    "Resource": "*"
  },
  {
    "Sid": "OrgCfnAccess",
    "Effect": "Allow",
    "Action": [
      "cloudformation:ActivateOrganizationsAccess"
    ],
    "Resource": "*"
  },
  {
    "Sid": "CfnStackActions",
    "Effect": "Allow",
    "Action": [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStackResources",
      "cloudformation:DescribeStackEvents",
      "cloudformation:GetTemplate",
      "cloudformation:RollbackStack",
      "cloudformation:TagResource",
      "cloudformation:UntagResource",
      "cloudformation:UpdateStack"
    ],
    "Resource": [

```

```

        "arn:aws:cloudformation:::stack/StackSet-AWS-QuickSetup-*",
        "arn:aws:cloudformation:::stack/AWS-QuickSetup-*",
        "arn:aws:cloudformation:::type/resource/*"
    ]
},
{
    "Sid": "CfnStackSetActions",
    "Effect": "Allow",
    "Action": [
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation>DeleteStackInstances",
        "cloudformation>DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DetectStackSetDrift",
        "cloudformation:ListStackInstanceResourceDrifts",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateStackSet"
    ],
    "Resource": [
        "arn:aws:cloudformation:::stackset/AWS-QuickSetup-*",
        "arn:aws:cloudformation:::type/resource/*",
        "arn:aws:cloudformation:::stackset-target/AWS-QuickSetup-*:*"
    ]
},
{
    "Sid": "ValidationReadonlyActions",
    "Effect": "Allow",
    "Action": [
        "iam:ListRoles",
        "iam:GetRole"
    ],
    "Resource": "*"
},
{
    "Sid": "IamRolesMgmt",
    "Effect": "Allow",
    "Action": [

```

```

        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:GetRole",
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies"
    ],
    "Resource": [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/service-role/AWS-QuickSetup-*"
    ]
},
{
    "Sid": "IamPassRole",
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/service-role/AWS-QuickSetup-*"
    ],
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": [
                "ssm.amazonaws.com",
                "ssm-quicksetup.amazonaws.com",
                "cloudformation.amazonaws.com"
            ]
        }
    }
},
{
    "Sid": "IamRolesPoliciesMgmt",
    "Effect": "Allow",
    "Action": [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
    ],
    "Resource": [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/service-role/AWS-QuickSetup-*"
    ]
},

```

```

    "Condition": {
      "ArnEquals": {
        "iam:PolicyARN": [
          "arn:aws:iam::aws:policy/
AWSSystemsManagerEnableExplorerExecutionPolicy",
          "arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentRolePolicy"
        ]
      }
    },
    {
      "Sid": "CfnStackSetsSLR",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/aws-service-role/
stacksets.cloudformation.amazonaws.com/
AWSServiceRoleForCloudFormationStackSetsOrgAdmin",
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM",
        "arn:aws:iam::*:role/aws-service-role/
accountdiscovery.ssm.amazonaws.com/AWSServiceRoleForAmazonSSM_AccountDiscovery",
        "arn:aws:iam::*:role/aws-service-role/ssm-quicksetup.amazonaws.com/
AWSServiceRoleForSSMQuickSetup",
        "arn:aws:iam::*:role/aws-service-role/resource-explorer-2.amazonaws.com/
AWSServiceRoleForResourceExplorer"
      ]
    }
  ]
}

```

AWS Systems Manager politica dell'operatore della console

È possibile creare una policy IAM come quella mostrata nell'esempio seguente e allegarla alle identità IAM. Questa policy garantisce l'accesso completo al funzionamento di Systems Manager, consentendogli di eseguire documenti di automazione per la diagnosi e la correzione.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ssm`: consente alle entità principali di accedere a tutte le API di Systems Manager.
- `ssm-quicksetup`: consente alle entità principali di gestire le configurazioni Quick Setup.
- `ec2`— Consente a Systems Manager di determinare lo stato dell'istanza abilitata Regioni AWS e di Amazon EC2.
- `cloudformation`: consente alle entità principali di leggere i propri stack Quick Setup.
- `organizations`— Consente ai responsabili di leggere la struttura di un'organizzazione e di AWS Organizations gestirne gli amministratori delegati durante l'onboarding a Systems Manager come organizzazione.
- `s3`: consente alle entità principali di elencare e ottenere oggetti in un bucket Amazon S3 per la diagnosi, creato durante il processo di onboarding di Systems Manager.
- `iam:PassRole`: consente alle entità principali di trasferire i ruoli da assumere a Systems Manager quando eseguono automazioni per la diagnosi e la correzione di nodi non gestiti.
- `iam:GetRole`: consente alle entità principali di ottenere informazioni specifiche sui ruoli di Quick Setup quando lavorano in Systems Manager.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:*",
        "ssm-quicksetup:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowEC2DescribeActions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource": "*"
    }
  ],
}
```



```

{
  "Sid": "CfnAccess",
  "Effect": "Allow",
  "Action": [
    "cloudformation:ListStacks",
    "cloudformation:ListStackSets",
    "cloudformation:ListStackInstances",
    "cloudformation:ListStackSetOperations",
    "cloudformation:ListStackSetOperationResults",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackSet",
    "cloudformation:DescribeStackSetOperation",
    "cloudformation:DescribeOrganizationsAccess",
    "cloudformation:DescribeStackInstance",
    "cloudformation:DetectStackSetDrift",
    "cloudformation:ListStackInstanceResourceDrifts"
  ],
  "Resource": "*"
},
{
  "Sid": "OrgsReadOnly",
  "Effect": "Allow",
  "Action": [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListRoots",
    "organizations:ListParents",
    "organizations:ListOrganizationalUnitsForParent",
    "organizations:DescribeOrganizationalUnit",
    "organizations:ListAWSServiceAccessForOrganization"
  ],
  "Resource": "*"
},
{
  "Sid": "AllowKMSOperations",
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": "arn:aws:kms:*:key/*",
  "Condition": {
    "StringEquals": {

```

```

        "aws:ResourceTag/SystemsManagerManaged": "true"
    },
    "ArnLike": {
        "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3::do-not-delete-ssm-
diagnosis-*"
    },
    "StringLike": {
        "kms:ViaService": "s3.*.amazonaws.com"
    },
    "Bool": {
        "aws:ViaAWSService": "true"
    }
},
{
    "Sid": "AllowReadS3BucketFromOrganization",
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3::do-not-delete-ssm-diagnosis*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceOrgId": "${aws:PrincipalOrgId}"
        }
    }
},
{
    "Sid": "AllowReadS3BucketFromSingleAccount",
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3::do-not-delete-ssm-diagnosis*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
    }
},
{
    "Effect": "Allow",

```

```

    "Action": "iam:PassRole",
    "Resource": [
        "arn:aws:iam::*:role/AWS-SSM-DiagnosisAdminRole*",
        "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
        "arn:aws:iam::*:role/AWS-SSM-RemediationAdminRole*",
        "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*"
    ],
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "ssm.amazonaws.com"
        }
    }
},
{
    "Sid": "IamReadOnly",
    "Effect": "Allow",
    "Action": "iam:GetRole",
    "Resource": [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/service-role/AWS-QuickSetup-*"
    ]
}
]
}

```

AWS Systems Manager politica di sola lettura per l'operatore della console

È possibile creare una policy IAM come quella mostrata nell'esempio seguente e allegarla alle identità IAM. Questa policy fornisce accesso in sola lettura per utilizzare Systems Manager.

- `ssm`: consente alle entità principali di accedere alle API di sola lettura di Systems Manager.
- `ssm-quicksetup`: consente alle entità principali di leggere le proprie configurazioni Quick Setup.
- `cloudformation`: consente alle entità principali di leggere i propri stack Quick Setup.
- `iam:GetRole`: consente alle entità principali di ottenere informazioni specifiche sui ruoli di Quick Setup durante l'utilizzo in Systems Manager.
- `ec2:DescribeRegions`: consente a Systems Manager di determinare le Regioni AWS abilitate.
- `organizations`— Consente ai responsabili di leggere la struttura di un'organizzazione AWS Organizations quando si iscrivono a Systems Manager come organizzazione.

- s3: consente alle entità principali di elencare e ottenere oggetti in un bucket Amazon S3, creato durante il processo di onboarding di Systems Manager.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "ssm-quicksetup:List*",
        "ssm-quicksetup:Get*",
        "cloudformation:Describe*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "iam:GetRole",
        "ec2:DescribeRegions",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowKMSOperations",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:*:*:key/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/SystemsManagerManaged": "true"
        },
        "ArnLike": {
```

```

        "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
    },
    "StringLike": {
        "kms:ViaService": "s3.*.amazonaws.com"
    },
    "Bool": {
        "aws:ViaAWSService": "true"
    }
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3:::do-not-delete-ssm-diagnosis*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceOrgId": "${aws:PrincipalOrgId}"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3:::do-not-delete-ssm-diagnosis*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
    }
}
]
}

```

Configurazione della console unificata di Systems Manager per un'organizzazione

Il processo di configurazione dell'esperienza di console unificata di Systems Manager va completata dalla Console di gestione AWS con pochi clic. Per configurare Systems Manager per un' AWS Organizations organizzazione, è necessario avere accesso all'account di gestione dell'organizzazione e a un altro account dell'organizzazione da utilizzare come amministratore delegato. L'accesso all'account di gestione è richiesto solo per abilitare o disabilitare Systems Manager. Per gestire i nodi, utilizzerai l'account amministratore delegato.

Prerequisiti

Nella gestione dei nodi all'interno di un'organizzazione, Systems Manager utilizza vari servizi dipendenti per configurare e migliorare la funzionalità della console unificata. Di conseguenza, è necessario che Systems Manager abiliti l'accesso affidabile e registri un account amministratore delegato per i seguenti servizi:

- AWS CloudFormation - Distribuisce le risorse necessarie per Systems Manager nei tuoi account.
- Esploratore di risorse AWS - Ricerca e filtro delle istanze EC2 nei tuoi account.
- AWS Systems Manager Explorer: monitoraggio e risoluzione dei problemi relativi allo stato delle risorse implementate per Systems Manager negli account.
- AWS Systems ManagerQuick Setup: implementa le configurazioni di Quick Setup richieste per Systems Manager negli account.

Prima di iniziare, assicurati di non aver già superato la quota per gli amministratori delegati per nessuno di questi servizi dipendenti. In caso contrario, non sarà possibile registrare gli account di amministratore delegato necessari per abilitare Systems Manager. Quando si abilita Systems Manager per un'organizzazione, viene incluso ogni account della stessa. Attualmente, non è previsto l'esclusione degli account dal processo di configurazione. Quando abiliti Systems Manager, puoi scegliere Regioni AWS quello che desideri includere. È possibile selezionare solo le Regioni che attualmente supportano l'esperienza di console unificata per Systems Manager. Per ulteriori informazioni sulle Regioni in cui è disponibile l'esperienza della console, consulta [Regioni AWS supportate](#).

Risorse per console unificata

Il processo di configurazione della console unificata Systems Manager completa molte attività prerequisite per conto dell'utente. A seconda delle funzionalità che scegli di configurare, è necessario eseguire l'abilitazione della configurazione di gestione host predefinita per fornire le autorizzazioni IAM richieste ai nodi e altro ancora. Di seguito è riportato un elenco dettagliato delle risorse create da Systems Manager per la console unificata. A seconda delle funzionalità che scegli di configurare, alcune risorse potrebbero non essere create.

Esploratore di risorse AWS viste gestite

- `AWSTManagedViewForSSM`: consente a Systems Manager di accedere alle informazioni sulle risorse indicizzate da Resource Explorer per l'organizzazione. Queste viste gestite possono essere aggiornate o eliminate solo da Systems Manager. Ciò significa che se si desidera eliminare le viste gestite o disattivare Resource Explorer, è necessario disabilitare la console unificata. Per ulteriori informazioni sulla disabilitazione della protezione, consulta [Disattivazione della console unificata Systems Manager](#). Per ulteriori informazioni sulle viste gestite, consulta [Viste gestite da AWS](#) nella Guida per l'utente di Resource Explorer.

Note

Quando si crea un indice di aggregazione per Resource Explorer in una Regione diversa da quella di origine, Systems Manager abbassa di livello l'indice attuale. Quindi, Systems Manager promuove l'indice locale nella Regione di origine come nuovo indice di aggregazione. Durante questo periodo, vengono visualizzati solo i nodi della Regione di origine. Il processo richiede fino a 24 ore per essere completato.

Ruoli IAM

- `RoleForOnboardingAutomation`: consente a Systems Manager di gestire le risorse durante il processo di configurazione. Per ulteriori informazioni sulla policy, consulta [AWSQuickSetupSSMManageResourcesExecutionPolicy](#).
- `RoleForLifecycleManagement`: consente a Lambda di gestire il ciclo di vita delle risorse create dal processo di configurazione. Per ulteriori informazioni sulla policy, consulta [AWSQuickSetupSSMLifecycleManagementExecutionPolicy](#).

- **RoleForAutomation**: un ruolo di servizio che Systems Manager Automation necessita per eseguire i runbook. Per ulteriori informazioni, consulta [Crea ruoli di servizio per l'automazione tramite la console](#).
- **AWSSSMDiagnosisAdminRole**: un ruolo amministrativo per avviare automazioni che utilizzano runbook di diagnosi. Per ulteriori informazioni sulle politiche, vedere [AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy](#), [AWS-SSM-Automation-DiagnosisBucketPolicy](#), e [AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy](#).
- **AWSSSMDiagnosisExecutionRole**: un ruolo di esecuzione dell'automazione per il runbook di diagnosi. Per ulteriori informazioni sulle politiche, vedere [AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy](#) e [AWS-SSM-Automation-DiagnosisBucketPolicy](#).
- **AWSSSMRemediationAdminRole**: un ruolo amministrativo per avviare automazioni che utilizzano runbook di correzione. Per ulteriori informazioni sulle politiche, vedere [AWS-SSM-RemediationAutomation-AdministrationRolePolicy](#), [AWS-SSM-Automation-DiagnosisBucketPolicy](#), e [AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy](#).
- **AWSSSMRemediationExecutionRole**: un ruolo di esecuzione dell'automazione per il runbook di correzione. Per ulteriori informazioni sulle politiche, vedere [AWS-SSM-RemediationAutomation-ExecutionRolePolicy](#) e [AWS-SSM-Automation-DiagnosisBucketPolicy](#).
- **ManagedInstanceCrossAccountManagementRole**: consente a Systems Manager di raccogliere informazioni sui nodi gestiti tra gli account.

Associazioni di State Manager

- **EnableDHMCAssociation**: viene eseguito quotidianamente e garantisce che la configurazione predefinita di gestione host sia abilitata.
- **SystemAssociationForEnablingExplorer**: viene eseguito quotidianamente e garantisce che Explorer sia abilitato. Explorer viene utilizzato per sincronizzare i dati dai nodi gestiti.
- **EnableAREXAssociation**— Funziona quotidianamente e garantisce che Esploratore di risorse AWS sia abilitato. Resource Explorer viene utilizzato per determinare quali istanze Amazon EC2 dell'organizzazione non sono gestite da Systems Manager.
- **SSMAgentUpdateAssociation**: viene eseguito ogni 14 giorni e garantisce l'installazione dell'ultima versione dell'SSM Agent disponibile di sui nodi gestiti.
- **SystemAssociationForInventoryCollection**: viene eseguito ogni 12 ore e raccoglie dati di inventario dai nodi gestiti.

Bucket S3

- **DiagnosisBucket**: memorizza i dati raccolti dall'esecuzione del runbook di diagnosi.

Funzioni Lambda

- **SSMLifecycleOperatorLambda**: consente alle entità principali di accedere a tutte le operazioni di AWS Configurazione rapida di Systems Manager .
- **SSMLifecycleResource**: risorsa personalizzata per gestire al meglio il ciclo di vita delle risorse create dal processo di configurazione.

Inoltre, una volta completato il processo di configurazione, è possibile selezionare l'attività per il nodo Diagnostica e correggi, per applicare automaticamente le correzioni ai nodi che non riportano i dati gestiti da Systems Manager. Ciò include l'identificazione di problemi come problemi di connettività di rete agli endpoint Systems Manager e altro ancora. Per ulteriori informazioni, consulta [Diagnosi e correzione](#).

Configura la console unificata

Per configurare Systems Manager per un'organizzazione

1. Accedi all'account di gestione dell'organizzazione.
2. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
3. Inserisci l'ID dell'account che desideri registrare come amministratore delegato.
4. Dopo aver registrato correttamente l'account di amministratore delegato, accedi all'account amministratore delegato appena registrato e torna alla console di Systems Manager per completare la configurazione di Systems Manager.
5. Seleziona Abilita Systems Manager.
6. Nella sezione Home Region, si determina una regione in cui si desidera che Systems Manager aggregi i dati del nodo. Per impostazione predefinita, Systems Manager seleziona la regione attualmente in uso. Per scegliere una regione di residenza diversa, sostituisci la console con quella che desideri utilizzare prima di configurare Systems Manager. I dati dei nodi vengono replicati tra account e regioni dell'organizzazione e archiviati nella regione di origine. La regione scelta non sarà modificabile dopo la configurazione di Systems Manager. Per utilizzare una regione diversa come regione principale dell'organizzazione, è necessario disattivare la console

unificata e completare nuovamente il processo di configurazione. Qualora l'organizzazione utilizzasse IAM Identity Center, sarà necessario selezionare la stessa regione in cui configurare il Centro identità IAM come regione di origine.

7. Nella sezione Regioni, seleziona le regioni in cui desideri abilitare Systems Manager.
8. Nella sezione Configurazioni delle funzionalità, scegli le opzioni da abilitare per la tua configurazione.

Abilita la configurazione predefinita per la gestione degli host (DHMC)

Consente a Systems Manager di configurare DHMC. Questa funzionalità consente a Systems Manager di utilizzare un ruolo IAM per assicurarsi che tutte le istanze Amazon EC2 nell'account e nella regione dispongano delle autorizzazioni necessarie per essere gestite da Systems Manager. Puoi anche specificare la frequenza di correzione delle deviazioni. La deviazione della configurazione si verifica ogni volta che un utente apporta modifiche a un servizio o a una funzionalità in conflitto con le selezioni effettuate tramite la configurazione. Systems Manager verifica la deviazione della configurazione e tenta di correggerla in base alla frequenza specificata. È necessario specificare un valore compreso tra 1 e 31 giorni. Se hai già configurato DHMC in una Regione, Systems Manager non modifica il ruolo IAM precedentemente selezionato. Per ulteriori informazioni su DHMC, consulta [Gestione automatica delle istanze EC2 con la configurazione di gestione host predefinita](#).

DHMC consente di gestire le istanze Amazon EC2 senza dover creare manualmente un profilo di istanza AWS Identity and Access Management (IAM). Ti invitiamo a scegliere questa opzione per assicurarti che le tue istanze EC2 dispongano delle autorizzazioni necessarie per essere gestite da Systems Manager.

Abilita la raccolta dei metadati dell'inventario

Consente a Systems Manager di configurare la raccolta dei seguenti tipi di metadati dai nodi:

- AWS componenti: driver EC2, agenti, versioni e altro ancora.
- Applicazioni: nomi delle applicazioni, editori, versioni e altro.
- Dettagli del nodo: nome del sistema, nome dei sistemi operativi, versione del sistema operativo, ultimo avvio, DNS, dominio, gruppo di lavoro, architettura del sistema operativo e altro.
- Configurazione di rete: indirizzo IP, indirizzo MAC, DNS, gateway, maschera di sottorete e altro.

- Servizi: nome, nome visualizzato, stato, servizi dipendenti, tipo di servizio, tipo di avvio e altro (solo nodi Windows Server).
- Ruoli Windows: nome, nome visualizzato, percorso, tipo di funzionalità, stato installato e altro (solo nodi Windows Server).
- Aggiornamenti di Windows: ID hotfix, installato da, data di installazione e altro (solo nodi Windows Server).

Specifica la frequenza con cui viene raccolto l'inventario. È necessario specificare un valore compreso tra 1 e 744 ore. Per ulteriori informazioni sull'inventario, uno strumento di AWS Systems Manager, consulta [AWS Systems Manager Inventory](#).

Abilita gli aggiornamenti automatici dell'agente di Systems Manager (SSM)

Consente a Systems Manager di verificare la presenza di una nuova versione dell'agente alla frequenza specificata. Il valore della frequenza deve essere compreso tra 1 e 31 giorni. Se è presente una nuova versione, Systems Manager aggiorna automaticamente l'agente sul nodo gestito alla versione più recente rilasciata. Systems Manager non installa l'agente su istanze in cui non è già presente. Per informazioni su quali AMIs hanno l'SSM Agent preinstallato, consulta [Trova AMI con il Agente SSM preinstallato](#).

Ti invitiamo a scegliere questa opzione per assicurarti che i tuoi nodi eseguano sempre la versione più aggiornata di SSM Agent. Per ulteriori informazioni su SSM Agent, incluse quelle su come installare manualmente l'agente, consulta [Lavorare con Agente SSM](#).

9. Seleziona Invia.

La configurazione dell'esperienza console unificata di Systems Manager richiede del tempo a seconda delle dimensioni dell'organizzazione.

Configurazione della console unificata di Systems Manager per singolo account e singola Regione

Per configurare l'esperienza di console unificata di Systems Manager per una singola Account AWS console non è necessario utilizzare Organizations o registrare un account amministratore delegato. Regione AWS Il processo di configurazione per l'esperienza della console Systems Manager completa molte attività prerequisite per conto dell'utente. A seconda delle funzionalità che scegli di configurare, è necessario eseguire l'abilitazione della configurazione di gestione host predefinita

per fornire le autorizzazioni IAM richieste ai nodi e altro ancora. Di seguito è riportato un elenco dettagliato delle risorse create da Systems Manager per la console unificata.

Per le relative informazioni, consulta [Configurare l'accesso alla console di Systems Manager](#).

Risorse per console unificata

A seconda delle funzionalità che scegli di configurare, alcune risorse potrebbero non essere create.

Ruoli IAM

- `RoleForOnboardingAutomation`: consente a Systems Manager di gestire le risorse durante il processo di configurazione. Per ulteriori informazioni sulla policy, consulta [AWSQuickSetupSSMManageResourcesExecutionPolicy](#).
- `RoleForLifecycleManagement`: consente a Lambda di gestire il ciclo di vita delle risorse create dal processo di configurazione. Per ulteriori informazioni sulla policy, consulta [AWSQuickSetupSSMLifecycleManagementExecutionPolicy](#).
- `RoleForAutomation`: un ruolo di servizio che Systems Manager Automation necessita per eseguire i runbook. Per ulteriori informazioni, consulta [Crea ruoli di servizio per l'automazione tramite la console](#).
- `AWSSSMDiagnosisAdminRole`: un ruolo di esecuzione dell'automazione per il runbook di diagnosi. Per ulteriori informazioni sulle politiche, vedere, [AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy](#), [AWS-SSM-Automation-DiagnosisBucketPolicy](#), e [AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy](#).
- `AWSSSMRemediationAdminRole`: un ruolo di esecuzione dell'automazione per il runbook di correzione. Per ulteriori informazioni sulle politiche, vedere [AWS-SSM-RemediationAutomation-AdministrationRolePolicy](#), [AWS-SSM-Automation-DiagnosisBucketPolicy](#), e [AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy](#).
- `ManagedInstanceCrossAccountManagementRole`: consente a Systems Manager di raccogliere informazioni sui nodi gestiti tra gli account.

Associazioni di State Manager

- `EnableDHMCAssociation`: viene eseguito quotidianamente e garantisce che la configurazione predefinita di gestione host sia abilitata.
- `SystemAssociationForEnablingExplorer`: viene eseguito quotidianamente e garantisce che Explorer sia abilitato. Explorer viene utilizzato per sincronizzare i dati dai nodi gestiti.

- **EnableAREXAssociation**— Viene eseguito quotidianamente e garantisce che Esploratore di risorse AWS sia abilitato. Resource Explorer viene utilizzato per determinare quali istanze Amazon EC2 dell'organizzazione non sono gestite da Systems Manager.
- **SSMAgentUpdateAssociation**: viene eseguito ogni 14 giorni e garantisce l'installazione dell'ultima versione dell'SSM Agent disponibile di sui nodi gestiti.
- **SystemAssociationForInventoryCollection**: viene eseguito ogni 12 ore e raccoglie dati di inventario dai nodi gestiti.

Bucket S3

- **DiagnosisBucket**: memorizza i dati raccolti dall'esecuzione del runbook di diagnosi.

Funzioni Lambda

- **SSMLifecycleOperatorLambda**: consente alle entità principali di accedere a tutte le operazioni di AWS Configurazione rapida di Systems Manager .
- **SSMLifecycleResource**: risorsa personalizzata per gestire al meglio il ciclo di vita delle risorse create dal processo di configurazione.

Inoltre, una volta completato il processo di configurazione, è possibile selezionare l'attività per il nodo Diagnostica e correggi, per applicare automaticamente le correzioni ai nodi che non riportano i dati gestiti da Systems Manager. Ciò include l'identificazione di problemi come problemi di connettività di rete agli endpoint Systems Manager e altro ancora.

Configura la console unificata

Per configurare Systems Manager su un singolo account e regione

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Seleziona Abilita Systems Manager.
3. Nella sezione Configurazioni delle funzionalità, scegli le opzioni da abilitare per la tua configurazione.

Abilita la configurazione predefinita per la gestione degli host (DHMC)

Consente a Systems Manager di configurare DHMC. Questa funzionalità consente a Systems Manager di utilizzare un ruolo IAM per assicurarsi che tutte le istanze Amazon EC2 nell'account e nella regione dispongano delle autorizzazioni necessarie per essere gestite da Systems Manager. Puoi anche specificare la frequenza di correzione delle deviazioni. La deviazione della configurazione si verifica ogni volta che un utente apporta modifiche a un servizio o a una funzionalità in conflitto con le selezioni effettuate tramite la configurazione. Systems Manager verifica la deviazione della configurazione e tenta di correggerla in base alla frequenza specificata. È necessario specificare un valore compreso tra 1 e 31 giorni. Se hai già configurato DHMC in una Regione, Systems Manager non modifica il ruolo IAM precedentemente selezionato. Per ulteriori informazioni su DHMC, consulta [Gestione automatica delle istanze EC2 con la configurazione di gestione host predefinita](#).

DHMC consente di gestire le istanze Amazon EC2 senza dover creare manualmente un profilo di istanza AWS Identity and Access Management (IAM). Ti invitiamo a scegliere questa opzione per assicurarti che le tue istanze EC2 dispongano delle autorizzazioni necessarie per essere gestite da Systems Manager.

Abilita la raccolta dei metadati dell'inventario

Consente a Systems Manager di configurare la raccolta dei seguenti tipi di metadati dai nodi:

- AWS componenti: driver EC2, agenti, versioni e altro ancora.
- Applicazioni: nomi delle applicazioni, editori, versioni e altro.
- Dettagli del nodo: nome del sistema, nome dei sistemi operativi, versione del sistema operativo, ultimo avvio, DNS, dominio, gruppo di lavoro, architettura del sistema operativo e altro.
- Configurazione di rete: indirizzo IP, indirizzo MAC, DNS, gateway, maschera di sottorete e altro.
- Servizi: nome, nome visualizzato, stato, servizi dipendenti, tipo di servizio, tipo di avvio e altro (solo nodi Windows Server).
- Ruoli Windows: nome, nome visualizzato, percorso, tipo di funzionalità, stato installato e altro (solo nodi Windows Server).
- Aggiornamenti di Windows: ID hotfix, installato da, data di installazione e altro (solo nodi Windows Server).

Specifica la frequenza con cui viene raccolto l'inventario. È necessario specificare un valore compreso tra 1 e 744 ore. Per ulteriori informazioni sull'inventario, uno strumento di AWS Systems Manager, consulta [AWS Systems Manager Inventory](#).

Attivare gli aggiornamenti automatici dell'agente di Systems Manager (SSM)

Consente a Systems Manager di verificare la presenza di una nuova versione dell'agente alla frequenza specificata. Il valore della frequenza deve essere compreso tra 1 e 31 giorni. Se è presente una nuova versione, Systems Manager aggiorna automaticamente l'agente sul nodo gestito alla versione più recente rilasciata. Systems Manager non installa l'agente su istanze in cui non è già presente. Per informazioni su quali AMIs hanno l'SSM Agent preinstallato, consulta [Trova AMI con il Agente SSM preinstallato](#).

Ti invitiamo a scegliere questa opzione per assicurarti che i tuoi nodi eseguano sempre la versione più aggiornata di SSM Agent. Per ulteriori informazioni su SSM Agent, incluse quelle su come installare manualmente l'agente, consulta [Lavorare con Agente SSM](#).

4. Seleziona Invia.

Disattivazione della console unificata Systems Manager

Per disabilitare la console unificata di Systems Manager per un'organizzazione, è necessario accedere all'account registrato come amministratore delegato per Systems Manager. Dopo aver effettuato l'accesso all'account amministratore delegato dell'organizzazione, è possibile disabilitare la configurazione dell'organizzazione nella sezione Impostazioni della console unificata. Quando si disabilita la configurazione della console unificata per l'organizzazione, Systems Manager elimina le risorse create, incluse le viste gestite di Resource Explorer, durante il processo di configurazione. La disabilitazione della configurazione per l'organizzazione non revoca l'accesso attendibile né annulla la registrazione degli account amministratore delegato per i servizi dipendenti. Nella procedura seguente viene descritto come disabilitare la configurazione per la console unificata.

Per le relative informazioni, consulta [Configurare l'accesso alla console di Systems Manager](#).

Per disabilitare la configurazione per la console unificata Systems Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Scegli Impostazioni nel pannello di navigazione.

3. Seleziona Disabilita. È necessario confermare che desideri disabilitare la configurazione per l'organizzazione. Questa operazione elimina le risorse create per la console unificata e non sarà annullabile.

Se non riesci ad accedere all'account amministratore delegato per Systems Manager, puoi disabilitare la configurazione unificata della console dall'account di gestione. Usa AWS CLI o SDK per chiamare l'`DeleteConfigurationManager` operazione API. Trasferisci il `ManagerArn` valore per la configurazione dell'organizzazione nel tuo account. Il formato per l'ARN del gestore è il seguente:

`arn:aws:ssm-quicksetup:account-id:configuration-manager/configuration-manager-id.`

 Note

Se non conosci il valore di *configuration-manager-id*, richiama l'azione `ListConfigurationManagers` API e filtra i risultati utilizzando il `AWSQuickSetupType-SSM` tipo.

Esecuzione di attività di gestione dei nodi con AWS Systems Manager

Gli argomenti seguenti descrivono come completare le attività comuni dei nodi. È possibile utilizzare la AWS Systems Manager console unificata per un' AWS Organizations organizzazione e per un singolo Account AWS individuo.

Argomenti

- [Esaminare approfondimenti nodo](#)
- [Esplorazione dei nodi](#)
- [Just-in-time accesso al nodo tramite Systems Manager](#)
- [Diagnosi e correzione](#)
- [Regolazione delle impostazioni di Systems Manager](#)

Esaminare approfondimenti nodo

È possibile ottenere approfondimenti sullo stato generale dei nodi gestiti e delle istanze EC2 non gestite nell'organizzazione o account utilizzando la nuova esperienza della console di Systems Manager.

Systems Manager fornisce una panoramica visiva dei nodi gestiti e delle istanze EC2 non ancora gestite da Systems Manager. (Un nodo gestito è qualsiasi macchina configurata per l'utilizzo con Systems Manager in ambienti [ibridi e multicloud](#). Per informazione sui tipi di macchine supportate, consulta [Tipi di macchine supportati in ambienti ibridi e multicloud](#).)

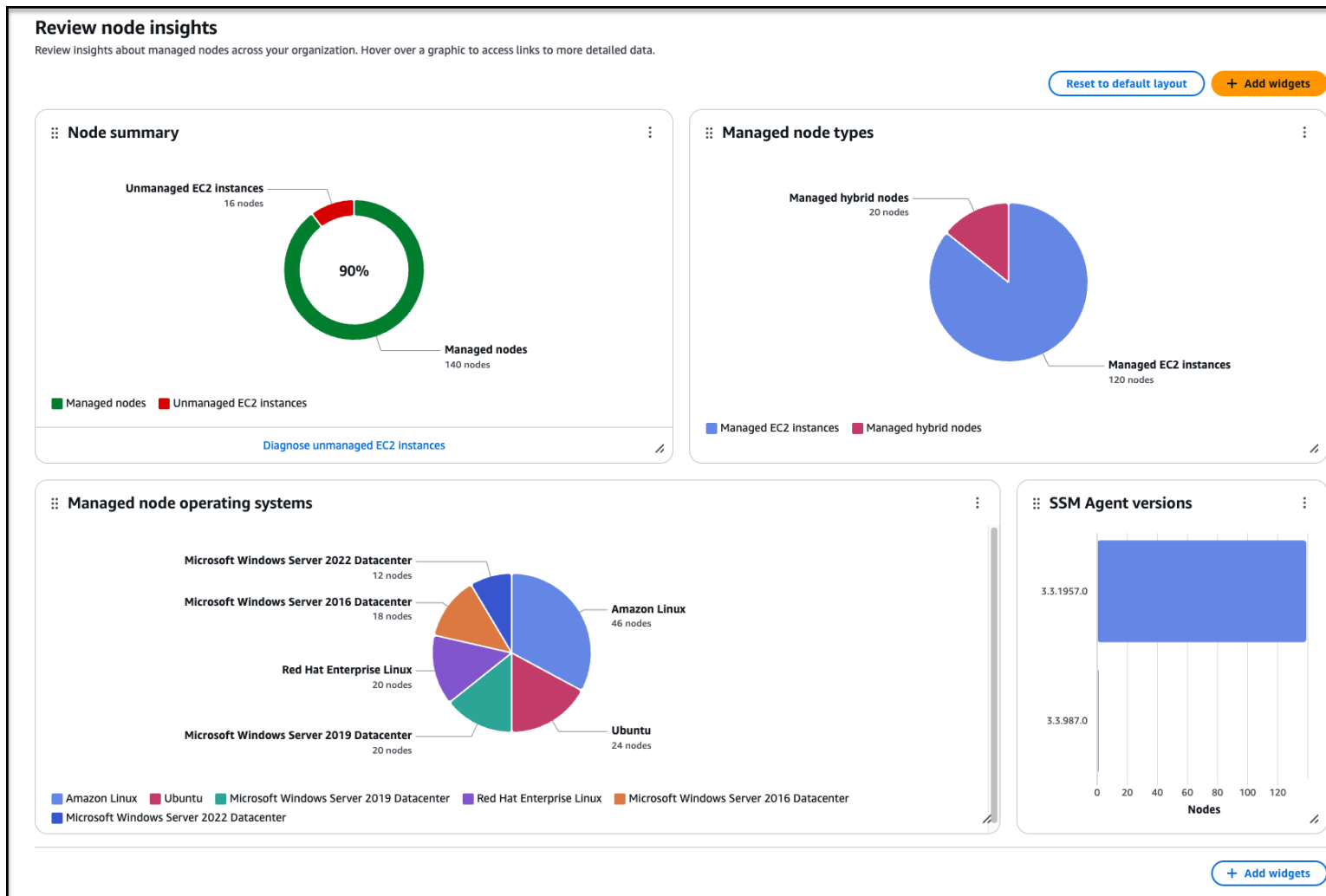
Questa panoramica viene fornita tramite singole caselle di rapporto, chiamate widget, che presentano grafici a torta interattivi e altri elementi grafici.

Prima di iniziare

Per esaminare le informazioni sui nodi, devi prima effettuare l'onboarding della tua organizzazione o del tuo account nella console unificata di Systems Manager. Per ulteriori informazioni, consulta [Configurazione AWS Systems Manager](#).

Dopo l'onboarding, apri la [console Systems Manager](#) e scegli Esamina approfondimenti nodo.

L'immagine seguente mostra le singole caselle di report, chiamate widget, disponibili nella pagina Esamina approfondimenti nodo.



Il display supporta widget che forniscono le seguenti informazioni.

Riepilogo nodo

Indica quante istanze EC2 dell'organizzazione o dell'account non sono attualmente nodi gestiti e quanti nodi gestiti sono presenti nel parco istanze dell'organizzazione o dell'account.

Cos'è un'istanza non gestita?

Quando si arresta un'istanza EC2 gestita, quest'ultima viene segnalata come "Non gestita" nella console di Systems Manager. Questo è un comportamento previsto perché SSM Agent non dispone di una connessione attiva al servizio.

Note

Questo è diverso da come AWS Config definisce un'istanza come non gestita. Se un'istanza è attualmente interrotta, AWS Config riporta lo stato dell'ultima connessione «heartbeat» tra SSM Agent l'istanza e il servizio Systems Manager.

Al riavvio, l'istanza si riconnette automaticamente al servizio di Systems Manager e il suo stato nella console unificata viene ripristinato su "Gestito" entro cinque minuti. Non è richiesto alcun intervento manuale e tutte le configurazioni di Systems Manager per l'istanza vengono mantenute durante il Stop/Start ciclo.

Tuttavia, se l'istanza non viene ancora segnalata come "Gestita", diversi minuti dopo l'avvio, è probabile che non sia configurata correttamente per la gestione di Systems Manager. In questo caso, consigliamo di eseguire una diagnosi per identificare il motivo per cui l'istanza rimane in uno stato non gestito. Per ulteriori informazioni, consulta [Diagnostica e correzione di istanze Amazon EC2 non gestite in Systems Manager](#).

Se la scansione diagnostica non è in grado di determinare il problema, fate riferimento ai seguenti argomenti per verificare che i requisiti per SSM Agent i ruoli AWS Identity and Access Management (IAM) e i prerequisiti di Systems Manager siano soddisfatti:

- [Risoluzione dei problemi Agente SSM](#)
- [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#)
- [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#)

Tipi di nodi gestiti

Mostra quanti nodi gestiti del parco sono istanze EC2 e quanti sono altri tipi di server. Altri tipi includono server locali, dispositivi AWS IoT Greengrass principali AWS IoT e dispositivi non AWS periferici e macchine virtuali (VM) in altri ambienti cloud. Passa il mouse sul grafico dei tipi di nodi per accedere ai collegamenti a maggiori dettagli nella pagina [Esplora i nodi](#).

Per ulteriori informazioni sul AWS supporto per ambienti ibridi e multicloud, consulta [AWS Soluzioni per ambienti ibridi e multicloud](#).

Versioni SSM Agent

Fornisce informazioni sulle installazioni di AWS Systems Manager Agent (SSM Agent) nella tua flotta. SSM Agent è un software Amazon che viene eseguito sui tuoi nodi gestiti. SSM Agent consente a Systems Manager di aggiornare, gestire e configurare queste risorse. L'agente

elabora le richieste dal servizio Systems Manager in Cloud AWS, quindi le esegue come specificato nella richiesta.

Per i nodi gestiti nel parco istanze, questo widget riporta le versioni SSM Agent del parco istanze, dalla più recente alla meno recente. È possibile consultare la grafica delle versioni SSM Agent per accedere ai link a maggiori dettagli nella pagina Esplora i nodi.

Per ulteriori informazioni su SSM Agent, consultare [Lavorare con Agente SSM](#).

Sistemi operativi a nodi gestiti

Fornisce una suddivisione della percentuale di ciascun sistema operativo sui nodi gestiti nel parco istanze. È possibile consultare la grafica dei Nodi gestiti dal sistema operativo per accedere ai collegamenti a maggiori dettagli nella pagina Esplora i nodi.

È possibile personalizzare il layout del widget nella pagina Esamina approfondimenti nodi utilizzando una funzionalità di trascinamento, o rimuovendo e aggiungendo widget al display.

Utilizza le informazioni nei seguenti argomenti per lavorare al meglio con i widget Systems Manager sull'approfondimento dei nodi.

Argomenti

- [Aggiungere o rimuovere widget dal Esamina approfondimenti nodo page](#)
- [Riorganizzazione dei widget nel Esamina approfondimenti nodo page](#)

Aggiungere o rimuovere widget dal Esamina approfondimenti nodo page

È possibile personalizzare il layout nella pagina Systems Manager Esamina approfondimenti nodi aggiungendo e rimuovendo i widget.

Note

Per impostazione predefinita, nella pagina sono visualizzati tutti i widget disponibili.

Per aggiungere o rimuovere widget da Esamina approfondimenti nodo page

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>

2. Dal riquadro di navigazione a sinistra, scegli Esamina approfondimenti nodi.
3. Per rimuovere un widget dal display, procedi come segue:
 - a. Scegli il menu Altre opzioni
 per il widget.
 - b. Scegli Remove widget (Rimuovi widget).
4. Per aggiungere un widget al display, procedi come segue:
 - a. Seleziona Add widget (Aggiungi widget).
 - b. Nel riquadro Aggiungi widget, tieni premuta la maniglia di trascinamento
 del widget per aggiungerlo al display.
 - c. Trascina il widget e rilascialo nel riquadro principale.

Riorganizzazione dei widget nel Esamina approfondimenti nodo page

È possibile personalizzare il layout nella pagina Esamina approfondimenti nodi riorganizzando i widget.

Per riorganizzare i widget in Esamina approfondimenti nodo page

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel riquadro di navigazione, scegli Esamina approfondimenti nodi.
3. Per personalizzare il layout del widget, scegli un widget che desideri spostare. Tieni premuta la maniglia di trascinamento
 del widget, quindi trascinalo nella nuova posizione.
4. Ripeti questo processo per ogni widget che desideri riposizionare.

Se il nuovo layout non piace, scegliere Ripristina il layout predefinito per spostare tutti i widget nella loro posizione originale.

Esplorazione dei nodi

È possibile utilizzare la pagina Esplora nodi su Systems Manager per esaminare i dettagli dei nodi gestiti nell'organizzazione o nell'account in base ai criteri specificati nei filtri. Puoi anche utilizzare l'integrazione di Systems Manager con Amazon Q Developer (Amazon Q), una soluzione di intelligenza artificiale AWS generativa, per effettuare ricerche tramite prompt di testo.

Prima di iniziare

Per utilizzare la funzionalità Explore nodes, devi prima effettuare l'onboarding della tua organizzazione o del tuo account sulla console unificata di Systems Manager. Per ulteriori informazioni, consulta [Configurazione della console unificata di Systems Manager per un'organizzazione](#).

Dopo l'onboarding, apri la [Console di Systems Manager](#) e scegli Esplora nodi.

Note

Quando si crea un indice di aggregazione per Resource Explorer in una regione diversa dalla propria regione di origine, Systems Manager riduce di livello l'indice corrente. Quindi, Systems Manager promuove l'indice locale nella Regione di origine come nuovo indice di aggregazione. Durante questo periodo, vengono visualizzati solo i nodi della Regione di origine. Il processo richiede fino a 24 ore per essere completato.

Argomenti

- [Esplorazione dei nodi utilizzando i filtri della console](#)
- [Esplorazione dei nodi utilizzando prompt di testo in Amazon Q](#)
- [Visualizzazione dei dettagli dei singoli nodi e operazioni intraprese su un nodo](#)
- [Effettuare il download o l'esportazione di un report sui nodi gestiti](#)
- [Gestione del contenuto e dell'aspetto dei report dei nodi](#)

Esplorazione dei nodi utilizzando i filtri della console

Nella console Systems Manager, è quindi possibile raggruppare i nodi gestiti in base alle seguenti visualizzazioni:

All nodes (No filter)

Elenca tutti i nodi gestiti nell'organizzazione o nell'account.

Explore nodes (56)
Explore details about managed nodes in your organization.

Group by
None

Nodes (56) Advanced instances

Find nodes

< 1 ... >

Node ID	Agent type	Agent version	Node status	Operating system name	Operating system type	Operating system version	Node type	Ac
i-00133d4e1c15e843b	amazon-ssm-agent	3.3.1230.0	Active	Ubuntu	Linux	20.04	EC2Instance	
i-00ba99a313b84a821	amazon-ssm-agent	3.3.1230.0	Active	Microsoft Windows Server 2022 Datacenter	Windows	10.0.20348	EC2Instance	
i-010e038ef4f248dbd	amazon-ssm-agent	3.3.1230.0	Active	Amazon Linux	Linux	2	EC2Instance	
i-013d9f572f5e5b6b3	amazon-ssm-agent	3.3.1230.0	Active	Microsoft Windows Server 2016 Datacenter	Windows	10.0.14393	EC2Instance	
i-018515ec864b6b34d	amazon-ssm-agent	3.3.987.0	Active	Ubuntu	Linux	24.04	EC2Instance	
i-0207b54c36e64ffac	amazon-ssm-agent	3.3.1230.0	Active	Amazon Linux	Linux	2	EC2Instance	
i-02384ada61f4a07a8	amazon-ssm-agent	3.3.1230.0	Active	Microsoft Windows Server 2019 Datacenter	Windows	10.0.17763	EC2Instance	

Node types

Fornisce schede per visualizzare separatamente i dati per le istanze Amazon Elastic Compute Cloud (Amazon EC2) e altri tipi di macchine. Altri tipi includono server locali, dispositivi AWS IoT Greengrass principali e dispositivi non periferici AWS IoT e macchine AWS virtuali in altri ambienti cloud.

Explore nodes (56)

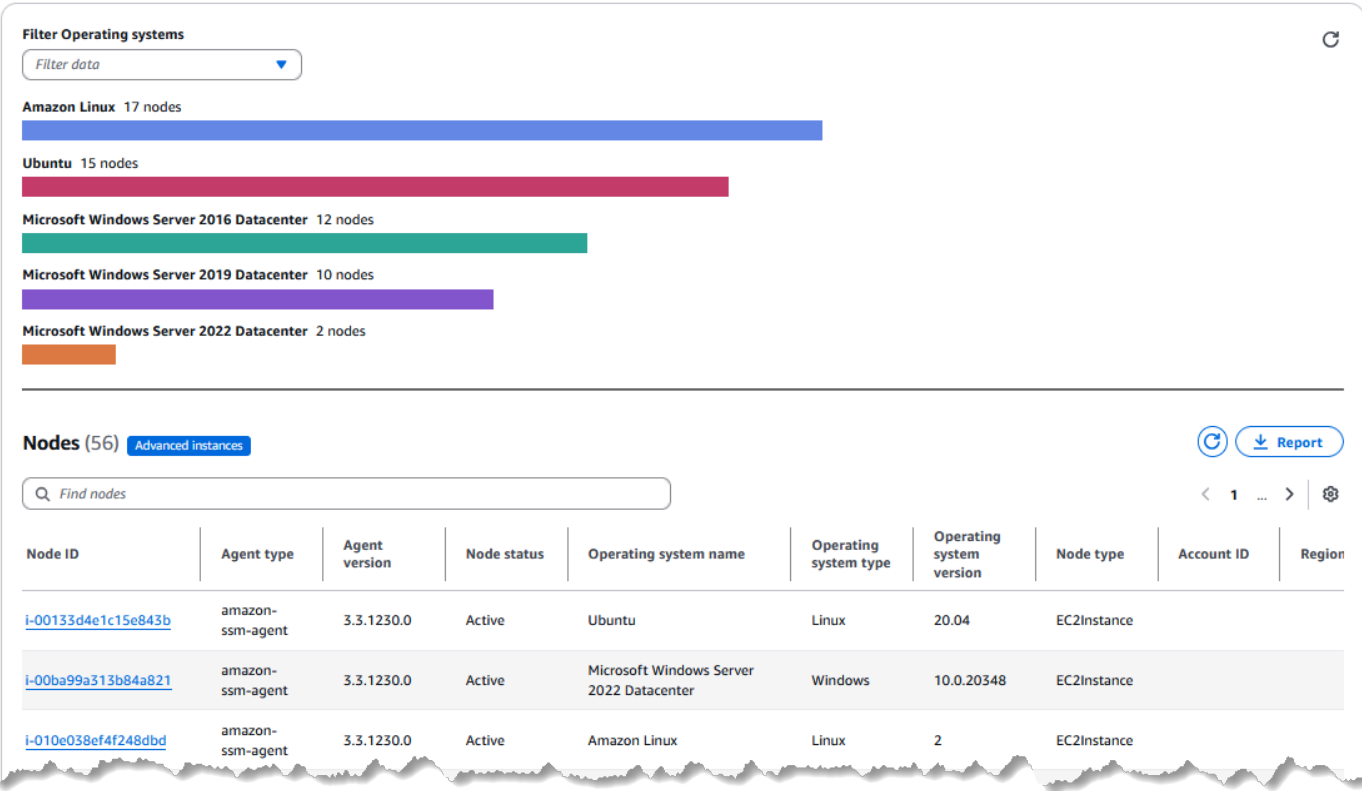
Explore details about managed nodes in your organization.

Group by

Node types

Managed EC2 instances

56



Operating systems

Fornisce una scheda per ogni tipo di sistema operativo dell'organizzazione o dell'account, come Amazon Linux e Microsoft Windows Server 2022 Datacenter. In ogni scheda, è possibile filtrare ulteriormente l'elenco selezionando solo versioni specifiche dei sistemi operativi, come Amazon Linux 2 e Amazon Linux 2023.

Explore nodes (56)

Explore details about managed nodes in your organization.

Group by

Operating systems ▾

Amazon Linux

17

Ubuntu

15

Microsoft Windows Server 2016 Datacenter

12

Microsoft Windows Server 2019 Datacenter

10

Microsoft Windows Server 2022 Datacenter

2

Filter Operating system versions

Filter data ▾

2 17 nodes

Nodes (17)

Advanced instances



Report

Find nodes

<

1

>



Node ID	Agent type	Agent version	Node status	Operating system name	Operating system type	Operating system version	Node type	Ac
i-010e038ef4f248dbd	amazon-ssm-agent	3.3.1230.0	Active	Amazon Linux	Linux	2	EC2Instance	
i-0207b54c36e64ffac	amazon-ssm-agent	3.3.1230.0	Active	Amazon Linux	Linux	2	EC2Instance	
i-03b5c28d6e10a42a1	amazon-ssm-agent	3.3.1230.0	Active	Amazon Linux	Linux	2	EC2Instance	
i-03b985ae75c76da56	amazon-ssm-agent	3.3.1230.0	Active	Amazon Linux	Linux	2	EC2Instance	

Agente SSM versions

Fornisce una scheda per ogni versione dell'SSM Agent installata sui nodi gestiti del parco istanze. In ogni scheda, è possibile filtrare ulteriormente l'elenco selezionando solo sistemi operativi specifici, come Amazon Linux e Microsoft Windows Server 2022 Datacenter.

Explore nodes (56)

Explore details about managed nodes in your organization.

Group by

SSM Agent versions

3.3.1230.0

48

3.3.987.0

8

Filter Operating systems

Filter data

Amazon Linux 17 nodes

Microsoft Windows Server 2016 Datacenter 12 nodes

Microsoft Windows Server 2019 Datacenter 10 nodes

Ubuntu 7 nodes

Microsoft Windows Server 2022 Datacenter 2 nodes

Nodes (48)

Advanced instances

Report

Find nodes

Node ID	Agent type	Agent version	Node status	Operating system name	Operating system type	Operating system version	Node type	Account ID	Region
i-00133d4e1c15e843b	amazon-ssm-agent	3.3.1230.0	Active	Ubuntu	Linux	20.04	EC2Instance		
i-00ba99a313b84a821	amazon-ssm-agent	3.3.1230.0	Active	Microsoft Windows Server 2022 Datacenter	Windows	10.0.20348	EC2Instance		
i-010e038ef4f248dbd	amazon-ssm-agent	3.3.1230.0	Active	Amazon Linux	Linux	2	EC2Instance		

Per ogni visualizzazione, è possibile perfezionare l'elenco dei nodi filtrando proprietà come lo stato del nodo, l'ID o l' Account AWS ID dell'unità organizzativa.

È possibile personalizzare la visualizzazione del rapporto scegliendo quali delle colonne di dati disponibili vengono visualizzate nella pagina Esplora nodi. Inoltre, è possibile scaricare rapporti in formato CSV o JSON, oppure esportarli in Amazon S3 in formato CSV.

Argomenti

- [Scelta di una visualizzazione dei filtri per i riepiloghi dei nodi gestiti](#)

Scelta di una visualizzazione dei filtri per i riepiloghi dei nodi gestiti

La pagina **Esplora i nodi** in Systems Manager consente di visualizzare i dati aggregati sulla flotta in base a diverse visualizzazioni di filtro disponibili.

Per scegliere una visualizzazione filtrante per i riepiloghi dei nodi gestiti

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>

2. Nel riquadro di navigazione, scegli **Esplora nodi**.

3. Per la visualizzazione **Filtro**, seleziona una delle opzioni di filtro e, facoltativamente, refinisci ulteriormente il rapporto:

- **Nodi gestiti:** nella casella di ricerca



seleziona una proprietà e un delimitatore, ad esempio `Node type = Managed EC2 instances`.

- **Sistemi operativi:** nell'elenco **Filtra versioni del sistema operativo**, è possibile selezionare un numero di versione del sistema operativo. Nella casella di ricerca



è possibile selezionare una proprietà e un delimitatore, ad esempio `Node type = Managed EC2 instances`.

- **Versioni di SSM Agent:** nell'elenco **Filtra versioni del sistema operativo**, è possibile selezionare un nome di sistema operativo. Nella casella di ricerca



è possibile selezionare una proprietà e un delimitatore, ad esempio `Node type = Managed EC2 instances`.

- **Tipi di nodi:** nell'elenco **Filtra versioni del sistema operativo**, è possibile selezionare un nome di sistema operativo. Nella casella di ricerca



è possibile selezionare una proprietà e un delimitatore, ad esempio `Node type = Managed EC2 instances`.

Dopo aver filtrato facoltativamente l'elenco, è possibile visualizzare i dettagli su uno specifico nodo gestito scegliendone l'ID nella colonna **ID nodo**. Da questa visualizzazione dettagliata, è possibile eseguire diverse azioni sul nodo.

Esplorazione dei nodi utilizzando prompt di testo in Amazon Q

Utilizzando l'integrazione di Systems Manager con Amazon Q Developer, è possibile utilizzare prompt di testo per visualizzare le informazioni create dall'IA generativa sui nodi gestiti.

Amazon Q Developer è un assistente AI-powered conversazionale generativo che può aiutarti a comprendere, creare, estendere e utilizzare le applicazioni. AWS Per accelerare la tua crescita AWS, il modello alla base di Amazon Q è arricchito con AWS contenuti di alta qualità per produrre risposte più complete, utilizzabili e referenziate. Per ulteriori informazioni, consulta [Cos'è Amazon Q Developer?](#) nella Guida per l'utente di Amazon Q Developer.

L'integrazione tra Systems Manager e Amazon Q consente di ottenere rapidamente visibilità e controllo su ambienti distribuiti di grandi dimensioni in più Account AWS regioni. È possibile utilizzare il sistema di query in linguaggio naturale per cercare rapidamente i dati dei nodi, quindi identificare i problemi e agire più rapidamente.

Quando fai una domanda in linguaggio naturale su nodi o istanze gestite, Amazon Q utilizza l'azione Systems Manager `ListNodes` e crea filtri in base all'input testuale per recuperare i risultati.

Ad esempio, supponi di fornire ad Amazon Q il seguente prompt:

List my managed nodes running Red Hat Enterprise Linux 9.2

Amazon Q determina quali filtri includere in una richiesta, quindi esegue una query simile alla seguente:

```
aws ssm list-nodes \
  --filters Key=PlatformName,Values='Red Hat Enterprise Linux',Type=Equal
  Key=PlatformVersion,Values=9.2,Type=Equal
```

Amazon Q genera quindi un rapporto sulle istanze Red Hat Enterprise Linux presenti nell'account, elencando informazioni come il numero di istanze, i relativi ID e regioni.

È possibile anche visualizzare un riepilogo JSON dei dettagli di ciascuna istanza, nonché aprire un link per visualizzare gli elenchi completi delle istanze EC2 o dei nodi gestiti nella pagina Systems Manager Esplora nodi. La pagina Esplora nodi mostra i risultati che corrispondono ai criteri di filtro inclusi nel prompt. Da lì, è possibile modificare o perfezionare i filtri per la richiesta, come descritto in [Esplorazione dei nodi](#).

Argomenti

- [Impara a creare prompt efficaci per chiedere informazioni sul parco istanze ad Amazon Q](#)

- [Esplorazione dei nodi gestiti utilizzando Amazon Q](#)

Impara a creare prompt efficaci per chiedere informazioni sul parco istanze ad Amazon Q

Migliore è la qualità della domanda o del prompt che invii ad Amazon Q, migliori saranno i risultati che otterrai.

Suggerimenti per i prompt di query

Tieni presente i seguenti suggerimenti quando richiedi ad Amazon Q informazioni sul parco istanze:

1. Per migliorare l'accuratezza dei risultati, utilizza i termini "nodi gestiti" e "istanze gestite" nei prompt, anziché solo "nodi" e "istanze".
2. Per ottenere risultati su più account che fanno parte di un'organizzazione, come configurato in AWS Organizations, è necessario accedere all'account amministratore delegato nella regione di residenza designata.
3. Nell'account amministratore delegato, utilizza termini per aiutare Amazon Q a capire che stai chiedendo informazioni su nodi e istanze all'interno dell'organizzazione, scegliendo specificamente termini come "nella mia organizzazione" o "nel mio account 123456789012".

Argomenti

- [Esempi di domande per Amazon Q](#)
- [Nomi e versioni dei sistemi operativi supportati per i prompt](#)

Esempi di domande per Amazon Q

Nella tabella seguente, forniamo domande di esempio che illustrano alcuni modi in cui è possibile creare query su Amazon Q che portino a risultati migliori.

Forniamo anche esempi dei filtri che Amazon Q applicherà all'esecuzione del [ListNodes](#) comando, generati dal contenuto del prompt.

Esempio di domanda in linguaggio naturale	Filtri applicati di Amazon Q
Show me my Windows managed nodes.	PlatformType = Windows

Esempio di domanda in linguaggio naturale	Filtri applicati di Amazon Q
List my managed instances in account 123456789012.	AccountId = 123456789012
Show me all managed nodes running Amazon Linux 2 across my organization.	PlatformName = Amazon Linux PlatformVersion = 2
Show me all managed instances running Microsoft Windows Server 2019 Datacenter in my organization.	PlatformName = Microsoft Windows Server 2019 Datacenter
Can you show me all managed nodes with SSM Agent version 3.3.1142.0?	AgentType = amazon-ssm-agent AgentVersion = 3.3.1142.0
List all Amazon Linux 2 managed instances in account 123456789012 that have SSM Agent version 3.3.1230.0.	PlatformName = Amazon Linux PlatformVersion = 2 AccountId = 123456789012 AgentType = amazon-ssm-agent AgentVersion = 3.3.1230.0
What Microsoft Windows Server 2012 R2 Enterprise managed nodes are running in the eu-central-1 region across my entire organization?	PlatformName = Microsoft Windows Server 2012 R2 Enterprise Region = eu-central-1
Show me all managed instances running Red Hat Linux 7 in ou-d6ty-gxdma6vm.	PlatformName = RHEL Linux PlatformVersion = 7 OrganizationalUnitId = ou-d6ty-gxdma6vm
What Ubuntu managed instances are in account 123456789012?	PlatformName = Ubuntu AccountId = 123456789012

Esempio di domanda in linguaggio naturale	Filtri applicati di Amazon Q
List my Linux managed instances.	PlatformType = Linux
Find my macOS managed nodes.	PlatformType = macOS
Show me all versions of Amazon Linux managed nodes in my org.	PlatformName = Amazon Linux
List managed nodes running Amazon Linux 2.	PlatformName = Amazon Linux PlatformVersion = 2
List the managed nodes with Ubuntu 22.04 in account 123456789012.	PlatformName = Ubuntu PlatformVersion = 22.04 AccountId = 123456789012
Find all managed nodes that have an SSM Agent version that is not 3.3.987.0.	AgentType = amazon-ssm-agent AgentVersion != 3.3.987.0
List all managed instances that are not running a Linux operating system.	PlatformType != Linux

Nomi e versioni dei sistemi operativi supportati per i prompt

Quando chiedi ad Amazon Q informazioni sui nodi gestiti dell'account, è utile fornire il nome di un sistema operativo così come indicato su Systems Manager. È possibile anche fornire numeri di versione per restringere ulteriormente i risultati. Ad esempio, come illustrato nelle tabelle seguenti, è possibile richiedere risultati specifici su **macOS 14.5**, **Microsoft Windows Server 2019 Datacenter**, and **AlmaLinux 9.2 through 9.4**, per citare solo alcuni esempi.

Questi elenchi sono da considerarsi non esaustivi e vengono proposti solo a titolo esemplificativo.

macOS

Nome piattaforma	Numeri di versione
macOS	13.2, 13.4, 13.7, 14.1, 14.5, 14.6.1, 15.0

Windows

Rilasci	Numeri di versione
Microsoft Windows Server 2012 R2 Datacenter	6,3,9600
Microsoft Windows Server 2012 R2 Standard	6,3,9600
Microsoft Windows Server 2012 Standard	6,2,9200
Microsoft Windows Server 2016 Datacenter	N/A
Microsoft Windows Server 2016 Standard	10,0,14393
Microsoft Windows Server 2019 Datacenter	N/A
Microsoft Windows Server 2019 Standard	N/A
Microsoft Windows Server 2022 Datacenter	N/A
Microsoft Windows Server 2022 Standard	100,20348

Linux

Nomi della piattaforma	Numeri di versione
AlmaLinux	8.10, 9.2, 9.3, 9.4
Amazon Linux 2	2.0 e versioni successive
Amazon Linux 2023	2023.0.20230315.0 e versioni successive

Nomi della piattaforma	Numeri di versione
BottleRocket	1.14.3, 1.16.1, 1.18.0, 1.19.1, 1.19.2, 1.19.5, 1.20.0, 1.20.1, 1.20.2, 1.20.3, 1.20.5, 1.21.1, 1.23.0, 1.24.0, 1.24.1, 1.25.0, 1.26.1,
CentOS Stream	9
Debian GNU/Linux	11-12
Oracle Linux Server	7.8, 8.2, 8.3, 8.8, 8.9, 8.10, 9.4
Red Hat Enterprise Linux	8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 9.2, 9.3, 9.4
Server Red Hat Enterprise Linux	17.3, 7.6, 7.7, 7.8, 7.9
Rocky Linux	8.6, 8.7, 8.8, 8.9, 8.10, 9.1, 9.2, 9.3, 9.4
Ubuntu Server	18,04, 20,04, 22,04, 24,04

Esplorazione dei nodi gestiti utilizzando Amazon Q

L'integrazione di Systems Manager con Amazon Q Developer ti consente di porre domande sui nodi gestiti della tua flotta. Puoi accedere a questa funzionalità da qualsiasi punto in Console di gestione AWS cui è disponibile l'interfaccia Amazon Q.

Per ulteriori informazioni sull'interazione con Amazon Q, consulta [Parlando di AWS con un Amazon Q Developer](#) nella Guida per l'utente di Amazon Q Developer.

Per esplorare i nodi gestiti utilizzando Amazon Q

- Da qualsiasi punto Console di gestione AWS, scegli l'icona Amazon Q ).
- Nel campo prompt nella parte inferiore del riquadro Amazon Q, fare una domanda sui nodi gestiti nell'account o nell'organizzazione.

 Tip

Per suggerimenti su come creare prompt efficaci, consulta le informazioni contenute in [Impara a creare prompt efficaci per chiedere informazioni sul parco istanze ad Amazon Q](#).

3. Esaminare le informazioni su nodi specifici o scegliere Apri la console AWS Systems Manager per continuare l'esplorazione.

Visualizzazione dei dettagli dei singoli nodi e operazioni intraprese su un nodo

Da un elenco nella pagina Esplora nodi in Systems Manager, è possibile selezionare un singolo nodo per visualizzare dettagli completi sulla macchina o eseguire una serie di azioni sul nodo. Generale, nella pagina dei dettagli, presenta informazioni complete sul nodo.

Per visualizzare i dettagli dei singoli nodi e intraprendere operazioni su un nodo

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel riquadro di navigazione, scegli Esplora nodi.
3. (Facoltativo) Segui i passaggi indicati in [Scelta di una visualizzazione dei filtri per i riepiloghi dei nodi gestiti](#) per rifinire l'elenco dei nodi gestiti visualizzati per l'organizzazione o l'account.
4. Nella colonna ID nodo, scegli l'ID collegato di un nodo.
5. Per visualizzare ulteriori dettagli sul nodo, nella barra di navigazione a sinistra, nell'elenco Proprietà, scegli una proprietà per visualizzare ulteriori informazioni su:
 - Tag: visualizza un elenco di tag applicati al nodo. È anche possibile aggiungere o rimuovere tag.
 - Inventario: scegli un tipo di inventario, ad esempio AWS:Application o AWS:Network, per visualizzare i dettagli dell'inventario per il nodo.
 - Associazioni: visualizza i dettagli su tutte le associazioni State Manager applicate al nodo, inclusi dettagli come lo stato e il nome del documento SSM associato.
 - Patch: visualizza informazioni di riepilogo sulle patch e sullo stato delle patch per il nodo.

- Conformità della configurazione: visualizza i dettagli di conformità per il nodo, come lo stato di conformità e la gravità dei problemi di conformità.

Per ulteriori informazioni sui dettagli sulle schede, consulta [the section called “Che cos'è la console unificata?”](#).

6. Per eseguire operazioni sul nodo, è possibile utilizzare le seguenti opzioni nel menu Operazioni del nodo:

 Note

Queste operazioni sono disponibili solo per i nodi gestiti nell' Account AWS e nella Regione in cui si sta lavorando attualmente. Per i nodi gestiti a cui potresti avere accesso in altri account o regioni, è invece possibile accedere a un elenco di proprietà.

- Connettiti, avvia sessione terminale: connettiti al nodo utilizzando [AWS Systems Manager Session Manager](#).
- Strumenti
 - Visualizza il file system: sfoglia il contenuto della struttura di directory del nodo. Aggiungi, rinomina e rimuovi le directory. Taglia o copia e incolla file.
 - Visualizza i contatori delle prestazioni: visualizza le informazioni sulle prestazioni del nodo come l'utilizzo della CPU, il traffico di rete e altri tipi di utilizzo.
 - Processi gestiti: visualizza le informazioni sull'utilizzo delle risorse nel nodo. Avvia o arresta i processi sul nodo.
 - Gestisci utenti e gruppi: visualizza, aggiungi o elimina account utente e gruppi di utenti sul nodo.
 - Comando Execute run: [AWS Systems Manager Run Command](#) da utilizzare per gestire la configurazione del nodo. Run Command utilizza i documenti di [Systems Manager](#) per eseguire modifiche su richiesta, ad esempio l'aggiornamento delle applicazioni o l'esecuzione di script di shell Linux e comandi Windows PowerShell .
 - Nodi di patch: utilizza la funzionalità Applica patch ora di [AWS Systems Manager Patch Manager](#) per eseguire un'operazione di applicazione di patch on-demand sul nodo dalla console.

 Note

Le attività precedenti possono essere avviate anche dal menu Strumenti nella barra di navigazione a sinistra.

- Impostazioni dei nodi
 - Aggiungere tag: applica coppie chiave-valore del tag aggiuntive al nodo.
 - Reimposta la password utente del nodo: imposta una nuova password per un utente specificato sul nodo.
 - Modifica il ruolo IAM: modifica il ruolo IAM associato al nodo. Creare un nuovo ruolo IAM da collegare al nodo.

Effettuare il download o l'esportazione di un report sui nodi gestiti

È possibile utilizzare la funzionalità Esplora i nodi di Systems Manager per visualizzare elenchi filtrati o non filtrati di nodi gestiti per l' AWS organizzazione o l'account nella console di Systems Manager. Nei casi in cui si desidera visualizzare i dati offline o elaborarli in un'altra applicazione, è possibile salvare il rapporto come file CSV o JSON.

A seconda delle dimensioni del report, viene richiesto di scaricarlo sul computer locale o esportarlo in un bucket Amazon S3. I report vengono salvati nei bucket S3 solo in formato CSV.

Per scaricare o esportare un report sul nodo gestito

1. Apri la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel riquadro di navigazione, scegli Esplora nodi.
3. (Facoltativo) Segui i passaggi indicati in [Scelta di una visualizzazione dei filtri per i riepiloghi dei nodi gestiti](#) per rifinire l'elenco dei nodi gestiti visualizzati per l'organizzazione o l'account.
4. Scegli Segnala
().
)
5. Se viene visualizzata la finestra di dialogo Scarica rapporto, esegui le seguenti operazioni:
 - a. In Nome file, immettere un nome per il file. È consigliabile specificare un nome che rappresenti l'ambito del rapporto, ad esempio all-organization-nodes o ec2-instances-out-of-date-agent.

- b. Per Colonne incluse, specificare se includere le colonne per tutti i dettagli dei nodi disponibili o solo quelle selezionate per la visualizzazione corrente.

 Tip

Per informazioni sulla gestione delle colonne nella visualizzazione del rapporto, consulta [Gestione del contenuto e dell'aspetto dei report dei nodi](#).

- c. Per Formato file, seleziona CSV o JSON, a seconda di come usi il file.
- d. Per Intestazione del foglio di calcolo, per includere una riga di intestazioni di colonna in un file CSV, seleziona Includi nomi di righe di colonne.
- e. Scegli Scarica.

Il rapporto viene salvato nella posizione di download predefinita in base alle impostazioni del browser.

- 6. Se viene visualizzata la finestra di dialogo Esporta in Amazon S3, procedi come segue:

- a. Per l'URI S3, inserisci l'URI del bucket in cui esportare il report.

 Tip

Per visualizzare un elenco dei bucket nella console Amazon S3, scegli Visualizza. Scegli Sfoglia S3 per selezionarlo da un elenco di bucket nell'account.

- b. Come metodo di autorizzazione, va specificato il ruolo di servizio da utilizzare per fornire le autorizzazioni per l'esportazione del report nel bucket.

Se viene scelto di lasciare che Systems Manager crei il ruolo per conto dell'utente, fornirà tutte le autorizzazioni e le dichiarazioni di fiducia necessarie per l'operazione.

Per utilizzare o creare il proprio ruolo, questo deve includere le autorizzazioni e le dichiarazioni di attendibilità richieste. Per ulteriori informazioni sulla creazione di questo ruolo, consulta [Creazione di un ruolo di servizio personalizzato per esportare i report di diagnosi in S3](#).

- c. Seleziona Invia.

Creazione di un ruolo di servizio personalizzato per esportare i report di diagnosi in S3

Quando si visualizzano elenchi filtrati o non filtrati di nodi gestiti per l'organizzazione o l'account AWS nella pagina Esplora nodi di Systems Manager, è possibile esportare l'elenco come report in un bucket Amazon S3 come file CSV.

A tale scopo, è necessario specificare un ruolo di servizio con le autorizzazioni e la policy di fiducia necessarie per l'operazione. È possibile selezionare l'opzione per cui Systems Manager creerà il ruolo durante il processo di download del report. In alternativa, è possibile creare autonomamente il ruolo e la relativa policy richiesta.

Per creare un ruolo di servizio personalizzato per l'esportazione dei report di diagnosi in S3

1. Segui i passaggi descritti in [Creazione di policy tramite l'editor JSON](#) nella Guida per l'utente IAM.
- Utilizza quanto segue per il contenuto della politica, assicurandoti di sostituirlo *placeholder values* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketAcl",
        "s3:ListBucket",

```

```

        "s3:PutLifecycleConfiguration",
        "s3:GetLifecycleConfiguration"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "111122223333"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ssm:ListNodes"
    ],
    "Resource": "*"
}
]
}

```

- Assegna un nome alla policy per riconoscerla facilmente nel passaggio successivo.
2. Segui i passaggi descritti in [Creazione di un ruolo IAM tramite una policy di fiducia personalizzata \(console\)](#) nella Guida per l'utente IAM.
- Per il passaggio 4, inserisci la seguente politica di attendibilità, assicurandoti di sostituirla *placeholder values* con le tue informazioni.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SSMAssumeRole",
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                }
            }
        }
    ]
}

```

```

    }
  }
]
}

```

3. Per il passaggio 10, scegli Passaggio 2: aggiungi autorizzazioni e seleziona il nome della policy creata nella fase precedente.

Dopo aver creato il ruolo, è possibile selezionarlo seguendo i passaggi in [Effettuare il download o l'esportazione di un report sui nodi gestiti](#).

Gestione del contenuto e dell'aspetto dei report dei nodi

È possibile utilizzare la funzionalità **Esplora i nodi** di Systems Manager per visualizzare elenchi filtrati o non filtrati di nodi gestiti per AWS l'organizzazione o l'account nella console di Systems Manager. È possibile scegliere tra più di una dozzina di campi da includere negli elenchi di nodi, ad esempio ID nodo, Nome del sistema operativo, Regione e altro ancora. È anche possibile riordinare le colonne degli elenchi e dei report e modificare la modalità di visualizzazione dell'elenco nella console.

Per gestire il contenuto e l'aspetto dei report del nodo

1. Apri la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel riquadro di navigazione, scegli **Esplora nodi**.
3. Nell'area **Nodi** scegli l'icona a ingranaggio delle preferenze
().
4. Nella finestra di dialogo **Preferenze** procedi come segue:
 - a. Per **Dimensioni della pagina**, scegli quante righe includere in ogni display di visualizzazione della console, 10, 25 o 50.
 - b. Per **A capo automatico**, seleziona la casella per visualizzare tutto il contenuto di una cella nella larghezza di colonna disponibile.
 - c. Per **Righe alternate** seleziona la casella per visualizzare righe alternate di sfondi chiari e ombreggiati.
 - d. Per **Seleziona contenuto visibile** procedi come segue:
 - Attiva o disattiva le singole colonne per la visualizzazione dell'elenco e i report.

- Per modificare l'ordine delle colonne, tieni premuta la maniglia



del nome di una colonna e trascinala verso l'alto o verso il basso nell'elenco.

5. Scegli Conferma.

Just-in-time accesso al nodo tramite Systems Manager

Systems Manager consente di migliorare la sicurezza dei nodi supportando l'accesso just-in-time. Just-in-time l'accesso ai nodi consente agli utenti di richiedere un accesso temporaneo e limitato nel tempo ai nodi, che è possibile approvare solo quando l'accesso è realmente necessario. Ciò elimina la necessità di fornire un accesso duraturo ai nodi gestiti dalle policy IAM. Inoltre, Systems Manager fornisce la registrazione delle sessioni RDP sui Windows Server nodi per aiutarvi a soddisfare i requisiti di conformità, eseguire l'analisi delle cause principali e altro ancora. Per utilizzare l'accesso al nodo just-in-time, è necessario configurare la console unificata Systems Manager.

Con l'accesso ai nodi just-in-time, puoi creare policy IAM granulari per garantire che solo gli utenti autorizzati possano inviare richieste di accesso ai tuoi nodi. Quindi crei policy di approvazione che definiscono le approvazioni necessarie per la connessione ai tuoi nodi. Per l'accesso immediato ai nodi just-in-time, sono disponibili politiche di approvazione automatica e di approvazione manuale. Una policy di approvazione automatica definisce a quali nodi gli utenti possono connettersi automaticamente. Le policy di approvazione manuale definiscono il numero e i livelli di approvazioni manuali da fornire per accedere ai nodi specificati. Inoltre, puoi creare una policy di negazione dell'accesso. Una policy di negazione dell'accesso impedisce esplicitamente l'approvazione automatica delle richieste di accesso ai nodi specificati. Una politica di negazione dell'accesso si applica a tutti gli account di un'organizzazione. AWS Organizations Auto-approval e le politiche di approvazione manuale si applicano solo al Account AWS Regioni AWS luogo in cui vengono create.

Quando un utente tenta di connettersi a un nodo, gli viene richiesto di inserire un motivo per l'accesso al nodo. Quindi, vengono valutate le tue policy di approvazione. A seconda delle policy, gli utenti o si connettono automaticamente al nodo di destinazione o Systems Manager crea automaticamente una richiesta di approvazione manuale per conto del richiedente. Gli approvatori specificati nella policy di approvazione manuale applicabile al nodo ricevono quindi una notifica della richiesta di accesso e possono approvare o rifiutare la richiesta. Gli approvatori e i richiedenti possono ricevere notifiche via e-mail o tramite Amazon Q Developer nell'integrazione delle applicazioni di chat con Slack o Microsoft Teams. Systems Manager concede l'accesso ai nodi richiesti, solo quando gli approvatori specificati forniscono tutte le approvazioni richieste. Una volta ricevute tutte le approvazioni richieste,

L'utente può avviare tutte le sessioni sul nodo necessarie per la durata della finestra di accesso specificata nella policy di approvazione. Systems Manager non termina automaticamente le sessioni di accesso ai nodi just-in-time. Come best practice, è necessario specificare i valori per la durata massima della sessione e le preferenze del timeout della sessione inattiva. Queste preferenze impediscono agli utenti di rimanere connessi ai nodi oltre la finestra di accesso approvata.

Si consiglia di utilizzare una combinazione di policy di approvazione per aiutarti a proteggere i nodi con dati più critici, consentendo al contempo agli utenti di connettersi a nodi meno critici senza alcun intervento. Ad esempio, puoi richiedere approvazioni manuali per le richieste di accesso ai nodi del database e approvare automaticamente le sessioni per i nodi di livello di presentazione non persistenti.

Systems Manager supporta l'accesso ai nodi just-in-time per gli utenti federati con IAM Identity Center o IAM. Quando un utente federato invia una richiesta di accesso, specifica il nodo di destinazione e il motivo per cui è necessario connettersi al nodo. Systems Manager confronta l'identità dell'utente con i parametri definiti nelle policy di approvazione dell'organizzazione. Quando vengono soddisfatte le condizioni della policy di approvazione automatica o gli approvatori forniscono manualmente le approvazioni, il richiedente è in grado di connettersi al nodo di destinazione. Quando un utente tenta di connettersi a un nodo approvato, Systems Manager crea e utilizza un token temporaneo per stabilire la sessione.

Poiché il servizio di Systems Manager gestisce l'autenticazione per le richieste di accesso e la creazione di sessioni, non è necessario utilizzare le policy IAM per gestire l'accesso ai nodi. Utilizzando l'accesso ai nodi just-in-time, Systems Manager aiuta l'organizzazione ad avvicinarsi ai privilegi zero, poiché è sufficiente consentire agli utenti di creare richieste di accesso, invece di consentire loro di avviare sessioni con autorizzazioni persistenti per i nodi. Per aiutarti a soddisfare i requisiti di conformità, Systems Manager mantiene tutte le richieste di accesso per un anno. Systems Manager emette anche EventBridge eventi per l'accesso immediato ai nodi in caso di richieste di accesso non riuscite e aggiornamenti di stato per le richieste di accesso per le approvazioni manuali. Per ulteriori informazioni, consultare [Monitoraggio degli eventi di Systems Manager con Amazon EventBridge](#).

Argomenti

- [Configurazione dell'accesso just-in-time con Systems Manager](#)
- [Avvia una sessione di accesso ai nodi just-in-time](#)
- [Gestire le richieste di accesso just-in-time](#)
- [Passaggio all'accesso ai nodi just-in-time da Session Manager](#)

- [Disabilitare l'accesso just-in-time con Systems Manager](#)
- [Just-in-time domande frequenti sull'accesso ai nodi](#)

Configurazione dell'accesso just-in-time con Systems Manager

Configurazione dell'accesso ai nodi just-in-time con molteplici passaggi inclusi in Systems Manager. Per prima cosa, scegli le destinazioni in cui configurare l'accesso ai nodi just-in-time. Gli obiettivi sono costituiti da unità AWS Organizations organizzative (OU) e Regioni AWS. Per impostazione predefinita, gli stessi obiettivi scelti durante la configurazione della console unificata di Systems Manager vengono selezionati per l'accesso ai nodi just-in-time. È possibile scegliere di impostare l'accesso ai nodi just-in-time per tutte le stesse destinazioni o per un sottoinsieme delle destinazioni specificate durante la configurazione della console unificata di Systems Manager. L'aggiunta di nuove destinazioni che non sono state selezionate durante la configurazione della console unificata di Systems Manager non è supportata.

Successivamente, creerai policy di approvazione per determinare quando le connessioni dei nodi richiedono l'approvazione manuale e vengono approvate automaticamente. Le policy di approvazione sono gestite da ogni account dell'organizzazione. Puoi anche condividere una policy dell'account amministratore delegato per negare esplicitamente l'approvazione automatica delle connessioni a nodi specifici.

Note

La configurazione dell'accesso ai nodi just-in-time non influisce sulle policy o preferenze IAM esistenti per le quali hai configurato Session Manager. Devi rimuovere l'autorizzazione all'azione `StartSession` API dalle tue policy IAM per assicurarti che venga utilizzato solo l'accesso just-in-time ai nodi quando gli utenti tentano di connettersi ai tuoi nodi. Dopo aver configurato l'accesso ai nodi just-in-time, ti consigliamo di testare le policy di approvazione con un sottoinsieme di utenti e nodi per verificare che le policy funzionino come desiderato, prima di rimuovere le autorizzazioni a Session Manager.

Supporto dell'autenticazione

Tieni presente i seguenti dettagli sul supporto di autenticazione utilizzato per l'accesso ai nodi just-in-time:

- Just-in-time l'accesso al nodo non supporta il tipo di Sign-On autenticazione singola quando ci si connette alle Windows Server istanze con Remote Desktop.
- Sono supportate solo Servizio di token di sicurezza AWS (AWS STS) credenziali di sicurezza AssumeRole temporanee. Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente IAM:
- [Credenziali di sicurezza temporanee in IAM](#)
- [Confronto AWS STS delle credenziali](#)
- [Richiesta di credenziali di sicurezza temporanee](#)

Le seguenti policy IAM descrivono le autorizzazioni necessarie per amministrare e consentire agli utenti di creare richieste di accesso ai nodi just-in-time, ai nodi con Systems Manager. Dopo aver verificato di disporre delle autorizzazioni necessarie per utilizzare l'accesso ai nodi just-in-time con Systems Manager, è possibile continuare il processo di configurazione. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Policy IAM per abilitare l'accesso ai nodi just-in-time

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "QuickSetupConfigurationManagers",
      "Effect": "Allow",
      "Action": [
        "ssm-quicksetup:CreateConfigurationManager",
        "ssm-quicksetup>DeleteConfigurationManager",
        "ssm-quicksetup:GetConfiguration",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:GetServiceSettings",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-quicksetup:ListConfigurations",
        "ssm-quicksetup:ListQuickSetupTypes",
        "ssm-quicksetup:ListTagsForResource",
        "ssm-quicksetup:TagResource",
        "ssm-quicksetup:UntagResource",
        "ssm-quicksetup:UpdateConfigurationDefinition",
        "ssm-quicksetup:UpdateConfigurationManager",

```

```

        "ssm-quicksetup:UpdateServiceSettings"
    ],
    "Resource": "*"
},
{
    "Sid": "QuickSetupDeployments",
    "Effect": "Allow",
    "Action": [
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:ListStackSets",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeOrganizationsAccess",
        "cloudformation:ActivateOrganizationsAccess",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackSetOperationResults",
        "cloudformation:DescribeStackEvents",
        "cloudformation:UntagResource",
        "ssm:DescribeAutomationExecutions",
        "ssm:GetAutomationExecution",
        "ssm:ListAssociations",
        "ssm:DescribeAssociation",
        "ssm:GetDocument",
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "ssm:GetOpsSummary",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAWSServiceAccessForOrganization",
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:CreatePolicy",
    ]
}

```

```

        "cloudformation:TagResource"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "cloudformation:RollbackStack",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation>DeleteStack"
    ],
    "Resource": [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-
JITNA*",
        "arn:aws:cloudformation:*:*:stack/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:type/resource/*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SSMQuickSetup"
    ]
},
{
    "Sid": "StackSetOperations",
    "Effect": "Allow",
    "Action": [
        "cloudformation:CreateStackSet",
        "cloudformation:UpdateStackSet",
        "cloudformation>DeleteStackSet",
        "cloudformation>DeleteStackInstances",
        "cloudformation:CreateStackInstances",
        "cloudformation:StopStackSetOperation"
    ],
    "Resource": [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-JITNA*",
        "arn:aws:cloudformation:*:*:type/resource/*",
        "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-
JITNA*:*"
    ]
},
{
    "Sid": "IamRolesMgmt",
    "Effect": "Allow",
    "Action": [
        "iam:CreateRole",
        "iam>DeleteRole",

```

```

        "iam:GetRole",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies"
    ],
    "Resource": [
        "arn:aws:iam::*:role/AWS-QuickSetup-JITNA*",
        "arn:aws:iam::*:role/service-role/AWS-QuickSetup-JITNA*"
    ]
},
{
    "Sid": "IamPassRole",
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": [
        "arn:aws:iam::*:role/AWS-QuickSetup-JITNA*",
        "arn:aws:iam::*:role/service-role/AWS-QuickSetup-JITNA*"
    ],
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": [
                "ssm.amazonaws.com",
                "ssm-quicksetup.amazonaws.com",
                "cloudformation.amazonaws.com"
            ]
        }
    }
},
{
    "Sid": "SSMAutomationExecution",
    "Effect": "Allow",
    "Action": "ssm:StartAutomationExecution",
    "Resource": [
        "arn:aws:ssm:us-east-1:111122223333:document/AWS-EnableExplorer",
        "arn:aws:ssm:us-east-1:111122223333:automation-execution/*"
    ]
},
{
    "Sid": "SSMAssociationPermissions",
    "Effect": "Allow",

```

```

        "Action": [
            "ssm:DeleteAssociation",
            "ssm:CreateAssociation",
            "ssm:StartAssociationsOnce"
        ],
        "Resource": "arn:aws:ssm:us-east-1:111122223333:association/*"
    },
    {
        "Sid": "SSMResourceDataSync",
        "Effect": "Allow",
        "Action": [
            "ssm:CreateResourceDataSync",
            "ssm:UpdateResourceDataSync"
        ],
        "Resource": "arn:aws:ssm:us-east-1:111122223333:resource-data-sync/
AWS-QuickSetup-*"
    },
    {
        "Sid": "ListResourceDataSync",
        "Effect": "Allow",
        "Action": [
            "ssm:ListResourceDataSync"
        ],
        "Resource": "*"
    },
    {
        "Sid": "CreateServiceLinkedRoles",
        "Effect": "Allow",
        "Action": [
            "iam:CreateServiceLinkedRole"
        ],
        "Condition": {
            "StringEquals": {
                "iam:AWSServiceName": [
                    "accountdiscovery.ssm.amazonaws.com",
                    "ssm.amazonaws.com",
                    "ssm-quicksetup.amazonaws.com",
                    "stacksets.cloudformation.amazonaws.com"
                ]
            }
        },
        "Resource": "*"
    },
    {

```



```

        "Sid": "CreateStackSetsServiceLinkedRole",
        "Effect": "Allow",
        "Action": [
            "iam:CreateServiceLinkedRole"
        ],
        "Resource": "arn:aws:iam::*:role/aws-
service-role/stacksets.cloudformation.amazonaws.com/
AWSServiceRoleForCloudFormationStackSetsOrgAdmin"
    },
    {
        "Sid": "AllowSsmJitnaPoliciesCrudOperations",
        "Effect": "Allow",
        "Action": [
            "ssm:CreateDocument",
            "ssm:UpdateDocument",
            "ssm:UpdateDocumentDefaultVersion",
            "ssm:GetDocument",
            "ssm:DescribeDocument",
            "ssm>DeleteDocument"
        ],
        "Resource": [
            "arn:aws:ssm:us-east-1:111122223333:document/SSM-
JustInTimeAccessDenyAccessOrgPolicy"
        ],
        "Condition": {
            "StringEquals": {
                "ssm:DocumentType": [
                    "AutoApprovalPolicy"
                ]
            }
        }
    },
    {
        "Sid": "AllowAccessRequestOpsItemOperations",
        "Effect": "Allow",
        "Action": [
            "ssm:GetOpsItem",
            "ssm:DescribeOpsItems",
            "ssm:GetOpsSummary",
            "ssm>DeleteOpsItem",
            "ssm:ListOpsItemEvents"
        ],
        "Resource": "*"
    },

```

```

    {
      "Sid": "IdentityCenterPermissions",
      "Effect": "Allow",
      "Action": [
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations",
        "identitystore:GetUserId",
        "identitystore:DescribeUser",
        "identitystore:DescribeGroup",
        "identitystore:ListGroupMembershipsForMember"
      ],
      "Resource": "*"
    }
  ]
}

```

Policy IAM per configurare l'accesso ai nodi just-in-time

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSsmJitnaPoliciesCrudOperations",
      "Effect": "Allow",
      "Action": [
        "ssm:CreateDocument",
        "ssm:UpdateDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm>DeleteDocument"
      ],
      "Resource": [
        "arn:aws:ssm:us-east-1:111122223333:document/*"
      ],
      "Condition": {
        "StringEquals": {
          "ssm:DocumentType": [
            "ManualApprovalPolicy",
            "AutoApprovalPolicy"
          ]
        }
      }
    }
  ]
}

```

```

        ]
      }
    }
  },
  {
    "Sid": "AllowSsmJitnaPoliciesListOperations",
    "Effect": "Allow",
    "Action": [
      "ssm:ListDocuments",
      "ssm:ListDocumentVersions"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::111122223333:role/SSM-
JustInTimeAccessTokenRole",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": [
          "justintimeaccess.ssm.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid": "AllowAccessRequestOpsItemOperations",
    "Effect": "Allow",
    "Action": [
      "ssm:GetOpsItem",
      "ssm:DescribeOpsItems",
      "ssm:GetOpsSummary",
      "ssm>DeleteOpsItem",
      "ssm:ListOpsItemEvents"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AllowSessionManagerPreferencesOperation",
    "Effect": "Allow",
    "Action": [
      "ssm:CreateDocument",
      "ssm:GetDocument",

```

```

        "ssm:DescribeDocument",
        "ssm:UpdateDocument",
        "ssm>DeleteDocument"
    ],
    "Resource": "arn:aws:ssm:us-east-1:111122223333:document/SSM-
SessionManagerRunShell",
    "Condition": {
        "StringEquals": {
            "ssm:DocumentType": "Session"
        }
    }
},
{
    "Sid": "AllowSessionManagerOperations",
    "Effect": "Allow",
    "Action": [
        "ssm:DescribeSessions",
        "ssm:GetConnectionStatus",
        "ssm:TerminateSession"
    ],
    "Resource": "*"
},
{
    "Sid": "AllowRDPConnectionRecordingOperations",
    "Effect": "Allow",
    "Action": [
        "ssm-guiconnect:UpdateConnectionRecordingPreferences",
        "ssm-guiconnect:GetConnectionRecordingPreferences",
        "ssm-guiconnect>DeleteConnectionRecordingPreferences"
    ],
    "Resource": "*"
},
{
    "Sid": "AllowRDPConnectionRecordingKmsOperation",
    "Effect": "Allow",
    "Action": [
        "kms:CreateGrant"
    ],
    "Resource": "arn:aws:kms:us-east-1:111122223333:key/*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged":
"true"
        }
    },

```

```

        "StringLike": {
            "kms:ViaService": "ssm-guiconnect.*.amazonaws.com"
        },
        "Bool": {
            "aws:ViaAWSService": "true"
        }
    },
    {
        "Sid": "AllowFleetManagerOperations",
        "Effect": "Allow",
        "Action": [
            "ssm-guiconnect:GetConnection",
            "ssm-guiconnect:ListConnections"
        ],
        "Resource": "*"
    },
    {
        "Sid": "SNSTopicManagement",
        "Effect": "Allow",
        "Action": [
            "sns:CreateTopic",
            "sns:SetTopicAttributes"
        ],
        "Resource": [
            "arn:aws:sns:us-east-1:111122223333:SSM-JITNA*"
        ]
    },
    {
        "Sid": "SNSListTopics",
        "Effect": "Allow",
        "Action": [
            "sns:ListTopics"
        ],
        "Resource": "*"
    },
    {
        "Sid": "EventBridgeRuleManagement",
        "Effect": "Allow",
        "Action": [
            "events:PutRule",
            "events:PutTargets"
        ],
        "Resource": [

```

```

        "arn:aws:events:us-east-1::rule/SSM-JITNA*"
    ],
    },
    {
        "Sid": "ChatbotSlackManagement",
        "Effect": "Allow",
        "Action": [
            "chatbot:CreateSlackChannelConfiguration",
            "chatbot:UpdateSlackChannelConfiguration",
            "chatbot:DescribeSlackChannelConfigurations",
            "chatbot:DescribeSlackWorkspaces",
            "chatbot>DeleteSlackChannelConfiguration",
            "chatbot:RedeemSlackOAuthCode",
            "chatbot>DeleteSlackWorkspaceAuthorization",
            "chatbot:GetSlackOAuthParameters"
        ],
        "Resource": "*"
    },
    {
        "Sid": "ChatbotTeamsManagement",
        "Effect": "Allow",
        "Action": [
            "chatbot:ListMicrosoftTeamsChannelConfigurations",
            "chatbot:CreateMicrosoftTeamsChannelConfiguration",
            "chatbot:UpdateMicrosoftTeamsChannelConfiguration",
            "chatbot:ListMicrosoftTeamsConfiguredTeams",
            "chatbot>DeleteMicrosoftTeamsChannelConfiguration",
            "chatbot:RedeemMicrosoftTeamsOAuthCode",
            "chatbot>DeleteMicrosoftTeamsConfiguredTeam",
            "chatbot:GetMicrosoftTeamsOAuthParameters",
            "chatbot:TagResource"
        ],
        "Resource": "*"
    },
    {
        "Sid": "SSMEmailSettings",
        "Effect": "Allow",
        "Action": [
            "ssm:UpdateServiceSetting",
            "ssm:GetServiceSetting"
        ],
        "Resource": [
            "arn:aws:ssm:us-east-1:111122223333:servicesetting/ssm/access-
request/email-role-mapping",

```

```

        "arn:aws:ssm:us-east-1:111122223333:servicesetting/ssm/access-
request/enabled-email-notifications"
    ],
    {
        "Sid": "AllowViewingJitnaCloudWatchMetrics",
        "Effect": "Allow",
        "Action": [
            "cloudwatch:GetMetricData",
            "cloudwatch:GetMetricStatistics",
            "cloudwatch:ListMetrics"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "cloudwatch:namespace": "AWS/SSM/JustInTimeAccess"
            }
        }
    },
    {
        "Sid": "QuickSetupConfigurationManagers",
        "Effect": "Allow",
        "Action": [
            "ssm-quicksetup:ListConfigurationManagers",
            "ssm-quicksetup:ListConfigurations",
            "ssm-quicksetup:ListQuickSetupTypes",
            "ssm-quicksetup:GetConfiguration",
            "ssm-quicksetup:GetConfigurationManager"
        ],
        "Resource": "*"
    },
    {
        "Sid": "QuickSetupDeployments",
        "Effect": "Allow",
        "Action": [
            "cloudformation:ListStacks",
            "cloudformation:DescribeStacks",
            "organizations:DescribeOrganization",
            "organizations:ListDelegatedAdministrators"
        ],
        "Resource": "*"
    },
    {
        "Sid": "ManualPolicy",

```

```

        "Effect": "Allow",
        "Action": [
            "sso:DescribeRegisteredRegions",
            "ssm:GetServiceSetting",
            "iam:ListRoles"
        ],
        "Resource": "*"
    },
    {
        "Sid": "SessionPreference",
        "Effect": "Allow",
        "Action": [
            "s3:ListAllMyBuckets"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AllowIamListForKMS",
        "Effect": "Allow",
        "Action": [
            "iam:ListUsers"
        ],
        "Resource": "arn:aws:iam::111122223333:user/*"
    },
    {
        "Sid": "KMSPermission",
        "Effect": "Allow",
        "Action": [
            "kms:TagResource",
            "kms:ListAliases",
            "kms:CreateAlias"
        ],
        "Resource": "*"
    },
    {
        "Sid": "KMSCreateKey",
        "Effect": "Allow",
        "Action": [
            "kms:CreateKey"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {

```



```

        "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged":
"true"
    },
    "ForAllValues:StringEquals": {
        "aws:TagKeys": [
            "SystemsManagerJustInTimeNodeAccessManaged"
        ]
    }
},
{
    "Sid": "AllowIamRoleForChatbotAction",
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": "arn:aws:iam::111122223333:role/role name",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": [
                "chatbot.amazonaws.com"
            ]
        }
    }
},
{
    "Sid": "AllowIamServiceRoleForChat",
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "arn:aws:iam::111122223333:role/aws-service-role/
management.chatbot.amazonaws.com/AWSServiceRoleForAWSChatbot"
},
{
    "Sid": "CloudWatchLogs",
    "Effect": "Allow",
    "Action": [
        "logs:DescribeLogGroups"
    ],
    "Resource": "arn:aws:logs*:111122223333:log-group::log-stream:"
},
{
    "Sid": "IdentityStorePermissions",

```

```

        "Effect": "Allow",
        "Action": [
            "sso:ListDirectoryAssociations",
            "identitystore:GetUserId",
            "sso-directory:SearchUsers",
            "sso-directory:SearchGroups",
            "identitystore:DescribeGroup",
            "identitystore:DescribeUser"
        ],
        "Resource": "*"
    }
]
}

```

Policy IAM per approvatori di richieste di accesso

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAccessRequestDescriptions",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeOpsItems",
                "ssm:GetOpsSummary",
                "ssm:ListOpsItemEvents"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowGetSpecificAccessRequest",
            "Effect": "Allow",
            "Action": [
                "ssm:GetOpsItem"
            ],
            "Resource": "arn:aws:ssm:us-east-1:111122223333:opsitem/*"
        },
        {
            "Sid": "AllowApprovalRejectionSignal",
            "Effect": "Allow",

```

```

        "Action": [
            "ssm:SendAutomationSignal"
        ],
        "Resource": "arn:aws:ssm:*:*:automation-execution/*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged":
"true"
            }
        }
    },
    {
        "Sid": "QuickSetupConfigurationManagers",
        "Effect": "Allow",
        "Action": [
            "ssm-quicksetup:ListConfigurationManagers",
            "ssm-quicksetup:ListConfigurations",
            "ssm-quicksetup:GetConfigurationManager",
            "ssm-quicksetup:ListQuickSetupTypes",
            "ssm-quicksetup:GetConfiguration"
        ],
        "Resource": "*"
    },
    {
        "Sid": "QuickSetupDeployments",
        "Effect": "Allow",
        "Action": [
            "cloudformation:ListStacks",
            "cloudformation:DescribeStacks",
            "organizations:DescribeOrganization",
            "organizations:ListDelegatedAdministrators"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AllowSsmJitnaPoliciesCrudOperations",
        "Effect": "Allow",
        "Action": [
            "ssm:GetDocument",
            "ssm:DescribeDocument"
        ],
        "Resource": [
            "arn:aws:ssm:us-east-1:111122223333:document/*"
        ],
    },

```

```

        "Condition": {
            "StringEquals": {
                "ssm:DocumentType": [
                    "ManualApprovalPolicy",
                    "AutoApprovalPolicy"
                ]
            }
        },
        {
            "Sid": "AllowSsmJitnaPoliciesListOperations",
            "Effect": "Allow",
            "Action": [
                "ssm:ListDocuments",
                "ssm:ListDocumentVersions"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IDCPermissions",
            "Effect": "Allow",
            "Action": [
                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
                "identitystore:GetUserId",
                "identitystore:DescribeUser",
                "identitystore:DescribeGroup",
                "identitystore:ListGroupMembershipsForMember"
            ],
            "Resource": "*"
        }
    ]
}

```

Policy IAM per gli utenti con accesso ai nodi just-in-time

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {

```

```

        "Sid": "AllowJITNAOperations",
        "Effect": "Allow",
        "Action": [
            "ssm:StartAccessRequest",
            "ssm:GetAccessToken"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AllowOpsItemCreationAndRetrieval",
        "Effect": "Allow",
        "Action": [
            "ssm:CreateOpsItem",
            "ssm:GetOpsItem"
        ],
        "Resource": "arn:aws:ssm:*:*:opsitem/*"
    },
    {
        "Sid": "AllowListAccessRequests",
        "Effect": "Allow",
        "Action": [
            "ssm:DescribeOpsItems",
            "ssm:GetOpsSummary",
            "ssm:ListOpsItemEvents",
            "ssm:DescribeSessions"
        ],
        "Resource": "*"
    },
    {
        "Sid": "RequestManualApprovals",
        "Action": "ssm:StartAutomationExecution",
        "Effect": "Allow",
        "Resource": "arn:aws:ssm:*:*:document/*",
        "Condition": {
            "StringEquals": {
                "ssm:DocumentType": "ManualApprovalPolicy"
            }
        }
    },
    {
        "Sid": "StartManualApprovalsAutomationExecution",
        "Effect": "Allow",
        "Action": "ssm:StartAutomationExecution",
        "Resource": "arn:aws:ssm:*:*:automation-execution/*"
    }

```

```

    },
    {
      "Sid": "CancelAccessRequestManualApproval",
      "Effect": "Allow",
      "Action": "ssm:StopAutomationExecution",
      "Resource": "arn:aws:ssm:*:*:automation-execution/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged":
"true"
        }
      }
    },
    {
      "Sid": "DescribeEC2Instances",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:GetPasswordData"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowListSSMManagedNodesAndTags",
      "Effect": "Allow",
      "Action": [
        "ssm:DescribeInstanceInformation",
        "ssm:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QuickSetupConfigurationManagers",
      "Effect": "Allow",
      "Action": [
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurations",
        "ssm-quicksetup:ListQuickSetupTypes",
        "ssm-quicksetup:GetConfiguration"
      ],
      "Resource": "*"
    }
  ],

```

```

{
  "Sid": "AllowSessionManagerOperations",
  "Effect": "Allow",
  "Action": [
    "ssm:DescribeSessions",
    "ssm:GetConnectionStatus"
  ],
  "Resource": "*"
},
{
  "Sid": "AllowRDPOperations",
  "Effect": "Allow",
  "Action": [
    "ssm-guiconnect:ListConnections",
    "ssm:GetConnectionStatus"
  ],
  "Resource": "*"
},
{
  "Sid": "QuickSetupDeployments",
  "Effect": "Allow",
  "Action": [
    "cloudformation:ListStacks",
    "cloudformation:DescribeStacks",
    "organizations:DescribeOrganization",
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource": "*"
},
{
  "Sid": "AllowSsmJitnaPoliciesReadOnly",
  "Effect": "Allow",
  "Action": [
    "ssm:GetDocument",
    "ssm:DescribeDocument"
  ],
  "Resource": [
    "arn:aws:ssm:*:111122223333:document/*"
  ],
  "Condition": {
    "StringEquals": {
      "ssm:DocumentType": [
        "ManualApprovalPolicy",
        "AutoApprovalPolicy"
      ]
    }
  }
}

```

```

        ]
    }
}
},
{
    "Sid": "AllowSsmJitnaPoliciesListOperations",
    "Effect": "Allow",
    "Action": [
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions"
    ],
    "Resource": "*"
},
{
    "Sid": "ExploreNodes",
    "Effect": "Allow",
    "Action": [
        "ssm:ListNodesSummary",
        "ssm:ListNodes",
        "ssm:DescribeInstanceProperties"
    ],
    "Resource": "*"
},
{
    "Sid": "IdentityStorePermissions",
    "Effect": "Allow",
    "Action": [
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations",
        "identitystore:GetUserId",
        "identitystore:DescribeUser",
        "identitystore:DescribeGroup"
    ],
    "Resource": "*"
}
]
}

```

Note

Per limitare l'accesso alle operazioni API che creano, aggiornano o eliminano le policy di approvazione, utilizza la chiave di condizione `ssm:DocumentType` per la

AutoApprovalPolicy i tipi di documento ManualApprovalPolicy . Le operazioni dell'API StartAccessRequest e GetAccessToken non supportano le seguenti chiavi di contesto globali:

- aws:SourceVpc
- aws:SourceVpce
- aws:VpcSourceIp
- aws:UserAgent
- aws:MultiFactorAuthPresent

Per ulteriori informazioni sulle chiavi di contesto di condizione per Systems Manager, consulta [Chiavi di condizione per AWS Systems Manager](#) nelle Informazioni di riferimento sull'autorizzazione del servizio.

La procedura seguente descrive come completare il primo passaggio di configurazione per l'accesso ai nodi just-in-time.

Per configurare l'accesso ai nodi just-in-time

1. Accedi all'account amministratore delegato di Systems Manager della tua organizzazione.
2. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
3. Seleziona l'accesso al Just-in-time nodo nel pannello di navigazione.
4. Seleziona Abilita la nuova esperienza.
5. Scegli le Regioni in cui desideri abilitare l'accesso ai nodi just-in-time. Per impostazione predefinita, le stesse Regioni scelte durante la configurazione della console unificata di Systems Manager vengono selezionate per l'accesso ai nodi just-in-time. La scelta di nuove Regioni non selezionate durante la configurazione della console unificata di Systems Manager non è supportata.
6. Seleziona Abilita accesso ai nodi just-in-time.

L'utilizzo dell'accesso ai nodi just-in-time per 30 giorni dopo l'abilitazione della funzionalità è gratuito. Dopo il periodo di prova di 30 giorni, l'utilizzo dell'accesso al nodo just-in-time è a pagamento. Per ulteriori informazioni, consulta [AWS Systems Manager Prezzi](#).

Crea policy di approvazione per i tuoi nodi

Le policy di approvazione definiscono le approvazioni di cui gli utenti hanno bisogno per accedere a un nodo. Poiché l'accesso ai nodi just-in-time elimina la necessità di autorizzazioni di lunga data ai nodi tramite le policy IAM, è necessario creare policy di approvazione per consentire l'accesso ai nodi. Se non esistono policy di approvazione applicabili a un nodo, gli utenti non possono richiederne l'accesso.

Nell'accesso al nodo just-in-time, esistono tre tipi di policy. I tipi di policy sono approvazione automatica, negazione dell'accesso e approvazione manuale.

Just-in-time tipi di policy di accesso ai nodi

- Una policy di approvazione automatica definisce a quali nodi gli utenti possono connettersi automaticamente.
- Le policy di approvazione manuale definiscono il numero e i livelli di approvazioni manuali da fornire per accedere ai nodi specificati.
- Una policy di negazione dell'accesso impedisce esplicitamente l'approvazione automatica delle richieste di accesso ai nodi specificati.

Una politica di negazione dell'accesso si applica a tutti gli account di un' AWS Organizations organizzazione. Ad esempio, potresti negare esplicitamente le approvazioni automatiche per il tuo gruppo ai nodi contrassegnati con la chiave. `Production Auto-approval` e le politiche di approvazione manuale si applicano solo al luogo in Regioni AWS cui vengono Account AWS create. Ciascun account membro nella tua organizzazione gestisce le proprie policy di approvazione. Le policy di approvazione sono valutate nell'ordine seguente:

1. Deny-access
2. Auto-approval
3. Manuale

Sebbene tu possa avere solo una policy di negazione dell'accesso per organizzazione e una di approvazione automatica per account e Regione, probabilmente avrai numerose policy di approvazione manuale in un account. Durante la valutazione delle policy di approvazione manuale, l'accesso ai nodi just-in-time favorisce sempre la policy più specifica per un nodo. Le policy di approvazione manuale sono valutate nell'ordine seguente:

1. Destinazione specifica dei tag
2. Tutte le destinazioni del nodo

Ad esempio, hai un nodo etichettato con la chiave `Demo`. Nello stesso account, hai una policy di approvazione manuale che si rivolge a tutti i nodi e richiede un'approvazione da un livello. Hai anche una policy di approvazione manuale che richiede due approvazioni da due livelli per i nodi contrassegnati con la chiave `Demo`. Systems Manager applica la policy che ha come destinazione il tag `Demo` al nodo, poiché è più specifica di quella che è destinata a tutti i nodi. Ciò ti consente di creare una politica generale per tutti i nodi del tuo account, assicurando che gli utenti possano inviare richieste di accesso e consentirti di creare politiche più granulari se necessario.

A seconda dell'organizzazione, potrebbero essere applicati più tag ai nodi. In questo scenario, se a un nodo si applicano più policy di approvazione manuale, le richieste di accesso hanno esito negativo. Ad esempio, un nodo viene contrassegnato con il `Database` e le chiavi `Production`. Nello stesso account, hai una policy di approvazione manuale che si applica ai nodi contrassegnati con la chiave `Production` e un'altra policy di approvazione manuale che si applica ai nodi contrassegnati con la chiave `Database`. Ciò si traduce in un conflitto per il nodo etichettato con entrambe le chiavi e le richieste di accesso hanno esito negativo. Systems Manager reindirizza l'utente alla richiesta non riuscita. Qui è possibile visualizzare i dettagli sulle policy e sui tag in conflitto, in modo che sia possibile apportare le modifiche necessarie, se si hanno le autorizzazioni richieste. In caso contrario, è possibile notificare a un collega della propria organizzazione le autorizzazioni necessarie per modificare le policy. I conflitti di policy che comportano richieste di accesso non riuscite generano EventBridge eventi che consentono la flessibilità nella creazione dei propri flussi di lavoro di risposta. Inoltre, Systems Manager invia notifiche via e-mail per i conflitti di policy che comportano richieste di accesso non riuscite ai destinatari specificati. Per ulteriori informazioni sulla configurazione delle notifiche via e-mail per i conflitti delle policy, consulta [Configura le notifiche per le richieste di accesso just-in-time](#).

In una policy di negazione dell'accesso, utilizzi il linguaggio delle policy Cedar per definire a quali nodi gli utenti non possono connettersi automaticamente nella tua organizzazione. Questa policy viene creata e condivisa dall'account amministratore delegato dell'organizzazione. La policy di negazione dell'accesso sostituisce tutte le politiche di approvazione automatica. È possibile avere una sola policy di negazione dell'accesso per organizzazione.

In una policy di approvazione automatica, si utilizza il linguaggio di policy Cedar per definire quali utenti possono connettersi automaticamente ai nodi specificati senza approvazione manuale. La durata di accesso per una richiesta di accesso approvata automaticamente è di un'ora. Questo valore

non può essere modificato. Puoi avere una sola policy di approvazione automatica per account e regione.

In una policy di approvazione manuale, si specifica la durata dell'accesso, il numero di livelli di approvazione richiesti, il numero di approvatori richiesti per livello e i nodi a cui questi possono approvare le richieste di accesso just-in-time. La durata dell'accesso per una policy di approvazione manuale deve essere compresa tra 1 e 336 ore. Se si specificano più livelli di approvazione, le approvazioni per il processo della richiesta di accesso vengono elaborate un livello alla volta. Ciò significa che tutte le approvazioni necessarie per un livello devono essere fornite prima che il processo di approvazione passi ai livelli successivi. Se si specificano più tag in una policy di approvazione manuale, questi vengono valutati come istruzioni `or` e non come istruzioni `and`. Ad esempio, se si crea una policy di approvazione manuale che include i tag `Application`, `Web` e `Test`, la policy si applica a qualsiasi nodo contrassegnato con una di queste chiavi. La policy non si applica solo ai nodi etichettati con tutte e tre le chiavi.

Ti consigliamo di utilizzare una combinazione di policy manuali con la tua policy di approvazione automatica per proteggere i nodi con dati più critici, consentendo al contempo agli utenti di connettersi ai nodi meno critici senza alcun intervento. Ad esempio, puoi richiedere approvazioni manuali per le richieste di accesso ai nodi del database e approvare automaticamente le sessioni per i nodi di livello di presentazione non persistenti.

Le procedure seguenti descrivono come creare policy di approvazione per l'accesso ai nodi just-in-time.

Argomenti

- [Crea policy di approvazione manuale per l'accesso ai nodi just-in-time](#)
- [Struttura dell'istruzione e operatori integrati per le policy di approvazione automatica e di negazione dell'accesso](#)
- [Crea una politica di approvazione automatica per l'accesso tempestivo ai nodi](#)
- [Crea una policy di negazione dell'accesso per l'accesso ai nodi just-in-time](#)
- [Crea policy di approvazione per l'accesso ai nodi just-in-time con Amazon Q](#)

Crea policy di approvazione manuale per l'accesso ai nodi just-in-time

Le seguenti procedure descrivono come creare policy di approvazione manuale. Systems Manager consente di creare fino a 50 policy di approvazione Account AWS manuali per mano Regione AWS.

Per creare una policy di approvazione manuale

1. Aprire la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Seleziona Gestisci l'accesso al nodo nel riquadro di navigazione.
3. Nella sezione Dettagli della policy del passaggio Crea policy di approvazione manuale, inserisci un nome e una descrizione per la policy di approvazione.
4. Inserisci un valore per la durata dell'accesso. Si tratta della quantità massima di tempo con cui un utente può avviare sessioni su un nodo dopo l'approvazione di una richiesta di accesso. Il valore deve essere compreso tra 1 e 336 ore.
5. Nella sezione Destinazioni del nodo, inserisci le coppie chiave-valore dei tag associate ai nodi a cui desideri applicare la policy. Se nessuno dei tag specificati nella policy è associato a un nodo, la policy non viene applicata al nodo.
6. Nella sezione Approvatori delle richieste di accesso, inserisci gli utenti o i gruppi a cui desideri approvare le richieste di accesso alle destinazioni dei nodi indicati nella policy. Gli approvatori delle richieste di accesso possono essere utenti e gruppi di IAM Identity Center o ruoli IAM. Puoi specificare fino a cinque approvatori per livello e fino a cinque livelli di approvatori.
7. Seleziona Crea policy di approvazione manuale.

Struttura dell'istruzione e operatori integrati per le policy di approvazione automatica e di negazione dell'accesso

La tabella seguente mostra la struttura delle policy di approvazione automatica e negazione dell'accesso.

Componente	Sintassi
effetto	permit forbid
scope	(principal, action, resource)
clausola condizionale	<pre>when { <i>principal or resource</i> has <i>attribute</i> <i>name</i> };</pre>

Componenti della policy

Una policy di approvazione automatica o di negazione dell'accesso contiene i seguenti componenti:

- **Effetto:** sia `permit` (consenti) che `forbid` (nega) l'accesso.
- **Ambito:** i principali, le azioni e le risorse a cui si applica l'effetto. È possibile lasciare indefinito l'ambito in Cedar non identificando principali, azioni o risorse specifici. In questo caso, la policy si applica a tutti i possibili principali, operazioni e risorse. Per l'accesso al nodo just-in-time, `action` è sempre `AWS::SSM::Action::"getTokenForInstanceAccess"`.
- **Clausola condizionale:** il contesto in cui si applica l'effetto.

Commenti

Puoi includere commenti nelle tue policy. I commenti sono definiti come una riga che inizia con `//` e termina con un carattere a capo.

Di seguito viene illustrato un esempio di commenti in una policy.

```
// Allows users in the Engineering group from the Platform org to automatically connect
// to nodes tagged with Engineering and Production keys.
permit (
  principal in AWS::IdentityStore::Group::"d4q81745-r081-7079-d789-14da1EXAMPLE",
  action == AWS::SSM::Action::"getTokenForInstanceAccess",
  resource
)
when {
  principal has organization && resource.hasTag("Engineering") &&
  resource.hasTag("Production") && principal.organization == "Platform"
};
```

Clausole multiple

Puoi utilizzare più clausole condizionali in un'istruzione di policy tramite l'operatore `&&`.

```
// Allow access if node has tag where the tag key is Environment
// & tag value is Development

permit(principal, action == AWS::SSM::getTokenForInstanceAccess, resource)
when {
  resource.hasTag("Environment") &&
```

```
resource.getTag("Environment") == "Development"
};
```

Caratteri riservati

L'esempio seguente mostra come scrivere una policy, se una proprietà di contesto utilizza un : (punto e virgola), che è un carattere riservato nel linguaggio delle policy.

```
permit (
    principal,
    action == AWS::SSM::Action::"getTokenForInstanceAccess",
    resource
)
when {
    principal has employeeNumber && principal.employeeNumber like "E-1*" &&
    resource.hasTag("Purpose") && resource.getTag("Purpose") == "Testing"
}
```

Per ulteriori esempi, consulta [Esempio di istruzioni di policy](#).

Just-in-time schema di accesso ai nodi

Di seguito è riportato lo schema Cedar per l'accesso al nodo just-in-time.

```
namespace AWS::EC2 {
    entity Instance tags String;
}

namespace AWS::IdentityStore {
    entity Group;

    entity User in [Group] {
        employeeNumber?: String,
        costCenter?: String,
        organization?: String,
        division?: String,
    };
}

namespace AWS::IAM {
```

```

    entity Role;

    type AuthorizationContext = {
        principalTags: PrincipalTags,
    };

    entity PrincipalTags tags String;
}

namespace AWS::SSM {

    entity ManagedInstance tags String;

    action "getTokenForInstanceAccess" appliesTo {
        principal: [AWS::IdentityStore::User],
        resource: [AWS::EC2::Instance, AWS::SSM::ManagedInstance],
        context: {
            "iam": AWS::IAM::AuthorizationContext
        }
    };
}

```

Built-in operators

Quando si crea il contesto di una policy di approvazione automatica o di negazione dell'accesso utilizzando varie condizioni, è possibile utilizzare l'operatore `&&`, per aggiungere ulteriori condizioni. Esistono anche molti altri operatori integrati che puoi utilizzare per aggiungere ulteriore forza espressiva alle condizioni della tua policy. La tabella seguente contiene tutti gli operatori integrati come riferimento.

Operatore	Tipi e sovraccarichi	Description
!	Booleano → Booleano	Logico no.
==	qualsiasi → qualsiasi	Uguaglianza. Funziona su argomenti di qualsiasi tipo, anche se i tipi non corrispondono. I valori di tipi diversi non sono mai uguali tra loro.

Operatore	Tipi e sovraccarichi	Description
<code>!=</code>	qualsiasi → qualsiasi	Disuguaglianza; l'esatto contrario di uguaglianza (vedi sopra).
<code><</code>	(long, long) → Booleano	Intero lungo minore di.
<code><=</code>	(long, long) → Booleano	Intero lungo minore di o uguale a.
<code>></code>	(long, long) → Booleano	Intero lungo maggiore di.
<code>>=</code>	(long, long) → Booleano	Intero lungo maggiore di o uguale a.
<code>in</code>	(entity, entity) → Booleano	Appartenenza alla gerarchia (riflessiva: A in A è sempre vero).
	(entity, set(entity)) → Booleano	Appartenenza alla gerarchia : A in [B, C, ...] è vero se (A e B) (A in C) ... errore, se l'insieme contiene una non entità.
<code>&&</code>	(Boolean, Boolean) → Booleano	Logico e (short-circuiting).
<code> </code>	(Boolean, Boolean) → Booleano	Logico o (short-circuiting).
<code>.exists()</code>	entità → Booleano	Esistenza dell'entità.

Operatore	Tipi e sovraccarichi	Description
has	(entity, attribute) → Booleano	L'operatore. Infix e <code>has f</code> verifica se il record o l'entità e ha un'associazione per l'attributo f. Restituisce <code>false</code> , se e non esiste o se e esiste, ma non ha l'attributo f. Gli attributi possono essere espressi come identificatori o stringhe letterali.
like	(string, string) → Booleano	L'operatore. Infix <code>t like p</code> verifica se il testo t corrisponde allo schema p, che può includere caratteri jolly *, che corrispondono a 0 o a più caratteri di qualche carattere . Per abbinare un carattere asterisco letterale int, puoi usare la speciale sequenza <code>*</code> di caratteri con escape in. p
.hasTag()	(entity, string) → Booleano	Verifica se all'entità è applicato il tag specificato.
.getTag()	(entity, string) → Booleano	Restituisce il valore della chiave del tag specificata.
.contains()	(set, any) → Booleano	Appartenenza al set (se B è un elemento di A).
.containsAll()	(set, set) → Booleano	Verifica se la serie A contiene tutti gli elementi della serie B.
.containsAny()	(set, set) → Booleano	Verifica se la serie A contiene tutti gli elementi della serie B.

Esempio di istruzioni di policy

Di seguito sono mostrati esempi di istruzioni della policy.

```
// Users assuming IAM roles with a principal tag of "Elevated" can automatically access
nodes tagged with the "Environment" key when the value equals "prod"
permit(principal, action == AWS::SSM::getTokenForInstanceAccess, resource)
when {
    // Verify IAM role principal tag
    context.iam.principalTags.getTag("AccessLevel") == "Elevated" &&

    // Verify the node has a tag with "Environment" tag key and a tag value of "prod"
    resource.hasTag("Environment") &&
    resource.getTag("Environment") == "prod"
};
```

```
// Identity Center users in the "Contractor" division can automatically access nodes
tagged with the "Environment" key when the value equals "dev"
permit(principal, action == AWS::SSM::getTokenForInstanceAccess, resource)
when {
    // Verify that the user is part of the "Contractor" division
    principal.division == "Contractor" &&

    // Verify the node has a tag with "Environment" tag key and a tag value of "dev"
    resource.hasTag("Environment") &&
    resource.getTag("Environment") == "dev"
};
```

```
// Identity Center users in a specified group can automatically access nodes tagged
with the "Environment" key when the value equals "Production"
permit(principal in AWS::IdentityStore::Group::"d4q81745-r081-7079-d789-14da1EXAMPLE",
    action == AWS::SSM::getTokenForInstanceAccess,
    resource)
when {
    resource.hasTag("Environment") &&
    resource.getTag("Environment") == "Production"
};
```

Crea una politica di approvazione automatica per l'accesso tempestivo ai nodi

Auto-approval le politiche utilizzano il linguaggio di policy Cedar per definire quali utenti possono connettersi automaticamente ai nodi specificati senza approvazione manuale. Una policy di

approvazione automatica contiene molteplici istruzioni di `permit`, che specificano il `principal` e la `resource`. Ogni istruzione include una clausola `when`, che definisce le condizioni per l'approvazione automatica.

Di seguito è riportato un esempio di policy di approvazione automatica.

```
permit (
    principal in AWS::IdentityStore::Group::"e8c17310-e011-7089-d989-10da1EXAMPLE",
    action == AWS::SSM::Action::"getTokenForInstanceAccess",
    resource
)
when {
    principal has costCenter && resource.hasTag("CostCenter") && principal.costCenter
    == resource.getTag("CostCenter")
};

permit (
    principal in AWS::IdentityStore::Group::"d4q81745-r081-7079-d789-14da1EXAMPLE",
    action == AWS::SSM::Action::"getTokenForInstanceAccess",
    resource
)
when {
    principal has organization && resource.hasTag("Engineering") &&
    resource.hasTag("Production") && principal.organization == "Platform"
};

permit (
    principal,
    action == AWS::SSM::Action::"getTokenForInstanceAccess",
    resource
)
when {
    principal has employeeNumber && principal.employeeNumber like "E-1*" &&
    resource.hasTag("Purpose") && resource.getTag("Purpose") == "Testing"
};
```

Le procedure seguenti descrivono come creare policy di approvazione automatica per l'accesso ai nodi just-in-time. La durata di accesso per una richiesta di accesso approvata automaticamente è di un'ora. Questo valore non può essere modificato. Puoi avere solo una politica di approvazione automatica per Account AWS volta. Regione AWS Per maggiori informazioni su come creare le istruzioni della policy, consulta [Struttura dell'istruzione e operatori integrati per le policy di approvazione automatica e di negazione dell'accesso](#).

Per creare una policy di approvazione automatica

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Seleziona Gestisci l'accesso al nodo nel riquadro di navigazione.
3. Nella scheda Policy di approvazione, seleziona Crea una policy di approvazione automatica.
4. Inserisci la tua istruzione della policy per quella con l'approvazione automatica nella sezione Istruzione per la policy. Puoi utilizzare le istruzioni di esempio fornite per creare la tua policy.
5. Seleziona Crea policy di approvazione automatica.

Crea una policy di negazione dell'accesso per l'accesso ai nodi just-in-time

Deny-access le politiche utilizzano il linguaggio di policy Cedar per definire a quali nodi gli utenti non possono connettersi automaticamente senza l'approvazione manuale. Una policy di negazione dell'accesso contiene molteplici istruzioni di `forbid`, che specificano il `principal` e la `resource`. Ogni istruzione include una clausola `when`, che definisce le condizioni per l'approvazione automatica del diniego.

Di seguito è riportato un esempio di policy di negazione dell'accesso.

```
forbid (
  principal in AWS::IdentityStore::Group::"e8c17310-e011-7089-d989-10da1EXAMPLE",
  action == AWS::SSM::Action::"getTokenForInstanceAccess",
  resource
)
when {
  resource.hasTag("Environment") && resource.getTag("Environment") == "Production"
};

forbid (
  principal,
  action == AWS::SSM::Action::"getTokenForInstanceAccess",
  resource
)
when {
  principal has division && principal.division != "Finance" &&
  resource.hasTag("DataClassification") && resource.getTag("DataClassification") ==
  "Financial"
};
```

```
forbid (
    principal,
    action == AWS::SSM::Action::"getTokenForInstanceAccess",
    resource
)
when {

    principal has employeeNumber && principal.employeeNumber like "TEMP-*" &&
    resource.hasTag("Criticality") && resource.getTag("Criticality") == "High"
};
```

Le procedure seguenti descrivono come creare una policy di negazione dell'accesso per l'accesso ai nodi just-in-time. Per maggiori informazioni su come creare le istruzioni della policy, consulta [Struttura dell'istruzione e operatori integrati per le policy di approvazione automatica e di negazione dell'accesso](#).

Note

Osservare le seguenti informazioni.

- È possibile creare policy di negazione dell'accesso, mentre si è connessi all'account di gestione AWS o a quello dell'amministratore delegato. È possibile avere una sola policy di negazione dell'accesso per organizzazione AWS Organizations .
- Just-in-time node access utilizza AWS Resource Access Manager (AWS RAM) per condividere la politica di negazione dell'accesso con gli account dei membri dell'organizzazione. Se desideri condividere la policy di negazione dell'accesso con gli account membri dell'organizzazione, devi abilitare la condivisione delle risorse dall'account di gestione della tua organizzazione. Per ulteriori informazioni, consulta [Abilitare la condivisione delle risorse con AWS Organizations](#) nella Guida per l'utente di AWS RAM .

Per creare una policy di negazione dell'accesso

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Seleziona Gestisci l'accesso al nodo nel riquadro di navigazione.
3. Nella scheda Policy di approvazione, seleziona Crea una policy di negazione dell'accesso.

4. Inserisci l'istruzione per la policy di negazione dell'accesso nella sezione Istruzione per la policy. Puoi utilizzare le istruzioni di esempio fornite per creare la tua policy.
5. Seleziona Crea policy di negazione dell'accesso.

Crea policy di approvazione per l'accesso ai nodi just-in-time con Amazon Q

L'uso di Amazon Q Developer per la riga di comando fornisce indicazioni e supporto su vari aspetti dello sviluppo del software. Per un accesso ai nodi just-in-time, Amazon Q ti aiuta a creare policy di approvazione generando e aggiornando il relativo codice, analizzando le istruzioni delle policy e altro ancora. Le seguenti informazioni descrivono come creare policy di approvazione utilizzando Amazon Q per la riga di comando.

Identificazione del caso d'uso

Il primo passaggio nella creazione delle policy di approvazione consiste nella definizione chiara del caso d'uso. Ad esempio, nella tua organizzazione potresti voler approvare automaticamente le richieste di accesso ai nodi con un tag `Environment:Testing`. Potresti anche voler negare esplicitamente le approvazioni automatiche ai nodi con un tag `Environment:Production`, se l'ID di un dipendente inizia con TEMP. Per i nodi con un tag `Tier:Database`, potresti voler richiedere due livelli di approvazioni manuali.

In un determinato scenario, si potrebbe preferire una policy o una condizione piuttosto che un'altra. Pertanto, si consiglia di definire in modo chiaro i comportamenti della policy e le istruzioni più adatte al tuo caso d'uso e alle tue preferenze.

Configurazione dell'ambiente di sviluppo

Installa Amazon Q per la riga di comando dove desideri sviluppare le tue policy di approvazione. Per informazioni sull'installazione di Amazon Q per la riga di comando, consulta [Installazione di Amazon Q per la riga di comando](#) nella Guida per l'utente di Amazon Q Developer.

Consigliamo inoltre di installare il server MCP per la AWS documentazione. Questo server MCP collega Amazon Q per la riga di comando alle risorse di documentazione più recenti. Per informazioni sull'utilizzo di MCP con Amazon Q per la riga di comando, consulta [Utilizzare MCP con Amazon Q Developer](#) nella Guida per l'utente di Amazon Q Developer.

Per ulteriori informazioni sul server AWS Documentation MCP, vedere [AWS Documentation MCP Server](#) sul sito Web. GitHub

Installa e configura il AWS CLI se non l'hai già fatto. Per informazioni, consulta [Installazione o aggiornamento della versione più recente del AWS CLI](#).

Sviluppa il contenuto della policy di approvazione

Con l'identificazione del caso d'uso e la configurazione dell'ambiente, puoi sviluppare il contenuto per le policy. Il caso d'uso e le preferenze determinano in gran parte il caso d'uso e le istruzioni utilizzate.

Se non sei sicuro come utilizzare una determinata policy o hai bisogno di ulteriori informazioni sul suo schema, consulta [Crea policy di approvazione per i tuoi nodi](#) e gli argomenti successivi. Questi argomenti spiegano in dettaglio come vengono valutate le policy e forniscono istruzioni di esempi funzionanti.

Le seguenti procedure descrivono come creare policy di approvazione utilizzando Amazon Q per la riga di comando.

Note

Amazon Q Developer utilizza l'IA generativa. Potrebbe essere necessario verificare le risposte. Consulta la [Policy sull'IA AWS responsabile](#).

Per creare una policy di approvazione utilizzando Amazon Q per la riga di comando

1. Apri il tuo terminale e avvia una sessione con Amazon Q.

```
$ q chat
```

2. Inserisci un prompt e descrivi il tipo di istruzione di policy che desideri creare. Ad esempio, utilizzando lo scenario precedente per una policy di approvazione, è possibile inserire il seguente prompt:

```
Create a Cedar policy statement that allows a principal to use the
"getTokenForInstanceAccess" action for a resource
that has a tag key "Environment" and tag value of "Testing". Use the following
example statement for reference to verify the syntax.
```

```
permit (
  principal in AWS::IdentityStore::Group::"e8c17310-e011-7089-d989-10da1EXAMPLE",
  action == AWS::SSM::Action::"getTokenForInstanceAccess",
```



```
    resource
  )
  when {
    principal has organization && resource.hasTag("Engineering") &&
    resource.hasTag("Production") && principal.organization == "Platform"
  };
```

The Cedar policy statement you create must be valid. Validate the Cedar statement using the AWS documentation provided for just-in-time node access policy statement structure and make sure you abide by the schema.

3. L'immissione di questo prompt di esempio ha prodotto il seguente risultato:

Based on the AWS documentation for Cedar policy statements and the examples provided, I'll create a valid Cedar policy statement that allows a principal to use the "getTokenForInstanceAccess" action for resources with the tag key "Environment" and tag value "Testing".

Here's the Cedar policy statement:

```
permit (
  principal,
  action == AWS::SSM::Action::"getTokenForInstanceAccess",
  resource
)
when {
  resource.hasTag("Environment") &&
  resource.getTag("Environment") == "Testing"
};
```

This policy statement:

1. Uses the permit effect to allow access
2. Applies to any principal (since no specific principal is defined)
3. Specifically targets the "getTokenForInstanceAccess" action
4. Applies to resources that have a tag with key "Environment" and value "Testing"
5. Uses the proper syntax for the condition clause with the hasTag() and getTag() operators

The statement follows the Cedar policy language structure as documented in the AWS Systems Manager documentation for just-in-time node access policies.

4. Per convalidare la sintassi, incolla l'istruzione della policy in un nuovo file Cedar. È inoltre possibile convalidare la dichiarazione utilizzando lo [strumento di convalida delle politiche](#) Cedar sul sito Web della politica Cedar.
5. Dopo aver convalidato l'istruzione, salva il file Cedar.
6. Dal tuo terminale, esegui il seguente AWS CLI comando per creare un documento SSM utilizzando il contenuto della tua politica. Prima di utilizzare le politiche di approvazione in un ambiente di produzione, testate le politiche di approvazione con un sottoinsieme di identità e nodi in un e. Account AWS Regione AWS

Note

Per una policy di approvazione automatica, il nome del documento deve essere `SSM-JustInTimeAccessAutoApprovalPolicy`. Può esserci solo una politica di approvazione automatica per e. Account AWS Regione AWS Per una policy di negazione dell'accesso, il nome del documento deve essere `SSM-JustInTimeAccessDenyAccess0rgPolicy`. Può esserci una sola politica di negazione dell'accesso per AWS Organizations organizzazione e la politica deve essere creata nell'account amministratore delegato per Systems Manager. I vincoli di denominazione per le policy di approvazione manuale sono gli stessi degli altri documenti SSM. Per ulteriori informazioni, consulta [CreateDocument](#).

Linux & macOS

```
aws ssm create-document \  
  --content file://path/to/file/policyContent.cedar \  
  --name "SSM-JustInTimeAccessAutoApprovalPolicy" \  
  --document-type "AutoApproval"
```

Windows

```
aws ssm create-document ^  
  --content file://C:\path\to\file\policyContent.cedar ^  
  --name "SSM-JustInTimeAccessAutoApprovalPolicy" ^  
  --document-type "AutoApproval"
```

PowerShell

```
$cedar = Get-Content -Path "C:\path\to\file\policyContent.cedar" | Out-String
New-SSMDocument `
    -Content $cedar `
    -Name "SSM-JustInTimeAccessAutoApprovalPolicy" `
    -DocumentType "AutoApproval"
```

Aggiorna le preferenze della sessione di accesso ai nodi just-in-time

Con l'accesso ai nodi just-in-time, puoi specificare le preferenze generali di sessione e registrazione in ciascuna Account AWS organizzazione Regione AWS . In alternativa, puoi utilizzarlo CloudFormation StackSets per creare un documento sulle preferenze di sessione in più account e regioni per avere preferenze di sessione coerenti. Per informazioni sullo schema per i documenti relativi alle preferenze di sessione, consulta [Schema documento di sessione](#).

Per scopi di registrazione, consigliamo di utilizzare l'opzione di streaming con Amazon CloudWatch Logs. Questa funzionalità consente di inviare un flusso continuo di registri dei dati di sessione a CloudWatch Logs. I dettagli essenziali, come i comandi eseguiti da un utente in una sessione, l'ID dell'utente che ha eseguito i comandi e i timestamp con cui i dati della sessione vengono trasmessi in streaming ai CloudWatch log, sono inclusi nello streaming dei dati delle sessioni. Durante lo streaming dei dati delle sessioni, i log servono JSON-formatted ad aiutarti a integrarti con le tue soluzioni di registrazione esistenti.

Systems Manager non termina automaticamente le sessioni di accesso ai nodi just-in-time. Come best practice, è necessario specificare i valori per la durata massima della sessione e le impostazioni del timeout della sessione inattiva. L'utilizzo di queste impostazioni consente di impedire a un utente di rimanere connesso a un nodo più a lungo del periodo di tempo approvato in una richiesta di accesso. La procedura seguente descrive come aggiornare le preferenze di sessione per l'accesso ai nodi just-in-time.

Important

È necessario contrassegnare le AWS KMS chiavi utilizzate per la Session Manager crittografia e la registrazione RDP nell'accesso al nodo just-in-time con la chiave SystemsManagerJustInTimeNodeAccessManaged del tag e il valore del tag. true

Per ulteriori informazioni sull'applicazione di tag alle chiavi KMS, consulta [Tag in AWS KMS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Per aggiornare le preferenze della sessione

1. Apri la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Scegli Impostazioni nel pannello di navigazione.
3. Seleziona la scheda di accesso al Just-in-time nodo.
4. Nella sezione Preferenze di sessione, seleziona Modifica.
5. Aggiorna le preferenze generali e di registrazione in base alle esigenze e seleziona Salva.

Configura le notifiche per le richieste di accesso just-in-time

È possibile configurare Systems Manager per inviare notifiche, quando un utente crea una richiesta di accesso ai nodi just-in-time agli indirizzi e-mail o al client di chat per approvatori e richiedenti. La notifica contiene il motivo della richiesta di accesso fornita dal richiedente Account AWS Regione AWS, lo stato della richiesta e l'ID del nodo di destinazione. Attualmente, Systems Manager supporta i client Slack e Microsoft Teams tramite l'integrazione con Amazon Q Developer nelle applicazioni di chat. Quando si utilizzano le notifiche tramite client di chat, gli approvatori delle richieste di accesso possono interagire direttamente con le richieste di accesso. Ciò elimina la necessità di accedere alla console per intervenire sulle richieste di accesso.

Prima di iniziare

Prima di configurare un client di chat per le notifiche di accesso ai nodi just-in-time, tieni presente il seguente requisito:

- Se utilizzi i ruoli IAM per gestire le identità degli utenti nel tuo account, devi associare manualmente gli indirizzi e-mail degli approvatori o dei richiedenti a cui desideri inviare le notifiche con il ruolo associato. In caso contrario, i destinatari previsti non possono essere avvisati via e-mail.

Le seguenti procedure descrivono come configurare le notifiche per le richieste di accesso ai nodi just-in-time.

Per configurare un client di chat per le notifiche di accesso ai nodi just-in-time

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Scegli Impostazioni nel pannello di navigazione.
3. Seleziona la scheda di accesso al Just-in-time nodo.
4. Nella sezione Chat, seleziona Configura nuovo client.
5. Nel menu a discesa Seleziona il tipo di client, scegli il tipo di client di chat che desideri configurare e seleziona Avanti.
6. Ti viene richiesto di consentire ad Amazon Q Developer nelle applicazioni di chat di accedere al tuo client di chat. Seleziona Consenti.
7. Nella sezione Configura canale, inserisci le informazioni per il tuo canale client di chat e seleziona i tipi di notifiche che desideri ricevere.
8. Se stai configurando le notifiche Slack, invita "@Amazon Q" su ogni canale Slack in cui vengono configurate le notifiche.
9. Seleziona Configura canale.

Note

Per consentire le richieste di approving/rejecting accesso direttamente da un canale Slack, assicurati che il ruolo IAM configurato con il canale Slack disponga delle `ssm:SendAutomationSignal` autorizzazioni e disponga di una politica di fiducia che includa il chatbot:

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "chatbot.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
}
```

Per configurare le notifiche via e-mail per le notifiche di accesso ai nodi just-in-time

1. Apri la console all'indirizzo. AWS Systems Manager <https://console.aws.amazon.com/systems-manager/>
2. Scegli Impostazioni nel pannello di navigazione.
3. Seleziona la scheda di accesso al Just-in-time nodo.
4. Nella sezione E-mail, seleziona Modifica.
5. Seleziona Aggiungi e-mail, scegli il ruolo IAM a cui desideri associare manualmente gli indirizzi e-mail.
6. Inserisci un indirizzo e-mail nel campo Indirizzo e-mail. Ogni volta che viene creata una richiesta di accesso, che richiede l'approvazione del ruolo IAM specificato, gli indirizzi e-mail che associ al ruolo vengono notificati.
7. Seleziona Aggiungi indirizzo e-mail.

Registrazione delle connessioni RDP

Just-in-time l'accesso al nodo include la possibilità di registrare le connessioni RDP effettuate ai Windows Server nodi. La registrazione delle connessioni RDP richiede un bucket S3 e una chiave AWS Key Management Service (AWS KMS) gestita dal cliente. AWS KMS key Viene utilizzato per crittografare temporaneamente i dati di registrazione mentre vengono generati e archiviati nelle risorse di Systems Manager. La chiave gestita dal cliente deve essere una chiave simmetrica con un utilizzo chiave di crittografia e decrittografia. Puoi utilizzare sia una chiave multiregione per la tua organizzazione che creare una chiave gestita dal cliente in ogni Regione in cui hai abilitato l'accesso ai nodi just-in-time.

Se hai abilitato la crittografia KMS sul bucket S3, in cui memorizzi le registrazioni, devi fornire l'accesso alla chiave gestita dal cliente utilizzata per la crittografia del bucket al principale del servizio `ssm-guiconnect`. Questa chiave gestita dal cliente può essere diversa da quella specificata nelle impostazioni di registrazione, che devono includere la chiave per cui è richiesta l'autorizzazione `kms:CreateGrant` per stabilire connessioni.

Configurazione della crittografia del bucket S3 per le registrazioni RDP

Le registrazioni delle connessioni vengono archiviate nel bucket S3, che specifichi quando abiliti la registrazione RDP.

Se si utilizza una chiave KMS come meccanismo di crittografia predefinito per il bucket S3 (SSE-KMS), è necessario consentire al responsabile del `ssm-guiconnect` servizio l'accesso all'`kms:GenerateDataKey` azione sulla chiave. Ti consigliamo di utilizzare una chiave gestita dal cliente quando utilizzi la SSE-KMS crittografia con il bucket S3. In questo modo, è possibile aggiornare la policy della chiave associata per una chiave gestita dal cliente. Non puoi aggiornare le politiche chiave per. Chiavi gestite da AWS

Important

È necessario etichettare le AWS KMS chiavi utilizzate per la Session Manager crittografia e la registrazione RDP nell'accesso al nodo just-in-time con la chiave del tag `SystemsManagerJustInTimeNodeAccessManaged` e il valore del tag. `true`
Per ulteriori informazioni sull'applicazione di tag alle chiavi KMS, consulta [Tag in AWS KMS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Utilizza la seguente policy della chiave gestita dal cliente per consentire al servizio `ssm-guiconnect` di accedere alla chiave KMS per l'archiviazione S3. Per informazioni sull'aggiornamento di una chiave gestita dal cliente, consulta [Modifica una policy della chiave](#) nella Guida per gli sviluppatori AWS Key Management Service .

Sostituisci ognuna *example resource placeholder* con le tue informazioni:

- *account-id* rappresenta l'ID di Account AWS chi avvia la connessione.
- *region* rappresenta la posizione Regione AWS in cui si trova il bucket S3. (È possibile utilizzare *, se il bucket riceverà registrazioni da molteplici Regioni. Esempio: `s3.*.amazonaws.com`.)

Note

Puoi utilizzare `aws:SourceOrgID` nella policy invece di `aws:SourceAccount`, se l'account appartiene a un'organizzazione di AWS Organizations.

```
{
  "Sid": "Allow the GUI Connect service principal to access S3",
  "Effect": "Allow",
  "Principal": {
```

```
    "Service": "ssm-guiconnect.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "account-id"
    },
    "StringLike": {
      "kms:ViaService": "s3.region.amazonaws.com"
    }
  }
}
```

Configurazione delle autorizzazioni IAM per la registrazione delle connessioni RDP

Oltre alle autorizzazioni IAM richieste per l'accesso ai nodi just-in-time, l'utente o il ruolo utilizzato devono disporre delle seguenti autorizzazioni in base all'attività da eseguire.

Autorizzazioni per la configurazione della registrazione delle connessioni

Per configurare la registrazione delle connessioni RDP, sono necessarie le seguenti autorizzazioni:

- `ssm-guiconnect:UpdateConnectionRecordingPreferences`
- `ssm-guiconnect:GetConnectionRecordingPreferences`
- `ssm-guiconnect>DeleteConnectionRecordingPreferences`
- `kms:CreateGrant`

Autorizzazioni per l'avvio delle connessioni

Per effettuare connessioni RDP con accesso ai nodi just-in-time, sono necessarie le seguenti autorizzazioni:

- `ssm-guiconnect:CancelConnection`
- `ssm-guiconnect:GetConnection`
- `ssm-guiconnect:StartConnection`
- `kms:CreateGrant`

Prima di iniziare

Per archiviare le registrazioni delle connessioni, devi prima creare un bucket S3 e aggiungere la seguente policy di bucket. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Per informazioni sull'aggiunta di una policy di bucket, consulta [Aggiunta di una policy di bucket tramite l'utilizzo della console Amazon S3](#) nella Guida per l'utente di Amazon Simple Storage Service.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ConnectionRecording",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "ssm-guiconnect.amazonaws.com"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

Abilitazione e configurazione della registrazione delle connessioni RDP

La seguente procedura descrive come abilitare e configurare la registrazione delle connessioni RDP.

Per abilitare e configurare la registrazione delle connessioni RDP

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Scegli Impostazioni nel pannello di navigazione.
3. Seleziona la scheda di accesso al Just-in-time nodo.
4. Nella sezione Registrazione RDP, seleziona Abilita registrazione RDP.
5. Scegli il bucket S3 in cui caricare le registrazioni delle sessioni.
6. Scegli la chiave gestita dal cliente da utilizzare per crittografare temporaneamente i dati di registrazione, mentre vengono generati e archiviati nelle risorse di Systems Manager. (Può trattarsi di una chiave gestita dal cliente diversa da quella utilizzata per crittografare il bucket.)
7. Seleziona Salva.

Valori dello stato di registrazione della connessione RDP

I valori di stato validi per le registrazioni delle connessioni RPD includono i seguenti elementi:

- **Recording** - La connessione è in fase di registrazione;
- **Processing** - Il video viene elaborato dopo il termine della connessione;
- **Finished** - Stato terminale completato: il video di registrazione della connessione è stato eseguito correttamente e caricato nel bucket specificato;
- **Failed** - Stato terminale non eseguito. La registrazione della connessione non è eseguita.
- **ProcessingError**- Durante l'elaborazione video failures/errors si sono verificati uno o più elementi intermedi. Le probabili cause includono errori di dipendenza dal servizio o autorizzazioni mancanti a causa di una configurazione errata del bucket S3 specificato per l'archiviazione delle registrazioni. Il servizio continua a tentare l'elaborazione, quando la registrazione è in questo stato.

Note

ProcessingError può essere il risultato del mancato consenso del principale del servizio `ssm-guiconnect` a caricare oggetti nel bucket S3, dopo aver stabilito la connessione. Un'altra probabile causa è la mancanza delle autorizzazioni KMS sulla chiave KMS utilizzata per la crittografia del bucket S3.

Modifica delle destinazioni

Quando configuri l'accesso al nodo just-in-time, scegli le destinazioni in cui desideri configurare l'accesso al nodo just-in-time. Gli obiettivi sono costituiti da unità AWS Organizations organizzative (OU) e Regioni AWS. Per impostazione predefinita, gli stessi obiettivi scelti durante la configurazione della console unificata Systems Manager vengono selezionati per l'accesso al nodo just-in-time. È possibile scegliere di configurare l'accesso ai nodi just-in-time per tutte le stesse destinazioni o per un sottoinsieme delle destinazioni specificate durante la configurazione della console unificata Systems Manager. L'aggiunta di nuove destinazioni che non erano state selezionate durante la configurazione della console unificata Systems Manager non è supportata. È possibile modificare le destinazioni selezionate dopo aver configurato l'accesso al nodo just-in-time.

La procedura seguente descrive come modificare le destinazioni per l'accesso al nodo just-in-time.

Per modificare le destinazioni

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Scegli Impostazioni nel pannello di navigazione.
3. Seleziona la scheda di accesso al Just-in-time nodo.
4. Nella sezione Destinazioni, seleziona Modifica.
5. Seleziona le unità organizzative e le Regioni in cui desideri utilizzare l'accesso al nodo just-in-time.
6. Seleziona Salva.

Modificare i provider di identità

Per impostazione predefinita, l'accesso ai nodi just-in-time utilizza IAM per un provider di identità. Dopo aver abilitato l'accesso al nodo just-in-time, i clienti che utilizzano la console unificata con un'organizzazione possono modificare questa impostazione per utilizzare IAM Identity Center. Just-in-time l'accesso al nodo non supporta IAM Identity Center come provider di identità quando è configurato per un singolo account e regione.

La procedura seguente descrive come modificare il provider di identità per l'accesso ai nodi just-in-time.

Per modificare i provider di identità

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Scegli Impostazioni nel pannello di navigazione.
3. Seleziona la scheda di accesso al Just-in-time nodo.
4. Nella sezione Identità utente, seleziona Modifica.
5. Scegli AWS IAM Identity Center.
6. Seleziona Salva.

Avvia una sessione di accesso ai nodi just-in-time

Dopo aver abilitato e configurato l'accesso ai nodi just-in-time e le preferenze di sessione e notifica, gli utenti sono pronti per avviare sessioni di accesso ai nodi just-in-time. È possibile avviare le sessioni utilizzando l'accesso al nodo just-in-time dalla console di Systems Manager o AWS Command Line Interface utilizzando il Session Manager plug-in. Just-in-time le sessioni di accesso ai nodi possono essere avviate su nodi nello stesso account e nella stessa regione. Le procedure seguenti descrivono come avviare sessioni con accesso ai nodi just-in-time.

Note

Se in precedenza gli utenti utilizzavano Session Manager per connettersi ai nodi, è necessario rimuovere le autorizzazioni di Session Manager, ad esempio `ssm:StartSession`, dalle policy IAM, per avviare sessioni utilizzando l'accesso ai nodi just-in-time. In caso contrario, continueranno a utilizzare Session Manager durante la connessione ai nodi.

Per avviare una sessione con accesso ai nodi just-in-time utilizzando la console

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel riquadro di navigazione, seleziona Esplora nodi.
3. Scegli il nodo a cui desideri connetterti.
4. Nel menu a discesa Azioni, seleziona Connettiti.

Se le policy di approvazione della tua organizzazione non ti consentono di connetterti automaticamente al nodo, ti verrà richiesto di inviare una richiesta di accesso. Dopo aver compilato le informazioni richieste e inviato la richiesta di accesso, potrai avviare le sessioni sul nodo, una volta ricevute tutte le approvazioni richieste.

Per avviare una sessione con accesso istantaneo al nodo utilizzando AWS CLI

1. Esegui il comando seguente per avviare il flusso di lavoro della richiesta di accesso, assicurandoti di sostituirlo *placeholder values* con le tue informazioni.

```
aws ssm start-access-request \  
  --targets Key=InstanceIds,Values=i-02573cafcfEXAMPLE \  
  --reason "Troubleshooting networking performance issue"
```

A seconda delle policy di approvazione della tua organizzazione o verrai connesso automaticamente al nodo o verrà avviato il processo di approvazione manuale. Per le richieste che richiedono l'approvazione manuale, annota l'ID della richiesta di accesso restituita nella risposta.

2. Attendi che vengano fornite tutte le approvazioni richieste.
3. Dopo aver fornito tutte le approvazioni richieste, esegui il comando seguente per ottenere un token di accesso contenente credenziali temporanee. Sostituisci *placeholder values* con le informazioni appropriate.

```
aws ssm get-access-token \  
  --access-request-id oi-12345abcdef
```

Annota il token di accesso restituito nella risposta.

4. Esegui il comando seguente per utilizzare le credenziali temporanee in AWS CLI, assicurandoti di sostituirle *placeholder values* con le tue informazioni.

```
export AWS_SESSION_TOKEN=AQoDYXdzEJr...<remainder of session token>
```

5. Esegui il comando seguente per avviare una sessione sul nodo, assicurandoti di sostituirla *placeholder values* con le tue informazioni.

```
aws ssm start-session \  
  --target i-02573cafcfEXAMPLE
```

Consentire l'accesso alla rete locale nel browser

Se accedi alla console di Systems Manager tramite un'interfaccia Amazon VPC endpoint con DNS privato abilitato, il tuo browser potrebbe bloccare la schermata di richiesta di accesso. Quando il DNS privato è abilitato, l'endpoint di Systems Manager per te si Regione AWS risolve in un indirizzo IP privato nel tuo VPC. Poiché la console viene servita da un indirizzo pubblico, i browser considerano le richieste a quell'indirizzo IP privato come richieste di rete locale. I browser bloccano queste richieste a meno che tu non conceda alla console l'autorizzazione per effettuarle. Questo comportamento è noto come Local Network Access (LNA) e in precedenza era chiamato Private Network Access (PNA).

Quando il browser blocca queste richieste, viene visualizzato il seguente comportamento:

- Scegli **Connetti**, ma la schermata di richiesta di accesso non si apre e la connessione non riesce.
- Le richieste bloccate non vengono visualizzate nella cronologia AWS CloudTrail degli eventi, perché il browser le blocca prima che arrivino AWS.

Ti consigliamo di concedere l'autorizzazione solo per l'indirizzo della console, invece di disattivare le protezioni della rete locale per tutti i siti web. Per consentire richieste di accesso ai nodi just-in-time in questa configurazione, utilizza uno dei seguenti metodi:

- Per Chromium-based i browser, ad esempio Google Chrome e Microsoft Edge, aggiungi l'indirizzo della console all'elenco del browser dei siti autorizzati ad accedere alla rete locale. Negli ambienti gestiti, l'amministratore può configurarlo utilizzando le policy aziendali del browser, come la Microsoft Edge `LocalNetworkAccessAllowedForUrIs` policy. Se il browser ti chiede di consentire l'accesso alla rete locale quando scegli **Connetti**, scegli di consentire la richiesta.
- Per Mozilla Firefox, consenti l'accesso alla rete locale per l'indirizzo della console.

Per ulteriori informazioni sulla configurazione di queste autorizzazioni, consulta la documentazione del browser. In alternativa, è possibile accedere alla console da un percorso di rete in cui l'endpoint di Systems Manager si risolve in un indirizzo IP pubblico.

Important

Alcuni browser forniscono un'impostazione che disattiva le protezioni della rete locale per tutti i siti Web. Poiché questa impostazione riduce la protezione della rete locale, non la

consigliamo. Se la usi per testare questo comportamento, rivedi la modifica rispetto ai requisiti di sicurezza della tua organizzazione e ripristinala quando hai finito.

Gestire le richieste di accesso just-in-time

Per una maggiore visibilità all'interno dell'organizzazione, Systems Manager replica le richieste di accesso all'account amministratore delegato dell'organizzazione. Per aiutarti a soddisfare i requisiti di conformità, Systems Manager mantiene tutte le richieste di accesso per un anno. Negli argomenti seguenti viene descritto come gestire l'accesso ai nodi just-in-time. Queste informazioni sono destinate agli approvatori delle richieste di accesso. Prima di iniziare, ti consigliamo di rivedere le tue policy IAM e di assicurarti di disporre delle autorizzazioni necessarie per amministrare l'accesso ai nodi just-in-time. Per ulteriori informazioni, consulta [Configurazione dell'accesso just-in-time con Systems Manager](#).

Argomenti

- [Approvazione e rifiuto delle richieste di accesso ai nodi just-in-time](#)

Approvazione e rifiuto delle richieste di accesso ai nodi just-in-time

Gli approvatori delle richieste di accesso possono approvare o rifiutare le richieste di accesso ai nodi just-in-time dalla console unificata Systems Manager o utilizzando lo strumento da riga di comando preferito. Queste informazioni sono destinate agli approvatori delle richieste di accesso. Se non disponi delle autorizzazioni necessarie per approvare o rifiutare le richieste di accesso, contatta l'amministratore. Le procedure seguenti descrivono come creare policy di approvazione per l'accesso ai nodi just-in-time.

Per approvare o rifiutare le richieste di accesso ai nodi just-in-time utilizzando la console

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Seleziona Gestisci l'accesso al nodo nel riquadro di navigazione.
3. Seleziona la scheda Richieste di accesso.
4. Seleziona l'interruttore Richieste per me.
5. Selezionare la casella di controllo accanto alla richiesta di accesso che desideri approvare o rifiutare.

6. Seleziona Approva o Rifiuta.

Dopo aver approvato una richiesta di accesso, puoi revocare l'approvazione in qualsiasi momento selezionando Revoca.

Per approvare o rifiutare le richieste di accesso ai nodi just-in-time utilizzando la riga di comando

1. Annota l'ID della richiesta di accesso dalla notifica. Ad esempio, *oi-12345abcdef*.
2. Esegui il comando seguente per restituire i dettagli sul flusso di lavoro di approvazione delle richieste di accesso, assicurandoti di sostituirlo *placeholder values* con le tue informazioni.

```
aws ssm get-ops-item \  
  --ops-item-id oi-12345abcdef
```

Annota il valore `automationExecutionId` nel campo `/aws/accessrequest` per i `OperationalData`. Ad esempio, *9231944f-61c6-40be-8bce-8ee2bEXAMPLE*.

3. Esegui il comando seguente per approvare o rifiutare la richiesta di accesso. Utilizza il tipo di segnale `Approve`, per approvare la richiesta e `Deny` per rifiutarla. Assicurarsi di sostituire *placeholder values* con le proprie informazioni.

```
aws ssm send-automation-signal \  
  --automation-execution-id 9231944f-61c6-40be-8bce-8ee2bEXAMPLE \  
  --signal-type "Approve"
```

Passaggio all'accesso ai nodi just-in-time da Session Manager

Quando si abilita l'accesso al nodo just-in-time, Systems Manager non apporta alcuna modifica alle risorse esistenti per Session Manager. Ciò garantisce che non si verifichino interruzioni dell'ambiente esistente e che gli utenti possano continuare ad avviare le sessioni, mentre creano e convalidano le policy di approvazione. Quando vuoi testare le tue policy di approvazione, devi modificare le policy IAM esistenti per completare la transizione all'accesso ai nodi just-in-time. Ciò include l'aggiunta delle autorizzazioni necessarie per l'accesso ai nodi just-in-time alle identità e la rimozione dell'autorizzazione per il funzionamento dell'API `StartSession` per Session Manager. Consigliamo di testare le politiche di approvazione con un sottoinsieme di identità e nodi in un `aws` `Account` `AWS` `Regione` `AWS`

Per ulteriori informazioni sulle autorizzazioni richieste per l'accesso ai nodi just-in-time, consulta [Configurazione dell'accesso just-in-time con Systems Manager](#).

Per ulteriori informazioni sulla modifica e le autorizzazioni a un'identità IAM, consulta [Aggiunta e rimozione di autorizzazioni a identità IAM](#) nella Guida per l'utente IAM.

Di seguito viene descritto un metodo dettagliato per passare all'accesso ai nodi just-in-time da Session Manager.

Il passaggio da Session Manager all'accesso ai nodi just-in-time richiede un'attenta pianificazione e verifica per garantire una transizione fluida senza interruzioni delle operazioni. Le sezioni seguenti descrivono come è possibile completare questo processo.

Prerequisiti

Prima di iniziare, assicurati di aver completato le seguenti attività:

- Configura la console unificata di Systems Manager.
- Hai verificato di disporre delle autorizzazioni per modificare le policy IAM nel tuo account.
- Ha identificato tutte le policy e i ruoli IAM che attualmente concedono le autorizzazioni a Session Manager.
- Hai documentato l'attuale configurazione di Session Manager, incluse le preferenze di sessione e le impostazioni di registrazione.

Valutazione

Valuta l'ambiente attuale e delinea i comportamenti di approvazione desiderati completando le seguenti attività:

1. Effettua un inventario dei nodi: identifica tutti i nodi a cui accedono attualmente gli utenti tramite Session Manager.
2. Identifica i modelli di accesso degli utenti: documenta quali utenti o ruoli devono accedere a quali nodi e in quali circostanze.
3. Mappa i flussi di lavoro di approvazione: stabilisci chi deve approvare le richieste di accesso per diversi tipi di nodi.
4. Rivedi la strategia di etichettatura: assicurati che i nodi siano etichettati correttamente per supportare le politiche di approvazione pianificate.

5. Verifica le policy IAM esistenti: identifica tutte le policy che includono le autorizzazioni a Session Manager.

Pianificazione

Strategia graduale

Quando si passa da Session Manager all'accesso ai nodi just-in-time, si consiglia di utilizzare un approccio graduale come il seguente:

1. Fase 1: installazione e configurazione: abilita l'accesso ai nodi just-in-time senza modificare le autorizzazioni a Session Manager esistenti.
2. Fase 2: sviluppo delle policy: crea e testa le policy di approvazione per i nodi.
3. Fase 3: migrazione pilota: modifica di un piccolo gruppo di nodi e utenti o ruoli non critici da Session Manager all'accesso ai nodi just-in-time.
4. Fase 4: migrazione completa: migra gradualmente tutti i nodi, gli utenti o i ruoli restanti.

Considerazioni sulla cronologia

Considera i seguenti fattori quando crei la cronologia per passare da Session Manager all'accesso ai nodi just-in-time:

- Dedica del tempo alla formazione degli utenti e all'adattamento al nuovo flusso di lavoro di approvazione.
- Pianifica le migrazioni durante periodi di minore attività operativa.
- Includi il tempo di buffer per la risoluzione dei problemi e gli adattamenti.
- Pianifica un periodo di funzionamento parallelo in cui entrambi i sistemi siano disponibili.

Passaggi dell'implementazione

Fase 1: installazione e configurazione

1. Abilita l'accesso ai nodi just-in-time nella console Systems Manager. Per informazioni dettagliate sulle fasi, consulta [Configurazione dell'accesso just-in-time con Systems Manager](#).
2. Configura le preferenze di sessione per l'accesso ai nodi just-in-time, in modo che corrispondano alle impostazioni attuali di Session Manager. Per ulteriori informazioni, consulta [Aggiorna le preferenze della sessione di accesso ai nodi just-in-time](#).

3. Configura le preferenze di notifica per le richieste di accesso. Per ulteriori informazioni, consulta [Configura le notifiche per le richieste di accesso just-in-time](#).
4. Se utilizzi connessioni RDP ai nodi Windows Server, configura la registrazione RDP. Per ulteriori informazioni, consulta [Registrazione delle connessioni RDP](#).

Fase 2: sviluppo delle policy

1. Crea policy IAM per amministratori e utenti con accesso ai nodi just-in-time.
2. Sviluppa policy di approvazione basate sui tuoi requisiti di sicurezza e sui tuoi casi d'uso.
3. Testa le policy in un ambiente non di produzione per assicurarti che funzionino come previsto.

Fase 3: migrazione del progetto pilota

1. Seleziona un piccolo gruppo di utenti e nodi non critici per il progetto pilota.
2. Crea nuove policy IAM per gli utenti del progetto pilota che includono autorizzazioni di accesso ai nodi just-in-time.
3. Rimuovi le autorizzazioni a Session Manager (`ssm:StartSession`) dalle policy IAM degli utenti del progetto pilota.
4. Addestra gli utenti del progetto pilota sul nuovo flusso di lavoro per le richieste di accesso.
5. Monitora il progetto pilota per individuare eventuali problemi e raccogli feedback.
6. Adatta le policy e le procedure in base ai risultati del progetto pilota.

Esempio di modifica della policy IAM per gli utenti del progetto pilota

Policy originale con autorizzazioni a Session Manager:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:StartSession",
        "ssm:ResumeSession",
```

```
        "ssm:TerminateSession"
      ],
      "Resource": "*"
    }
  ]
}
```

Policy modificata per l'accesso ai nodi just-in-time:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:StartAccessRequest",
        "ssm:GetAccessToken",
        "ssm:ResumeSession",
        "ssm:TerminateSession"
      ],
      "Resource": "*"
    }
  ]
}
```

Fase 4: migrazione completa

Sviluppa una pianificazione per la migrazione degli utenti e dei nodi restanti in batch.

Metodologia di effettuazione del test

Durante tutto il processo di migrazione, esegui i seguenti test:

- Convalida delle policy: verifica che le policy di approvazione si applichino correttamente ai nodi e agli utenti previsti.
- Flusso di lavoro delle richieste di accesso: testa il flusso di lavoro completo dalla richiesta di accesso alla creazione della sessione per scenari di approvazione automatica e manuale.

- **Notifiche:** verifica che gli approvatori ricevano le notifiche tramite i canali configurati (e-mail, Slack, Microsoft Teams).
- **Registrazione e monitoraggio:** verifica che i log delle sessioni e le richieste di accesso siano acquisiti e archiviati correttamente.

Best practice per una migrazione di successo

- **Comunica tempestivamente e spesso:** informa gli utenti sulla cronologia della migrazione e sui vantaggi dell'accesso ai nodi just-in-time.
- **Inizia con sistemi non critici:** inizia la migrazione con ambienti di sviluppo o test prima di passare alla produzione.
- **Documenta tutto:** conserva registrazioni dettagliate delle policy di approvazione, delle modifiche alle policy IAM e delle impostazioni di configurazione.
- **Monitora e adatta:** monitora continuamente le richieste di accesso e i flussi di lavoro di approvazione, adattando le policy in base alle esigenze.
- **Stabilisci la governance:** crea un processo per rivedere e aggiornare regolarmente le policy di approvazione, man mano che l'ambiente cambia.

Disabilitare l'accesso just-in-time con Systems Manager

Important

Dopo aver disabilitato l'accesso ai nodi just-in-time, gli utenti potrebbero non essere in grado di connettersi ai nodi a meno che non siano già configurati altri metodi di connessione.

Per disabilitare l'accesso ai nodi just-in-time

1. A seconda della configurazione, effettuate una delle seguenti operazioni:
 - Per configurare l'organizzazione, accedi all'account amministratore delegato di Systems Manager per la tua organizzazione.
 - Per configurare un account singolo, accedi all'account in cui hai impostato l'accesso al nodo just-in-time.
2. Apri la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>

3. Scegliere Settings (Impostazioni) nel riquadro di navigazione.
4. Nella scheda Accesso al Just-in-time nodo, scegli Disabilita.

Just-in-time domande frequenti sull'accesso ai nodi

Come posso passare da Session Manager all'accesso just-in-time ai nodi?

Dopo aver configurato la console unificata e abilitato l'accesso ai nodi just-in-time, modifica le politiche IAM esistenti per completare la transizione. Ciò include l'aggiunta delle autorizzazioni necessarie per l'accesso ai nodi just-in-time e la rimozione dell'autorizzazione per il funzionamento dell'API `StartSession` per Session Manager. Per ulteriori informazioni sulle policy IAM per l'accesso ai nodi just-in-time, consulta [Configurazione dell'accesso just-in-time con Systems Manager](#).

Devo configurare la console unificata per utilizzare l'accesso ai nodi just-in-time?

Sì, la configurazione della console unificata è un prerequisito per l'accesso ai nodi just-in-time. Tuttavia, dopo aver configurato la console unificata e abilitato l'accesso ai nodi just-in-time, esistono diversi metodi per connettersi a questi ultimi. Ad esempio, puoi avviare sessioni di accesso ai nodi just-in-time dalla console Amazon EC2 e dal AWS CLI. Per ulteriori informazioni sulla configurazione della console unificata, consulta [Configurazione della console unificata di Systems Manager per un'organizzazione](#).

L'accesso ai nodi just-in-time comporta dei costi?

Systems Manager offre una versione di prova gratuita di 30 giorni per accedervi. Dopo il periodo di prova, l'accesso al nodo just-in-time comporta dei costi. Per ulteriori informazioni, consulta [AWS Systems Manager Prezzi](#).

Qual è la precedenza delle policy di approvazione per l'accesso ai nodi just-in-time?

Le policy di approvazione sono valutate nell'ordine seguente:

1. Deny-access
2. Auto-approval
3. Manuale

Come vengono valutate le policy di approvazione manuale?

Just-in-time l'accesso ai nodi favorisce sempre la policy più specifica per un nodo. Le policy di approvazione manuale sono valutate nell'ordine seguente:

1. Destinazione specifica dei tag
2. Tutte le destinazioni del nodo

Cosa succede se non c'è una policy di approvazione applicabile a un nodo?

Per connettersi a un nodo utilizzando l'accesso ai nodi just-in-time, è necessario applicare una policy di approvazione al nodo. Se non esistono policy di approvazione applicabili a un nodo, gli utenti non possono richiedervi l'accesso.

È possibile destinare molteplici policy di approvazione a un tag?

Un tag può essere designato una sola volta nelle tue policy di approvazione.

Cosa succede se molteplici policy di approvazione manuale si applicano a un nodo a causa della sovrapposizione dei tag?

Quando a un nodo si applicano molteplici policy di approvazione manuale, si verifica un conflitto e gli utenti non sono in grado di richiedere l'accesso al nodo. Tienilo a mente quando crei le policy di approvazione manuale, poiché alcune istanze potrebbero avere molteplici tag, a seconda del caso.

Posso utilizzare l'accesso ai nodi just-in-time per richiedere l'accesso e avviare sessioni su nodi tra account e Regioni?

Just-in-time node access supporta la richiesta di accesso e l'avvio di sessioni su nodi nello stesso account e nella stessa regione del richiedente.

Posso utilizzare l'accesso ai nodi just-in-time per richiedere l'accesso e avviare sessioni su nodi registrati con un'attivazione ibrida?

Sì, l'accesso ai nodi just-in-time supporta la richiesta dell'accesso e l'avvio delle sessioni su nodi registrati con un'attivazione ibrida. Il nodo deve essere registrato nello stesso account e nella stessa Regione del richiedente.

Perché viene visualizzata una pagina vuota quando provo a connettermi utilizzando l'accesso al nodo just-in-time su Session Manager?

Una schermata vuota può avere più di una causa. Se accedi alla console di Systems Manager tramite un'interfaccia Amazon VPC endpoint con DNS privato abilitato, il tuo browser potrebbe applicare la sua politica di accesso alla rete locale. Questa policy può bloccare la richiesta. La richiesta non è inoltre presente nella cronologia AWS CloudTrail degli eventi, perché il browser la interrompe prima che arrivi AWS. Per dettagli e soluzioni alternative, consulta [Consentire l'accesso alla rete locale nel browser](#)

Altrimenti, verifica che al nodo si applichi un criterio di approvazione e di disporre delle autorizzazioni necessarie per creare richieste di accesso. Per ulteriori informazioni, consulta [Cosa succede se non c'è una policy di approvazione applicabile a un nodo?](#) e [Configurazione dell'accesso just-in-time con Systems Manager](#).

Diagnosi e correzione

Tramite la console unificata di Systems Manager, è possibile identificare i problemi in tutto il parco in un'unica operazione di diagnosi. Per le organizzazioni, è quindi possibile tentare di risolverli su tutti gli obiettivi o solo su quelli selezionati attraverso un'unica operazione di automazione. Per un'organizzazione, in qualità di amministratore di account delegato, è possibile selezionare gli obiettivi in tutti gli account e le regioni. Se si utilizza un singolo account, è possibile selezionare gli obiettivi in una singola regione alla volta.

Systems Manager diagnostica e consente di risolvere al meglio diversi tipi di errori di implementazione, nonché deviazioni sulle configurazioni. Systems Manager può anche identificare le istanze di Amazon Elastic Compute Cloud (Amazon EC2) nel tuo account o organizzazione che Systems Manager non può trattare come un nodo gestito. Il processo di diagnosi delle istanze EC2 identifica problemi relativi a configurazioni errate in un cloud privato virtuale (VPC), in un'impostazione DNS (Domain Name Service) o in un gruppo di sicurezza Amazon Elastic Compute Cloud (Amazon EC2).

Note

Systems Manager supporta sia istanze EC2 che altri tipi di macchine in un ambiente [ibrido e multicloud](#) come nodi gestiti. Per essere un nodo gestito, l'agente AWS Systems Manager (SSM Agent) deve essere installato sulla macchina e Systems Manager deve disporre dell'autorizzazione per eseguire operazioni sulla macchina.

Per le istanze EC2, è possibile fornire questa autorizzazione a livello di account utilizzando un ruolo AWS Identity and Access Management (IAM) o a livello di istanza utilizzando un profilo dell'istanza. Per ulteriori informazioni, consulta [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#).

Per le macchine non EC2, questa autorizzazione viene fornita utilizzando un ruolo di servizio IAM. Per ulteriori informazioni, consulta [Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud](#).

Prima di iniziare

Per utilizzare la funzione Diagnosi e correzione per rilevare le istanze EC2 non gestite, devi prima integrare l'organizzazione o l'account nella console unificata di Systems Manager. Durante questo processo, occorre scegliere l'opzione per creare i ruoli IAM e le policy gestite necessarie per queste operazioni. Per ulteriori informazioni, consulta [Configurazione della console unificata di Systems Manager per un'organizzazione](#).

Utilizza i seguenti argomenti per identificare e correggere alcuni tipi comuni di implementazioni non riuscite, configurazioni errate e istanze EC2 non gestite.

Argomenti

- [Diagnosi e correzione delle implementazioni non riuscite](#)
- [Diagnostica e correzione di configurazioni deviate](#)
- [Diagnostica e correzione di istanze Amazon EC2 non gestite in Systems Manager](#)
- [Tipi di impatto delle operazioni del runbook sulla correzione](#)
- [Visualizzazione dello stato di avanzamento dell'esecuzione e della cronologia delle correzioni in Systems Manager](#)

Diagnosi e correzione delle implementazioni non riuscite

Systems Manager diagnostica e, successivamente, aiuta a risolvere i seguenti tipi di installazioni non riuscite:

- Configurazione di base per gli account membri dell'organizzazione
- Configurazione di base per l'account di amministratore delegato
- Configurazione di base per l'account

Utilizza la procedura seguente per tentare di risolvere questo tipo di problemi.

Per diagnosticare e correggere le implementazioni non riuscite

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel riquadro di navigazione, scegli Diagnostica e correggi.
3. Scegli la scheda Problemi di implementazione.
4. Nella sezione Implementazioni non riuscite, esamina l'elenco dei relativi esiti.
5. Nella colonna Fase di configurazione, scegli il nome di un esito per esaminare ulteriori dettagli sul problema. Ad esempio: configurazione di base per gli account dei membri dell'organizzazione.
6. Nella pagina dei dettagli relativa all'implementazione non riuscita, è possibile visualizzare un elenco di account e il numero di regioni all'interno hanno subito errori di implementazione.
7. Seleziona un ID account per visualizzare le informazioni sul motivo degli errori in quell'account.
8. Nell'area Regioni non riuscite, esamina le informazioni fornite per il Motivo dello stato. Queste informazioni indicano il motivo della mancata implementazione, il che potrebbe fornire informazioni sulle modifiche alla configurazione da apportate.
9. Se desideri riprovare l'implementazione senza apportare modifiche alla configurazione, scegli Ridistribuisce.

Diagnostica e correzione di configurazioni deviate

Systems Manager diagnostica e, successivamente, aiuta a correggere i seguenti tipi di configurazioni deviate:

- Configurazione di base per gli account membri dell'organizzazione
- Configurazione di base per l'account di amministratore delegato
- Configurazione di base per l'account

Utilizza la seguente procedura per tentare di rimediare a questi tipi di configurazioni deviate.

Per diagnosticare e correggere configurazioni deviate

1. <https://console.aws.amazon.com/systems-manager/> Apri la console all'indirizzo. AWS Systems Manager

2. Nel riquadro di navigazione, scegli Diagnostica e correggi.
3. Scegli la scheda Problemi di implementazione.
4. Nella sezione Implementazioni deviate, esamina l'elenco degli esiti delle implementazioni deviate.

oppure

Per eseguire una nuova diagnosi, scegli Rileva la deviazione.

5. Nella colonna Fase di configurazione, scegli il nome di un esito per esaminare ulteriori dettagli sul problema. Ad esempio: configurazione di base per gli account dei membri dell'organizzazione.
6. Nella pagina dei dettagli relativa all'implementazione non riuscita, è possibile visualizzare un elenco di account e indicare quante regioni di ciascuna hanno subito deviazioni di configurazione.
7. Seleziona un ID account per visualizzare le informazioni sul motivo delle deviazioni di configurazione in quell'account.
8. Nell'area Risorse deviate, la colonna Risorse riporta i nomi delle risorse che hanno subito una deviazione. La colonna Tipo di deviazione riporta se la risorsa è stata modificata o eliminata.
9. Per ridistribuire la configurazione desiderata, scegli Ridistribuisce.

Diagnostica e correzione di istanze Amazon EC2 non gestite in Systems Manager

Per gestire al meglio le istanze Amazon Elastic Compute Cloud (Amazon EC2) con Systems Manager, è possibile utilizzare l'esperienza unificata della console di Systems Manager per effettuare le seguenti operazioni:

1. Esegui un processo di diagnosi manuale o pianificato per identificare quali istanze EC2 dell'account o dell'organizzazione non sono attualmente gestite da Systems Manager.
2. Identifica i problemi di rete o di altro tipo che impediscono a Systems Manager di assumere il controllo della gestione delle istanze.
3. Esegui un'esecuzione di automazione per risolvere automaticamente il problema, oppure accedi alle informazioni per risolvere il problema manualmente.

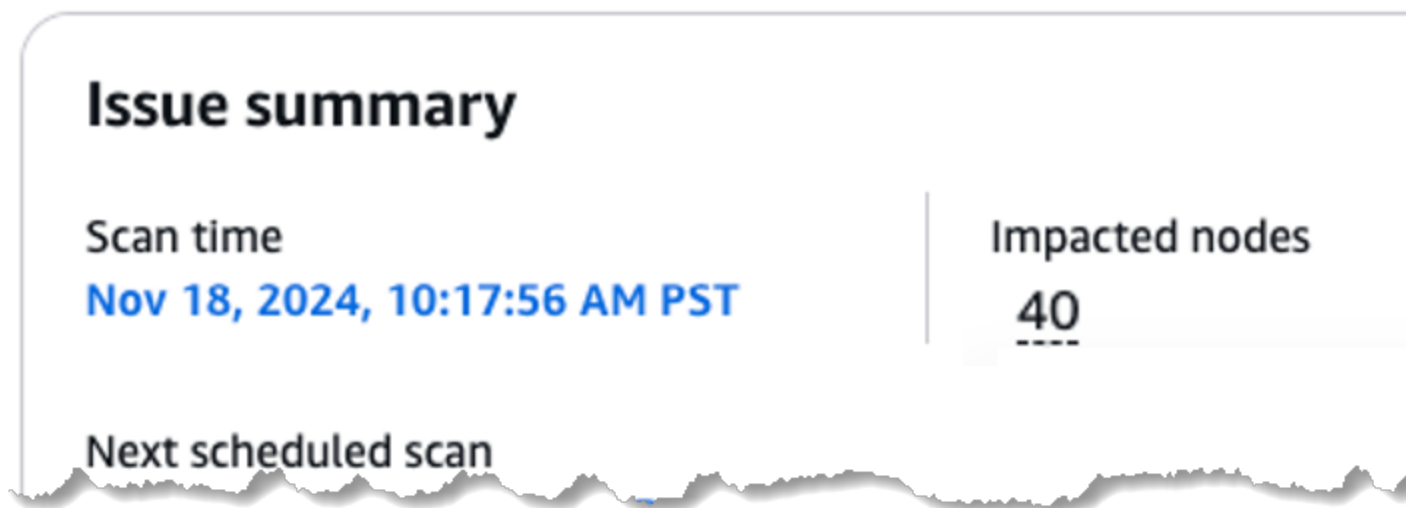
Utilizza le informazioni contenute nei seguenti argomenti per diagnosticare e risolvere i problemi che impediscono a Systems Manager di gestire le istanze EC2.

In che modo Systems Manager conta i nodi interessati nell'elenco "Problemi relativi alle istanze EC2 non gestite"

Il numero di nodi segnalati come non gestiti nella scheda Problemi alle istanze EC2 non gestite rappresenta il numero totale di istanze con uno dei seguenti valori di stato al momento della scansione della diagnosi:

- Running
- Stopped
- Stopping

Questo numero è riportato come Nodi interessati nell'area di Riepilogo del problema. Nell'immagine seguente, il numero di nodi interessati non attualmente gestiti da Systems Manager è 40.



A differenza del rapporto sulle istanze EC2 non gestite nella pagina Esamina approfondimenti nodi, questo conteggio delle istanze EC2 non è dinamico. Rappresenta gli esiti ottenuti durante l'ultima scansione diagnostica segnalata, mostrati come valore del tempo di scansione. Consigliamo pertanto di eseguire una scansione diagnostica per le istanze EC2 non gestite a intervalli regolari per mantenere aggiornato il numero riportato di nodi interessati.

Per informazioni sui conteggi delle istanze non gestite nella pagina Rivedi gli approfondimenti sui nodi, consulta [Cos'è un'istanza non gestita?](#) nell'argomento [Esaminare approfondimenti nodo](#).

Argomenti

- [Categorie di problemi diagnosticabili relativi alle istanze EC2 non gestite](#)

- [Esecuzione di una diagnosi e di una riparazione opzionale per le istanze EC2 non gestite](#)
- [Pianificazione di una scansione ricorrente per istanze EC2 non gestite](#)

Categorie di problemi diagnosticabili relativi alle istanze EC2 non gestite

Questo argomento elenca le principali categorie di problemi di gestione EC2 e i problemi specifici di ciascuna categoria che Systems Manager contribuisce a diagnosticare e risolvere. In alcuni casi, Systems Manager identifica il problema, ma non fornisce una correzione automatica. In questi casi, la console Systems Manager indirizza alle informazioni per risolvere manualmente un problema.

Il processo di diagnosi esamina ogni gruppo di istanze EC2 contemporaneamente in base al cloud privato virtuale (VPC) a cui appartengono.

Tipi di problema

- [Categoria di problema: configurazione del gruppo di sicurezza e comunicazioni HTTPS](#)
- [Categoria di problema: configurazione DNS o nome host DNS](#)
- [Categoria di problema: configurazione dell'endpoint VPC](#)
- [Categoria del problema: configurazione ACL di rete](#)
- [Categoria del problema: ruoli e autorizzazioni IAM](#)
- [Categoria di problema: versione SSM Agent](#)
- [Categoria di problema: controllo dello stato dell'istanza](#)
- [Categoria di problema: configurazione del sistema operativo](#)
- [Categoria di problema: configurazione del servizio Systems Manager \(configurazione predefinita per la gestione degli host\)](#)
- [Categoria di problema: problemi di attivazione ibrida](#)

Categoria di problema: configurazione del gruppo di sicurezza e comunicazioni HTTPS

Un'operazione di diagnosi potrebbe rilevare che non è SSM Agent possibile comunicare con il servizio Systems Manager tramite HTTPS. In questi casi, è possibile scegliere di eseguire un runbook Automation che tenti di aggiornare i gruppi di sicurezza collegati alle istanze.

 Note

A volte, Systems Manager può non essere in grado di risolvere automaticamente questi problemi, ma è possibile modificare manualmente i gruppi di sicurezza interessati.

Tipi di problema supportati

- Gruppo di sicurezza dell'istanza: il traffico in uscita non è consentito sulla porta 443
- **ssm** Gruppo di sicurezza dell'endpoint VPC: il traffico in entrata non è consentito sulla porta 443
- **ssmmessages** Gruppo di sicurezza dell'endpoint VPC: il traffico in entrata non è consentito sulla porta 443
- **ec2messages** Gruppo di sicurezza dell'endpoint VPC: il traffico in entrata non è consentito sulla porta 443

Per ulteriori informazioni, consulta [Verifica le regole di accesso sui gruppi di sicurezza degli endpoint](#) nell'argomento [Risoluzione dei problemi Agente SSM](#).

Categoria di problema: configurazione DNS o nome host DNS

Un'operazione di diagnosi può rilevare che il Domain Name System (DNS) o i nomi host DNS non sono configurati correttamente per il VPC. In questi casi, si può scegliere di eseguire un runbook Automation che tenti di abilitare gli attributi `enableDnsSupport` e `enableDnsHostnames` del VPC interessato.

Tipi di problema supportati

- Il supporto DNS è disabilitato in un VPC.
- Un nome host DNS è disabilitato in un VPC.

Per ulteriori informazioni, consulta [Verifica gli attributi del tuo VPC DNS-related](#) nell'argomento [Risoluzione dei problemi Agente SSM](#).

Categoria di problema: configurazione dell'endpoint VPC

Un'operazione di diagnosi può rilevare che gli endpoint VPC non sono configurati correttamente per il VPC.

Se gli endpoint VPC richiesti da SSM Agent non esistono, Systems Manager tenta di eseguire un runbook Automation per creare gli endpoint VPC e li associa a una sottorete in ogni zona di disponibilità (AZ) regionale pertinente. Se gli endpoint VPC richiesti esistono ma non sono associati a una sottorete in cui è stato rilevato il problema, il runbook associa gli endpoint VPC alla sottorete interessata.

Note

Systems Manager non supporta la risoluzione di tutti i problemi dell'endpoint VPC non configurato correttamente. In questi casi, Systems Manager indirizza l'utente alle istruzioni manuali per la correzione anziché eseguire un runbook Automation.

Tipi di problema supportati

- Non è PrivateLink stato trovato alcun `ssm.region.amazonaws.com` endpoint per.
- Non è PrivateLink stato `ssmmessages.region.amazonaws.com` trovato alcun endpoint per.
- Non è PrivateLink stato `ec2messages.region.amazonaws.com` trovato alcun endpoint per.

Tipi di problemi diagnosticabili

Systems Manager è in grado di diagnosticare i seguenti tipi di problemi, ma al momento non è disponibile alcun runbook per risolverli. È possibile modificare manualmente la configurazione per questi problemi.

- La sottorete di un'istanza non è collegata a un endpoint `ssm.region.amazonaws.com`.
- La sottorete di un'istanza non è collegata a un endpoint `ssmmessages.region.amazonaws.com`.
- La sottorete di un'istanza non è collegata a un endpoint `ec2messages.region.amazonaws.com`.

Per ulteriori informazioni, consulta [Verifica la configurazione VPC](#) nell'argomento [Risoluzione dei problemi Agente SSM](#).

Categoria del problema: configurazione ACL di rete

Un'operazione di diagnosi potrebbe rilevare che gli elenchi di controllo degli accessi alla rete (NACL) non sono configurati correttamente per il VPC, bloccando il traffico necessario per le comunicazioni

con Systems Manager. I NACL sono stateless, quindi sia le regole in uscita che quelle in entrata devono consentire il traffico di Systems Manager.

Systems Manager è in grado di identificare i problemi di configurazione NACL e fornire indicazioni per la risoluzione manuale.

Tipi di problema supportati

- Subnet di istanza NACL: il traffico in uscita non è consentito sulla porta 443 verso gli endpoint di Systems Manager
- NACL della sottorete di istanza: il traffico in entrata non è consentito sulle porte temporanee (1024-65535) per le risposte di Systems Manager

Tipi di problemi diagnosticabili

Systems Manager è in grado di diagnosticare i seguenti problemi di configurazione NACL, ma è necessaria una correzione manuale:

- Il NACL della sottorete di un'istanza blocca il traffico HTTPS (porta 443) in uscita verso gli endpoint di Systems Manager
- Il NACL della sottorete di un'istanza blocca il traffico effimero sulla porta in entrata (1024-65535) necessario per le risposte di Systems Manager

Per ulteriori informazioni, consulta [Risoluzione dei problemi relativi all'agente SSM e ACL di rete personalizzati per il tuo VPC](https://docs.aws.amazon.com/vpc/latest/userguide/custom-network-acl.html#nacl-ephemeral-ports). <https://docs.aws.amazon.com/vpc/latest/userguide/custom-network-acl.html#nacl-ephemeral-ports>

Categoria del problema: ruoli e autorizzazioni IAM

Un'operazione di diagnosi potrebbe rilevare che i ruoli o le autorizzazioni IAM non sono configurati correttamente per consentire all'istanza EC2 di comunicare con Systems Manager. In questi casi, Systems Manager identifica le autorizzazioni mancanti e fornisce indicazioni per la correzione.

Tipi di problema supportati

- Nessun profilo di istanza allegato: all'istanza EC2 non è associato un profilo di istanza IAM
- Policy gestita SSM mancante: il ruolo IAM associato al profilo dell'istanza non include la policy AmazonSSMManagedInstanceCore gestita o le autorizzazioni equivalenti

- Autorizzazioni SSM insufficienti: il ruolo IAM non consente le azioni minime richieste per la comunicazione con Systems Manager (ssm:UpdateInstanceInformation, ssm:messages:, ssm:messages:, ec2:messages:CreateControlChannel) CreateDataChannel GetMessages

Per ulteriori informazioni, consulta [Configure instance permissions for Systems Manager nella Amazon Web Services Systems Manager User Guide](#).

Categoria di problema: versione SSM Agent

Un'operazione di diagnosi potrebbe rilevare che l'agente SSM installato sull'istanza EC2 è obsoleto e non è più compatibile con i requisiti di servizio di Systems Manager. In questi casi, Systems Manager identifica la versione obsoleta dell'agente e fornisce indicazioni per la risoluzione.

Tipi di problema supportati

- Versione dell'agente SSM obsoleta: l'istanza esegue una versione dell'agente SSM precedente alla versione minima supportata richiesta per la connettività di Systems Manager
- Versione dell'agente incompatibile con le funzionalità correnti: la versione dell'agente installata non supporta i protocolli di comunicazione richiesti utilizzati dal servizio Systems Manager

Per ulteriori informazioni, consulta [Verifica del numero](#) di versione dell'agente SSM e [Automating updates to SSM Agent](#) nella Amazon Web Services Systems Manager User Guide.

Categoria di problema: controllo dello stato dell'istanza

Un'operazione di diagnosi potrebbe rilevare che l'istanza EC2 non supera i controlli dello stato del sistema o dell'istanza, il che impedisce all'agente SSM di stabilire una comunicazione con il servizio Systems Manager. In questi casi, Systems Manager identifica il fallimento del controllo dello stato e fornisce una guida per la risoluzione.

Tipi di problema supportati

- Errore nel controllo dello stato del sistema: l'infrastruttura host sottostante che supporta l'istanza ha segnalato un problema che impediva la connettività di Systems Manager
- Errore nel controllo dello stato dell'istanza: il sistema operativo o la configurazione di rete dell'istanza non risponde correttamente, bloccando la comunicazione con SSM Agent

Per ulteriori informazioni, consulta la sezione Controlli [dello stato delle istanze Amazon EC2](#) nella Amazon Web Services Systems Manager User Guide.

Categoria di problema: configurazione del sistema operativo

Un'operazione di diagnosi potrebbe rilevare che i OS-level problemi impediscono all'agente SSM di funzionare o comunicare con il servizio Systems Manager. In questi casi, Systems Manager analizza l'output della console dell'istanza per identificare errori di avvio, guasti del servizio o altri problemi del sistema operativo.

Tipi di problema supportati

- Servizio SSM Agent non in esecuzione: il servizio SSM Agent è stato interrotto o si è bloccato a causa di OS-level problemi quali l'esaurimento delle risorse o i conflitti di servizio
- Errori di avvio rilevati: l'output della console dell'istanza indica il panico del kernel, il danneggiamento del file system o altri errori di avvio critici che impediscono il normale funzionamento
- OS-level blocco della rete: un firewall basato su host (come iptables o Windows Firewall) blocca il traffico HTTPS in uscita necessario per le comunicazioni con Systems Manager
- esaurimento dello spazio su disco: il volume principale o la partizione di sistema non dispone di spazio libero sufficiente, il che impedisce all'agente SSM di funzionare correttamente

Note

Systems Manager diagnostica i OS-level problemi analizzando l'output della console dell'istanza. La correzione automatica non è disponibile per questi problemi perché richiedono l'accesso diretto al sistema operativo dell'istanza. Systems Manager fornisce indicazioni per la risoluzione manuale.

Per ulteriori informazioni, consulta [Troubleshooting SSM Agent](#) nella Amazon Web Services Systems Manager User Guide.

Categoria di problema: configurazione del servizio Systems Manager (configurazione predefinita per la gestione degli host)

Un'operazione di diagnosi potrebbe rilevare che la configurazione predefinita di gestione degli host (DHMC) non è configurata correttamente nell'account e nella regione. DHMC consente a Systems Manager di gestire automaticamente le istanze EC2 senza richiedere un profilo di istanza su ciascuna istanza. Se DHMC non è abilitato o il ruolo associato non dispone delle autorizzazioni necessarie, le istanze senza un profilo di istanza non possono essere gestite.

Tipi di problema supportati

- DHMC non abilitato: la configurazione predefinita di gestione dell'host non è attivata nell'account e nella regione. Le istanze senza un profilo di istanza non possono essere gestite da Systems Manager
- Ruolo DHMC privo delle politiche richieste: il ruolo IAM configurato per DHMC non include la policy AmazonSSMManagedInstanceCore gestita o le autorizzazioni equivalenti richieste per la connettività di Systems Manager
- La politica di attendibilità del ruolo DHMC non è configurata correttamente: il ruolo IAM configurato per DHMC non ha la relazione di fiducia corretta che consente al servizio Systems Manager di assumerla

Per ulteriori informazioni, consulta la configurazione [predefinita della gestione degli host](#) nella Guida per l'utente di Amazon Web Services Systems Manager.

Categoria di problema: problemi di attivazione ibrida

Un'operazione di diagnosi potrebbe rilevare che i nodi ibridi attivati (istanze esterne ad Amazon Web Services, come server locali o VM in altri ambienti cloud) presentano problemi di registrazione o connettività con Systems Manager. In questi casi, Systems Manager identifica i problemi di attivazione e registrazione specifici degli ambienti ibridi.

Tipi di problema supportati

- Attivazione scaduta: l'attivazione ibrida utilizzata per registrare il nodo gestito è scaduta. È necessario creare una nuova attivazione per registrare nodi aggiuntivi
- Limite di registrazione all'attivazione raggiunto: è stato raggiunto il numero massimo di registrazioni consentite dall'attivazione. È necessario creare una nuova attivazione con un limite di registrazione più elevato oppure è necessario annullare la registrazione delle registrazioni esistenti
- Conflitto di registrazione dell'agente: esiste una registrazione in conflitto per il nodo, in genere causata dalla clonazione di una macchina virtuale precedentemente registrata con Systems Manager senza prima annullare la registrazione
- Connettività agli endpoint di Systems Manager: il nodo ibrido non può raggiungere gli endpoint del servizio Systems Manager richiesti dalla sua posizione di rete

Per ulteriori informazioni, consulta [Creare un'attivazione ibrida per registrare i nodi con Systems Manager](#) e [Risoluzione dei problemi di disponibilità dei nodi gestiti](#) nella Amazon Web Services Systems Manager User Guide.

Esecuzione di una diagnosi e di una riparazione opzionale per le istanze EC2 non gestite

Utilizzate la seguente procedura per diagnosticare i VPC-related problemi relativi alla rete e che potrebbero impedire a Systems Manager di gestire le istanze EC2.

L'operazione di diagnosi rileva e raggruppa problemi dei seguenti tipi:

- Problemi di configurazione di rete: tipi di problemi di rete che impediscono alle istanze EC2 di comunicare con il servizio Systems Manager nel cloud. Per questi problemi sono disponibili operazioni di correzione. Per ulteriori informazioni sui problemi di configurazioni di rete, consulta [Categorie di problemi diagnosticabili relativi alle istanze EC2 non gestite](#).
- Ruoli e autorizzazioni IAM: problemi relativi ai profili e alle autorizzazioni delle istanze IAM mancanti o mal configurati, necessari per consentire alle istanze EC2 di comunicare con Systems Manager.
- Versione dell'agente SSM: problemi relativi alle versioni obsolete o incompatibili installate sulle istanze EC2. SSM Agent
- Controllo dello stato dell'istanza: problemi relativi ai controlli dello stato del sistema o dell'istanza non riusciti che SSM Agent impediscono di stabilire una comunicazione con Systems Manager.
- Configurazione del sistema operativo: problemi relativi a OS-level problemi che SSM Agent impediscono l'esecuzione o la comunicazione con Systems Manager.
- Configurazione del servizio Systems Manager: problemi relativi alla configurazione predefinita della gestione degli host (DHMC) non configurata correttamente nell'account e nella regione.
- Problemi di attivazione ibrida: problemi relativi ai nodi attivati con sistemi ibridi che presentano problemi di registrazione o connettività con Systems Manager.
- Problemi non identificati: un elenco degli esiti relativi ai casi in cui l'operazione di diagnostica non è riuscita a determinare il motivo per cui le istanze EC2 non sono in grado di comunicare con il servizio Systems Manager nel cloud.

Per eseguire una diagnosi e una correzione per le istanze EC2 non gestite

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel riquadro di navigazione, scegli Diagnostica e correggi.
3. Scegli la scheda Problemi alle istanze EC2 non gestite.
4. Nella sezione Riepilogo del problema, scegli Esegui nuova diagnosi.

oppure

Se è la prima volta che diagnostichi problemi EC2 non gestiti, nella sezione Diagnostica istanze EC2 non gestite, scegli Esegui.

 Tip

Durante la diagnosi, scegli Visualizza avanzamento o Visualizza esecuzioni per monitorare lo stato corrente dell'esecuzione. Per ulteriori informazioni, consulta [Visualizzazione dello stato di avanzamento dell'esecuzione e della cronologia delle correzioni in Systems Manager](#).

5. Una volta completata la diagnosi, esegui le seguenti operazioni:
 - Per qualsiasi problema segnalato nelle sezioni relative ai ruoli e alle autorizzazioni IAM, alla versione dell'agente SSM, al controllo dello stato dell'istanza, alla configurazione del sistema operativo, alla configurazione del servizio Systems Manager o ai problemi di attivazione ibrida, scegli il link Ulteriori informazioni per informazioni sulla risoluzione del problema.
 - Per qualsiasi problema segnalato nella sezione Problemi non identificati, scegli il link Ulteriori informazioni per informazioni sulla risoluzione del problema.
 - Per i problemi segnalati nella sezione Problemi sulla configurazioni di rete, continua con il passaggio successivo.
6. Nell'elenco dei tipi di esito, nella colonna Suggerimenti, scegli il link per un problema specifico, ad esempio 2 suggerimenti.
7. Nel riquadro Suggerimenti che si apre, scegli tra le mitigazioni disponibili:
 - Ulteriori informazioni: apri un argomento con informazioni su come risolvere un problema manualmente.

- Visualizza il runbook: apri un riquadro con informazioni sul runbook Automation da eseguire per risolvere il problema con le istanze EC2, oltre alle opzioni per generare un'anteprima delle operazioni che il runbook intraprenderebbe. Passa alla fase successiva.
8. Nel riquadro del runbook, eseguire queste operazioni:
- a. Per la Descrizione del documento, consulta il contenuto, che fornisce un'anteprima delle operazioni che il runbook intraprende per correggere i problemi relativi alle istanze EC2 non gestite. Scegli Visualizza i passaggi per visualizzare in anteprima le singole operazioni che il runbook intraprenderebbe.
 - b. Per Destinazioni, esegui queste operazioni:
 - Per gestire le riparazioni per un'organizzazione, per Account, specifica se questo runbook riguarderà tutti gli account o solo un sottoinsieme di account a scelta.
 - Per le regioni, specifica se questo runbook si rivolge Regioni AWS a tutti i membri del tuo account o della tua organizzazione o solo a un sottoinsieme di regioni a tua scelta.
 - c. Per l'Anteprima del runbook, consulta attentamente le informazioni. Queste informazioni spiegano quale sarebbe l'ambito e l'impatto se si scegliesse di eseguire il runbook.

 Note

La scelta di eseguire il runbook comporterebbe dei costi, quindi esamina attentamente le informazioni di anteprima prima di decidere se procedere.

Il contenuto di Anteprima del runbook fornisce le seguenti informazioni:

- In quante regioni verrebbe eseguita l'operazione del runbook.
- (Solo per le organizzazioni) In quante unità organizzative (UO) verrà eseguita l'operazione.
- I tipi di operazioni che verrebbero intraprese e quante di ciascuna.

I tipi di operazioni includono quanto segue:

- Mutante: una fase del runbook apporterebbe modifiche alle destinazioni tramite operazioni che creano, modificano o eliminano risorse.

- **Non-mutating:** la fase del runbook recupererebbe i dati sulle risorse ma non apporterebbe modifiche ad esse. Questa categoria include generalmente `Describe*`, `List*`, `Get*` e simili operazioni API di sola lettura.
- **Indeterminato:** un passaggio indeterminato richiama le esecuzioni eseguite da un altro servizio di orchestrazione come `Run Command`. AWS Lambda AWS Step Functions AWS Systems Manager Un passaggio indeterminato ha la possibilità di richiamare anche un'API di terze parti. Systems Manager Automation non conosce l'esito dei processi di orchestrazione o delle esecuzioni di API di terze parti, quindi i risultati delle fasi sono indeterminati.

d. In questo caso, è possibile scegliere una delle seguenti operazioni:

- Arresta il runbook senza eseguirlo.
- Scegli **Esegui** per eseguire il runbook con le opzioni che già selezionate.

Per scegliere di eseguire l'operazione, vai su **Visualizza avanzamento** o **Visualizza esecuzioni** per monitorare lo stato corrente dell'esecuzione. Per ulteriori informazioni, consulta [Visualizzazione dello stato di avanzamento dell'esecuzione e della cronologia delle correzioni in Systems Manager](#).

Pianificazione di una scansione ricorrente per istanze EC2 non gestite

Puoi eseguire una scansione su richiesta per le istanze Amazon EC2 nel tuo account o organizzazione che Systems Manager non è in grado di gestire a causa di problemi di configurazione. È anche possibile pianificare questa scansione in modo che avvenga automaticamente a intervalli regolari.

Per pianificare una scansione ricorrente per istanze EC2 non gestite

1. Apri la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel riquadro di navigazione, scegli **Diagnostica e correggi**.
3. Scegli la scheda **Problemi alle istanze EC2 non gestite**.
4. Nella sezione **Diagnostica istanze EC2 non gestite**, attiva **Pianifica diagnosi ricorrenti**.
5. Per **Frequenza diagnostica**, seleziona se eseguire la diagnosi una volta al giorno o una volta alla settimana.

6. (Facoltativo) In Ora di inizio, inserisci un'ora, in formato 24 ore, per l'inizio della diagnosi. Ad esempio, per le 20:15, inserisci **20:15**.

L'ora inserita si riferisce al fuso orario locale corrente.

Se non si specifica un orario, la scansione diagnostica verrà eseguita immediatamente. Systems Manager pianifica inoltre l'esecuzione della scansione in futuro all'ora corrente. Se si specifica un orario, Systems Manager attende l'esecuzione della scansione diagnostica all'ora specificata.

7. Scegli Esegui. La diagnosi viene eseguita immediatamente, ma verrà eseguita anche secondo la pianificazione specificata.

Tipi di impatto delle operazioni del runbook sulla correzione

Systems Manager esegue operazioni di diagnosi che rilevano determinati tipi di implementazioni fallite e configurazioni deviate, nonché alcuni tipi di problemi di configurazione che impediscono a Systems Manager di gestire le istanze EC2. I risultati della diagnosi includono raccomandazioni per i runbook Automation da eseguire per tentare di risolvere un problema. Per ulteriori informazioni su queste operazioni di diagnosi, consulta i seguenti argomenti:

- [Diagnosi e correzione delle implementazioni non riuscite](#)
- [Diagnostica e correzione di configurazioni deviate](#)
- [Diagnostica e correzione di istanze Amazon EC2 non gestite in Systems Manager](#)

Quando Systems Manager identifica un problema da risolvere eseguendo un runbook Automation sulle risorse interessate, fornisce un'anteprima di esecuzione. L'anteprima di esecuzione fornisce informazioni sui tipi di modifiche che l'esecuzione del runbook apporterebbe agli obiettivi. Queste informazioni includono il numero di ciascuno dei tre tipi di modifiche identificati dalla diagnosi.

I tipi di modifiche consistono come segue:

- **Mutating**: una fase di runbook apporterebbe modifiche alle destinazioni tramite operazioni che creano, modificano o eliminano risorse.
- **Non-Mutating**: una fase del runbook recupererebbe i dati sulle risorse, non apportandoci nessuna modifica. Questa categoria include generalmente `Describe*`, `List*`, `Get*` e simili operazioni API di sola lettura.
- **Undetermined**: un passaggio indeterminato richiama le esecuzioni eseguite da un altro servizio di orchestrazione come AWS Lambda, o AWS Step Functions, uno strumento in. Run Command

AWS Systems Manager Un passaggio indeterminato potrebbe anche richiamare un'API di terze parti o eseguire un Python PowerShell o uno script. Systems Manager Automation non è in grado di rilevare quale sarebbe il risultato dei processi di orchestrazione o delle esecuzioni di API di terze parti, pertanto non li valuta. È necessario esaminare manualmente i risultati di tali fasi per determinarne l'impatto.

Consulta la tabella seguente per informazioni sul tipo di impatto delle operazioni di automazione supportate.

Tipi di impatto delle operazioni di correzione supportate

La tabella presenta il tipo di impatto, mutante e indeterminato Non-mutating, di varie azioni che possono essere incluse in un runbook di correzione.

Azione ¹	Impact type (Tipo di impatto)
aws:approve	Non-mutating
aws:assert AwsResourceProperty	Non-mutating
aws:branch	Non-mutating
aws: modifica InstanceState	Mutante
aws:copyImage	Mutante
aws:createImage	Mutante
aws:createStack	Mutante
aws:createTags	Mutante
aws:deleteImage	Mutante
aws:deleteStack	Mutante
aws:executeAutomation	Indeterminato
aws: esegui AwsApi	Indeterminato

Azione ¹	Impact type (Tipo di impatto)
aws:executeScript	Indeterminato
aws: esegui StateMachine	Indeterminato
aws: invoke LambdaFunction	Indeterminato
aws:invokeWebhook	Indeterminato
aws:loop	Varia. Dipende dalle operazioni del loop.
aws:pause	Non-mutating
aws:runCommand	Indeterminato
aws:runInstances	Mutante
aws:sleep	Non-mutating
aws:updateVariable	Mutante
aws: aspetta ForAwsResourceProperty	Non-mutating

¹ Per ulteriori informazioni sulle operazioni di automazione, consultare [Riferimento alle operazioni del servizio di automazione di Systems Manager](#).

Visualizzazione dello stato di avanzamento dell'esecuzione e della cronologia delle correzioni in Systems Manager

È possibile visualizzare un elenco di tutte le operazioni di correzione completate e in corso, eseguite tramite la funzionalità Diagnosi e correzione in Systems Manager.

I dati nell'elenco della cronologia di esecuzione riportano i seguenti tipi di informazioni:

- Il tipo di esecuzione, *Diagnosis* o *Remediation*.
- Lo stato di esecuzione, ad esempio *Success* o *Failed*.
- Gli orari in cui l'esecuzione è iniziata e terminata.

Per visualizzare lo stato di avanzamento dell'esecuzione e la cronologia delle correzioni

1. Apri la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel riquadro di navigazione, scegli Diagnostica e correggi.
3. Scegli Visualizza esecuzioni.

 Tip

Quando è in corso un'esecuzione, è inoltre possibile scegliere Visualizza lo stato di avanzamento per aprire la pagina della cronologia delle esecuzioni.

4. (Facoltativo) Nella barra di ricerca , inserisci una frase per restringere l'elenco delle esecuzioni, ad esempio **EC2** o **VPC**.
5. (Facoltativo) Per visualizzare ulteriori dettagli su un'esecuzione, nella colonna Nome esecuzione, scegli un nome per l'operazione, ad esempio **AWS-DiagnoseUnmanagedEC2NetworkIssues**.

Nel riquadro dei dettagli, puoi esaminare le informazioni su tutti i passaggi tentati durante l'operazione. È inoltre possibile esaminare tutti gli input e gli output per l'esecuzione.

Regolazione delle impostazioni di Systems Manager

Le opzioni nelle pagine delle Impostazioni abilitano e configurano le funzionalità nella console unificata di Systems Manager. Le opzioni visualizzate dipendono dall'account a cui si è effettuato l'accesso e dal fatto che Systems Manager sia già stato configurato.

 Note

Le opzioni nella pagina Impostazioni non influiscono sugli strumenti di Systems Manager (precedentemente denominati funzionalità).

Impostazioni di configurazione dell'account

Se Systems Manager è abilitato, la pagina di configurazione dell'account mostra l'opzione per disabilitare Systems Manager se una delle seguenti condizioni è vera: il tuo account non è un membro di Organizations o l'amministratore delegato non ha aggiunto il tuo account Organizations a Systems Manager. La disattivazione di Systems Manager implica che Systems Manager non visualizza la console unificata. Tutti gli strumenti di Systems Manager funzioneranno ancora.

Impostazioni di configurazione organizzativa

Nella scheda Configurazione organizzativa, la sezione Regione principale mostra la regione Regione AWS scelta come regione principale durante la configurazione. Negli ambienti con più account e più regioni che utilizzano AWS Organizations, Systems Manager aggrega automaticamente i dati dei nodi da tutti gli account e le regioni nella regione principale. L'aggregazione dei dati in questo modo consente di visualizzare i dati dei nodi tra account e regioni in un'unica posizione.

Note

Se si desidera modificare la regione di origine, è necessario disattivare Systems Manager e, in seguito, riattivarlo. Per disabilitare Systems Manager, scegli Disabilita.

La sezione Configurazione organizzativa mostra le unità AWS organizzative Regioni AWS scelte durante la configurazione. Per modificare le unità organizzative e le regioni che visualizzano i dati dei nodi in Systems Manager, scegli Modifica. Per ulteriori informazioni sulla configurazione di Systems Manager per Organizations, consulta [Configurazione AWS Systems Manager](#).

Configurazioni delle funzionalità

La sezione Configurazioni delle funzionalità consente di abilitare e configurare le funzionalità chiave di Systems Manager che migliorano la gestione dei nodi in tutta l'organizzazione. Queste funzionalità interagiscono per fornire la gestione automatizzata, il monitoraggio della conformità e la manutenzione dei nodi gestiti.

È possibile configurare queste funzionalità durante la configurazione iniziale di Systems Manager o modificarle in un secondo momento tramite la pagina Impostazioni. Ogni funzionalità può essere abilitata o disabilitata indipendentemente in base ai requisiti dell'organizzazione.

Configurazione di gestione host predefinita

La Configurazione di gestione host predefinita (Default Host Management Configuration, DHMC) configura automaticamente istanze Amazon Elastic Compute Cloud (Amazon EC2) nell'organizzazione per essere gestite da Systems Manager. Se abilitata, DHMC garantisce che le istanze EC2 nuove ed esistenti dispongano delle autorizzazioni e delle configurazioni AWS Identity and Access Management (IAM) necessarie per comunicare con i servizi di Systems Manager.

DHMC offre i seguenti vantaggi:

- Assegnazione automatica dei ruoli IAM: assicura che le istanze EC2 abbiano i ruoli e le policy IAM richiesti per funzionare come nodi gestiti.
- Correzione della deriva: corregge automaticamente la deriva della configurazione quando le istanze perdono lo stato di nodo gestito.
- Onboarding semplificato: riduce i passaggi di configurazione manuale per le nuove istanze.
- Configurazione coerente: mantiene impostazioni uniformi in tutta la flotta EC2.

Configurazione della frequenza di correzione della deviazione

La correzione della deviazione rileva e corregge automaticamente quando le istanze EC2 perdono la configurazione dei nodi gestiti. È possibile configurare la frequenza con cui Systems Manager verifica e corregge le deviazioni di configurazione.

Per configurare la configurazione di gestione host predefinita

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella sezione Configurazioni delle funzionalità, individua la voce Configurazione predefinita della gestione dell'host.
4. Per abilitare DHMC, attiva l'interruttore di selezione.
5. Per la frequenza di correzione della derivazione, scegli con quale frequenza desideri che Systems Manager verifichi e corregga la deviazione della configurazione:
 - Ogni giorno: controlla e corregge la deviazione una volta al giorno
 - Settimanale: verifica e corregge la deriva una volta alla settimana
 - Mensile: verifica e corregge la deriva una volta al mese

6. Selezionare Salva.

Note

Quando abiliti DHMC, Systems Manager crea i ruoli e le policy IAM necessari nel tuo account. Questi ruoli consentono alle istanze EC2 di comunicare con i servizi Systems Manager. Per ulteriori informazioni sulla creazione dei ruoli IAM tramite DHMC, consulta la sezione [Gestire le istanze EC2 con Systems Manager](#).

Raccolta dei metadati dell'inventario

La raccolta dei metadati dell'inventario raccoglie automaticamente informazioni dettagliate sui nodi gestiti, tra cui applicazioni installate, configurazioni di rete, aggiornamenti di sistema e altri metadati di sistema. Queste informazioni aiutano a mantenere la conformità, eseguire analisi di sicurezza e comprendere la composizione dell'infrastruttura.

La raccolta dell'inventario offre i seguenti vantaggi:

- **Monitoraggio della conformità:** tieni traccia del software e delle configurazioni installati per i report sulla conformità.
- **Analisi della sicurezza:** identificazione del software obsoleto e delle potenziali vulnerabilità di sicurezza.
- **Gestione delle risorse:** mantieni un inventario aggiornato della tua infrastruttura.
- **Funzionalità di interrogazione:** utilizza i dati raccolti con Amazon Q Developer per le query in linguaggio naturale.

Tipi di dati di inventario raccolti

Quando la raccolta dei metadati dell'inventario è abilitata, Systems Manager raccoglie i seguenti tipi di informazioni dai nodi gestiti:

- **Applicazioni:** pacchetti software e applicazioni installati
- **Configurazioni di rete:** interfacce di rete, indirizzi IP e impostazioni di rete
- **Aggiornamenti di sistema:** patch installate e aggiornamenti disponibili
- **Proprietà del sistema:** specifiche hardware, dettagli del sistema operativo e configurazioni del sistema

- Servizi: servizi in esecuzione e relative configurazioni

Configurazione della frequenza di raccolta dell'inventario

È possibile configurare la frequenza con cui Systems Manager raccoglie i metadati dell'inventario dai nodi gestiti. Una raccolta più frequente fornisce informazioni più aggiornate ma può aumentare l'utilizzo del AWS servizio.

Per configurare la raccolta dei metadati dell'inventario

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella sezione Configurazioni delle funzionalità, individua la raccolta dei metadati dell'inventario.
4. Per abilitare la raccolta dell'inventario, attiva l'interruttore di selezione.
5. Per la frequenza di raccolta, scegli la frequenza con cui desideri che Systems Manager raccolga i dati di inventario:
 - Ogni giorno: raccoglie i dati di inventario una volta al giorno
 - Settimanale: raccoglie i dati di inventario una volta alla settimana
 - Mensile: raccoglie i dati di inventario una volta al mese
6. Selezionare Salva.

Important

La raccolta dell'inventario richiede che i nodi gestiti dispongano delle autorizzazioni necessarie per raccogliere informazioni di sistema. Assicurati che i tuoi nodi gestiti abbiano i ruoli e le policy IAM appropriati. Per ulteriori informazioni sulle autorizzazioni richieste, consultare [AWS Systems Manager Inventory](#).

Agente SSM aggiornamenti

SSM AgentGli aggiornamenti automatici assicurano che i nodi gestiti eseguano la versione più recente di SSM Agent. Mantenere l'agente aggiornato consente di accedere alle funzionalità più recenti, ai miglioramenti della sicurezza e alle correzioni di bug.

SSM Agent gli aggiornamenti automatici offrono i seguenti vantaggi:

- Funzionalità più recenti: accesso a nuove funzionalità e miglioramenti di Systems Manager
- Aggiornamenti di sicurezza: installazione automatica di patch e correzioni di sicurezza
- Affidabilità migliorata: correzioni di bug e miglioramenti dell'affidabilità
- Manutenzione ridotta: elimina la necessità di aggiornamenti manuali degli agenti

Configurazione dell'aggiornamento automatico dell'agente

È possibile configurare la frequenza con cui Systems Manager verifica e installa gli aggiornamenti dell'SSM Agent sui nodi gestiti. Gli aggiornamenti regolari aiutano a garantire prestazioni e sicurezza ottimali.

Per configurare Agente SSM aggiornamenti

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella sezione Configurazioni delle funzionalità, individua Aggiornamenti dell'.
4. Per abilitare gli aggiornamenti automatici, attiva l'interruttore.
5. Per Frequenza degli aggiornamenti, scegli la frequenza con cui desideri che Systems Manager controlli e installi gli aggiornamenti degli agenti:
 - Ogni giorno: verifica la presenza di aggiornamenti una volta al giorno
 - Settimanale: verifica la presenza di aggiornamenti una volta alla settimana
 - Mensile: verifica la presenza di aggiornamenti una volta al mese
6. Selezionare Salva.

Impostazioni di diagnosi e correzione

Le impostazioni Diagnosis and Remediate determinano se Systems Manager esegue automaticamente la scansione dei nodi per assicurarsi che possano comunicare con Systems Manager. Se abilitata, la funzionalità viene eseguita automaticamente in base a una pianificazione definita dall'utente. La funzionalità identifica quali nodi non sono in grado di connettersi a Systems Manager e perché. Questa funzionalità fornisce anche runbook consigliati per risolvere problemi di rete e altri problemi che impediscono la configurazione dei nodi come gestiti.

Pianificazione di una scansione diagnostica ricorrente

Systems Manager diagnostica e consente di risolvere al meglio diversi tipi di errori di implementazione, nonché deviazioni sulle configurazioni. Systems Manager è anche in grado di identificare le istanze di Amazon Elastic Compute Cloud (Amazon EC2) nel tuo account o organizzazione che Systems Manager non può trattare come nodi gestiti. Il processo di diagnosi delle istanze EC2 identifica problemi relativi a configurazioni errate in un cloud privato virtuale (VPC), in un'impostazione DNS (Domain Name Service) o in un gruppo di sicurezza Amazon Elastic Compute Cloud (Amazon EC2).

Per limitarsi a identificare i nodi che non possono connettersi a Systems Manager, la funzione di diagnosi ricorrente *Schedule* consente di automatizzare una scansione diagnostica ricorrente. Le scansioni consentono di identificare al meglio quali nodi non sono in grado di connettersi a Systems Manager e perché. Utilizza la seguente procedura per abilitare e configurare una scansione diagnostica ricorrente dei nodi.

Per pianificare una scansione diagnostica ricorrente

1. Apri la console all'indirizzo. AWS Systems Manager <https://console.aws.amazon.com/systems-manager/>
2. Nel riquadro di navigazione, scegli Impostazioni, quindi la scheda Diagnostica e correggi.
3. Attiva l'opzione Pianifica diagnosi ricorrenti.
4. Per Periodo di scansione, scegli la frequenza con cui desideri che venga eseguita la scansione.
5. (Facoltativo) In Ora di inizio, inserisci un'ora, in formato 24 ore, per l'inizio della diagnosi. Ad esempio, per le 20:15, inserisci **20:15**.

L'ora inserita si riferisce al fuso orario locale corrente.

Se non si specifica un orario, la scansione diagnostica verrà eseguita immediatamente. Systems Manager pianifica inoltre l'esecuzione della scansione in futuro all'ora corrente. Se si specifica un orario, Systems Manager attende l'esecuzione della scansione diagnostica all'ora specificata.

6. Selezionare Salva.
7. Al termine della scansione, visualizza i dettagli selezionando Diagnostica e correggi nel riquadro di navigazione a sinistra.

Per ulteriori informazioni sulla funzionalità Diagnostica e correggi, consulta [Diagnosi e correzione](#).

Aggiornamento della crittografia del bucket S3

Quando si esegue l'onboarding di Systems Manager, Quick Setup crea un bucket Amazon Simple Storage Service (Amazon S3) nell'account amministratore delegato per le configurazioni. AWS Organizations Per le configurazioni con account singolo, il bucket viene memorizzato nell'account da configurare. Questo bucket viene utilizzato per archiviare i metadati generati durante le scansioni diagnostiche.

Per ulteriori informazioni sulla configurazione della console unificata di Systems Manager, consulta [Configurazione AWS Systems Manager](#).

Per impostazione predefinita, i dati nel bucket sono crittografati utilizzando una chiave AWS Key Management Service (AWS KMS) che AWS possiede e gestisce per te.

Puoi scegliere di utilizzare una AWS KMS chiave diversa per la crittografia del bucket. Come altra alternativa, puoi utilizzare la crittografia lato server con AWS KMS keys (SSE-KMS) utilizzando una chiave gestita dal cliente (CMK). Per informazioni, consulta [Utilizzo dei bucket Amazon S3 e delle policy dei bucket per Systems Manager](#).

Per utilizzare una diversa AWS KMS chiave per la crittografia del bucket S3

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel riquadro di navigazione, scegli Impostazioni, quindi la scheda Diagnostica e correggi.
3. Nell'area Aggiorna la crittografia del bucket S3, scegli Modifica.
4. Seleziona la casella di controllo Personalizza le impostazioni di crittografia (avanzate).
5. Per Scegli una AWS KMS chiave, scegli o inserisci l'Amazon Resource Name (ARN) della chiave.

 Tip

Per creare una nuova chiave, scegli Crea una chiave AWS KMS .

6. Selezionare Salva.

Utilizzo dei bucket Amazon S3 e delle policy dei bucket per Systems Manager

Durante il processo di [onboarding](#) di AWS Systems Manager, Quick Setup crea un bucket Amazon Simple Storage Service (Amazon S3) nell'account amministratore delegato per le configurazioni dell'organizzazione. Per le configurazioni con account singolo, il bucket viene memorizzato nell'account da configurare.

È possibile utilizzare Systems Manager per eseguire operazioni di diagnostica sul parco istanze per identificare i casi di implementazioni fallite e configurazioni deviate. Systems Manager rileva anche i casi in cui i problemi di configurazione impediscono a Systems Manager di gestire le istanze EC2 nell'account o nell'organizzazione. I risultati di queste operazioni diagnostiche vengono archiviati in questo bucket Amazon S3, che è protetto sia da un metodo di crittografia che da una policy di bucket S3. Per informazioni sulle operazioni di diagnostica che inviano dati a questo bucket, consulta [Diagnosi e correzione](#).

Modifica del metodo di crittografia del bucket

Per impostazione predefinita, il bucket S3 utilizza la crittografia lato server con chiavi gestite da Amazon S3 (). SSE-S3

Puoi invece utilizzare la crittografia lato server con AWS KMS keys (SSE-KMS) utilizzando una chiave gestita dal cliente come alternativa alle chiavi gestite da Amazon S3, come spiegato in.

[Passare a un AWS KMS chiave gestita dal cliente per crittografare le risorse S3](#)

Contenuti della policy di bucket

La policy di bucket impedisce l'individuazione reciproca degli account dei membri di un'organizzazione. Le autorizzazioni di lettura e scrittura per il bucket sono consentite solo per i ruoli di diagnosi e riparazione creati per Systems Manager. Il contenuto di queste policy generate dal sistema è presentato su [Policy di bucket S3 per la console di Systems Manager unificata](#).

Warning

La modifica della policy predefinita di bucket consente agli account membri di un'organizzazione di scoprirsi l'un l'altro oppure di leggere i risultati di diagnosi relativi alle istanze di un altro account. Consigliamo di utilizzare estrema cautela qualora si scegliesse di modificare questa policy.

Argomenti

- [Passare a un AWS KMS chiave gestita dal cliente per crittografare le risorse S3](#)
- [Policy di bucket S3 per la console di Systems Manager unificata](#)

Passare a un AWS KMS chiave gestita dal cliente per crittografare le risorse S3

Durante il processo di onboarding per la console unificata di Systems Manager, Quick Setup crea un bucket Amazon Simple Storage Service (Amazon S3) nell'account amministratore delegato. Questo bucket viene utilizzato per archiviare i dati di output della diagnosi generati durante le esecuzioni dei runbook di correzione. Per impostazione predefinita, il bucket utilizza la crittografia lato server con chiavi gestite da Amazon S3 (). SSE-S3

È possibile esaminare il contenuto di queste policy su [Policy di bucket S3 per la console di Systems Manager unificata](#).

Tuttavia, puoi invece utilizzare la crittografia lato server con AWS KMS keys (SSE-KMS) utilizzando una chiave gestita dal cliente come alternativa a una. AWS KMS key

Completa le seguenti attività per configurare Systems Manager per l'utilizzo della tua chiave KMS.

Attività 1: Aggiungere un tag a una chiave KMS esistente

AWS Systems Manager utilizza la tua chiave KMS solo se è contrassegnata dalla seguente coppia chiave-valore:

- Chiave: `SystemsManagerManaged`
- Valore: `true`

Utilizza la seguente procedura per fornire l'accesso alla crittografia del bucket S3 con la tua chiave KMS.

Per aggiungere un tag alla tua chiave KMS esistente

1. Apri la AWS KMS console all'indirizzo. <https://console.aws.amazon.com/kms>
2. Nella sezione di navigazione a sinistra, scegli Chiavi gestite dal cliente.
3. Seleziona il AWS KMS key da utilizzare con AWS Systems Manager.
4. Seleziona la scheda Tag, quindi scegli Modifica.

5. Seleziona Aggiungi tag.
6. Esegui questa operazione:
 - a. In Chiave di tag, specifica **SystemsManagerManaged**.
 - b. In Valore del tag, inserisci **true**.
7. Selezionare Salva.

Attività 2: modificare una politica chiave KMS esistente

Utilizza la seguente procedura per aggiornare la politica delle chiavi [KMS](#) della tua chiave KMS per consentire ai AWS Systems Manager ruoli di crittografare il bucket S3 per tuo conto.

Per modificare una politica chiave KMS esistente

1. Apri la AWS KMS console all'indirizzo. <https://console.aws.amazon.com/kms>
2. Nella sezione di navigazione a sinistra, scegli Chiavi gestite dal cliente.
3. Seleziona il AWS KMS key da utilizzare con AWS Systems Manager.
4. Nella scheda Policy della chiave, seleziona Modifica.
5. Aggiungi la seguente dichiarazione JSON al Statement campo e sostituiscila *placeholder values* con le tue informazioni.

Assicurati di aggiungere sul Account AWS campo tutti gli ID integrati nella tua organizzazione.
AWS Systems Manager Principal

Per individuare il nome corretto del bucket nella console Amazon S3, nell'account amministratore delegato, individua il bucket nel formato do-not-delete-ssm-*operational-account-id-home-region-disambiguator*.

```
{
  "Sid": "EncryptionForSystemsManagerS3Bucket",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "account-id-1",
      "account-id-2",
      ...
    ]
  },
  "Action": ["kms:Decrypt", "kms:GenerateDataKey"],
```

```
"Resource": "*",
"Condition": {
  "StringEquals": {
    "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket"
  },
  "StringLike": {
    "kms:ViaService": "s3.*.amazonaws.com"
  },
  "ArnLike": {
    "aws:PrincipalArn": "arn:aws:iam::*:role/AWS-SSM-*"
  }
}
}
```

 Tip

In alternativa, puoi aggiornare la policy delle chiavi KMS utilizzando la chiave di [condizione](#) `aws:PrincipalOrg ID` per concedere AWS Systems Manager l'accesso alla tua chiave KMS.

Attività 3: Specificare la chiave KMS nelle impostazioni di Systems Manager

Dopo aver completato le due attività precedenti, utilizzare la procedura seguente per modificare la crittografia del bucket S3. Questa modifica garantisce che il processo di Quick Setup configurazione associato possa aggiungere le autorizzazioni per consentire a Systems Manager di accettare la chiave KMS.

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella scheda Diagnostica e correggi, nella sezione Aggiorna la crittografia del bucket S3, scegli Modifica.
4. Seleziona la casella di controllo Personalizza le impostazioni di crittografia (avanzate).
5. Nella casella di ricerca
()
scegli l'ID di una chiave esistente, oppure incolla l'ARN di una chiave esistente.
6. Scegli Salva.

Policy di bucket S3 per la console di Systems Manager unificata

Questo argomento include le policy di bucket di Amazon S3 create da Systems Manager quando si integra un'organizzazione o un singolo account nella console unificata di Systems Manager.

Warning

La modifica della policy di bucket predefinita consente agli account membri di un'organizzazione di scoprirsi l'un l'altro oppure di leggere i risultati di diagnosi relativi alle istanze di un altro account. Consigliamo di utilizzare estrema cautela qualora si scegliesse di modificare questa policy.

Policy del bucket Amazon S3 per un'organizzazione

Il bucket di diagnosi viene creato con la seguente policy di bucket predefinita durante l'onboarding di un'organizzazione in Systems Manager.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyHTTPRequests",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "Bool": {
          "aws:SecureTransport": "false"
        }
      }
    },
    {
      "Sid": "DenyNonSigV4Requests",
      "Effect": "Deny",
```

```

    "Principal": "*",
    "Action": "s3:*",
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ],
    "Condition": {
        "StringNotEquals": {
            "s3:SignatureVersion": "AWS4-HMAC-SHA256"
        }
    }
},
{
    "Sid": "AllowAccessLog",
    "Effect": "Allow",
    "Principal": {
        "Service": "logging.s3.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/access-logs/*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "000000000000"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-bucket"
        }
    }
},
{
    "Sid": "AllowCrossAccountRead",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/actions/*/
${aws:PrincipalAccount}/*",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "organization-id"
        }
    }
},
{
    "Sid": "AllowCrossAccountWrite",

```



```

        "Effect": "Allow",
        "Principal": "*",
        "Action": [
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws:s3:::bucket-name/actions/*/"
    },
    {
        "Sid": "${aws:PrincipalAccount}/*",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": "organization-id"
            },
            "ArnLike": {
                "aws:PrincipalArn": [
                    "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole-operational-123456789012-home-region",
                    "arn:aws:iam::*:role/AWS-SSM-DiagnosisAdminRole-operational-123456789012-home-region",
                    "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole-operational-123456789012-home-region",
                    "arn:aws:iam::*:role/AWS-SSM-RemediationAdminRole-operational-123456789012-home-region"
                ]
            }
        }
    },
    {
        "Sid": "AllowCrossAccountListUnderAccountOwnPrefix",
        "Effect": "Allow",
        "Principal": "*",
        "Action": "s3:ListBucket",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": "organization-id"
            },
            "StringLike": {
                "s3:prefix": "*/${aws:PrincipalAccount}/*"
            }
        }
    },
    {
        "Sid": "AllowCrossAccountGetConfigWithinOrganization",
        "Effect": "Allow",

```

```

        "Principal": "*",
        "Action": "s3:GetEncryptionConfiguration",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": "organization-id"
            }
        }
    }
]
}

```

Policy del bucket Amazon S3 per un singolo account

Il bucket di diagnosi viene creato con la seguente policy di bucket predefinita durante l'onboarding di un singolo account in Systems Manager.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyHTTPRequests",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "Bool": {
          "aws:SecureTransport": "false"
        }
      }
    },
    {
      "Sid": "DenyNonSigV4Requests",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",

```

```
"Resource": [  
  "arn:aws:s3:::amzn-s3-demo-bucket",  
  "arn:aws:s3:::amzn-s3-demo-bucket/*"  
],  
"Condition": {  
  "StringNotEquals": {  
    "s3:SignatureVersion": "AWS4-HMAC-SHA256"  
  }  
}  
}
```

Utilizzo AWS Systems Manager strumenti

I gruppi di strumenti di Systems Manager sono raggruppati in quattro categorie. La seguente documentazione descrive i vari strumenti AWS Systems Manager e come configurarli e utilizzarli. Scegli le schede in ciascuna categoria per ulteriori informazioni sui rispettivi strumenti.

Strumenti per nodi

Un nodo gestito è qualsiasi macchina configurata per l'uso con Systems Manager in ambienti [ibridi e multicloud](#).

Compliance

Utilizzare [Compliance](#) (Conformità) per analizzare il parco istanze di nodi gestiti per controllare la conformità della patch e individuare le incongruenze di configurazione. È possibile raccogliere e aggregare dati da più Account AWS database Regioni AWS e quindi analizzare in dettaglio risorse specifiche non conformi. Per impostazione predefinita, Compliance mostra i dati di conformità dell'applicazione di patch di Patch Manager e le associazioni di State Manager. È inoltre possibile personalizzare il servizio e creare tipi di conformità personali in base ai propri requisiti IT o aziendali.

Distributor

Utilizzare [Distributor](#) per creare e implementare i pacchetti ai nodi gestiti. ConDistributor, è possibile creare un pacchetto software personalizzato o trovare pacchetti software AWS forniti da agenti, ad esempio, da installare sui nodi gestiti di Systems AmazonCloudWatchAgent Manager. Dopo aver installato un pacchetto per la prima volta, è possibile utilizzare Distributor per disinstallare e reinstallare una nuova versione del pacchetto o eseguire un aggiornamento sul posto che aggiunga file nuovi o modificati. Distributor pubblica le risorse, ad esempio i pacchetti software, nei nodi gestiti di Systems Manager.

Fleet Manager

[Fleet Manager](#) è un'esperienza di interfaccia utente unificata che consente di gestire in remoto i nodi. Con Fleet Manager è possibile visualizzare lo stato di integrità e delle prestazioni dell'intero parco istanze da un'unica console. È inoltre possibile raccogliere dati da singoli dispositivi e istanze per eseguire processi comuni di risoluzione dei problemi e gestione dalla console. Ciò include la visualizzazione del contenuto di directory e file, la gestione del registro di Windows, la gestione degli utenti del sistema operativo e altro ancora.

Hybrid Activations

Per configurare macchine non EC2 nel tuo ambiente ibrido e multicloud come nodi gestiti, crea un'[attivazione ibrida](#). Dopo aver completato l'attivazione, l'utente riceverà un codice di attivazione e un ID. Questa combinazione codice e ID ha la stessa funzione di un ID di accesso e una chiave segreta di Amazon Elastic Compute Cloud (Amazon EC2) al fine di fornire un accesso sicuro al servizio Systems Manager dalle istanze gestite.

È inoltre possibile creare un'attivazione per i dispositivi edge se si desidera gestirli utilizzando Systems Manager.

Inventory

[Inventory](#) consente di automatizzare il processo di raccolta di inventario software dai nodi gestiti. È possibile utilizzare Inventory per raccogliere i metadati relativi ad applicazioni, file, componenti, patch e altro ancora.

Patch Manager

Utilizzare [Patch Manager](#) per automatizzare il processo di correzione dei nodi gestiti con aggiornamenti correlati alla sicurezza e di altro tipo. È possibile utilizzare Patch Manager per applicare patch sia per i sistemi operativi sia per le applicazioni. (In Windows Server, il supporto delle applicazioni è limitato ai soli aggiornamenti delle applicazioni Microsoft).

Questo strumento consente di scansionare i nodi gestiti alla ricerca di patch mancanti e di applicarle singolarmente o a grandi gruppi di nodi gestiti utilizzando i tag. Patch Manager utilizza le linee di base delle patch, che possono includere regole per l'approvazione automatica delle patch entro pochi giorni dal loro rilascio e un elenco di patch approvate e rifiutate. È possibile installare patch di sicurezza a intervalli regolari programmandone l'esecuzione come attività di manutenzione della finestra di Systems Manager oppure è possibile applicare patch ai nodi gestiti on demand in qualsiasi momento.

Per i sistemi operativi Linux, è possibile definire i repository da utilizzare per le operazioni di applicazione di patch all'interno della tua baseline delle patch. Ciò consente di assicurarsi che gli aggiornamenti vengano installati solo da repository attendibili indipendentemente dai repository configurati nel nodo gestito. Per Linux, puoi anche aggiornare qualsiasi pacchetto sul nodo gestito, non solo quelli classificati come aggiornamenti di sicurezza del sistema operativo. È inoltre possibile generare report di patch che vengono inviati a un bucket S3 a scelta dell'utente. Per un singolo nodo gestito, i report includono dettagli di tutte le patch per il computer. Per un report su tutti i nodi gestiti, viene fornito solo un riepilogo del numero di patch mancanti.

Run Command

Utilizzare [Run Command](#) per gestire da remoto e in modo sicuro la configurazione dei nodi gestiti su larga scala. Utilizza Run Command per eseguire modifiche on-demand, come ad esempio l'aggiornamento di applicazioni o l'esecuzione di script della shell Linux e comandi Windows PowerShell su una serie target di decine o centinaia di nodi gestiti.

Session Manager

Utilizzalo [Session Manager](#) per gestire i tuoi dispositivi edge e le istanze Amazon Elastic Compute Cloud (Amazon EC2) tramite una shell interattiva basata su browser in un solo passaggio o tramite AWS CLI. Session Manager fornisce una gestione sicura e verificabile dei dispositivi periferici e delle istanze senza dover aprire porte in entrata, mantenere bastion host o gestire chiavi SSH. Session Manager consente inoltre di rispettare le politiche aziendali che richiedono un accesso controllato ai dispositivi periferici, rigide pratiche di sicurezza e registri completamente verificabili con dettagli di accesso.

State Manager

Utilizzare [State Manager](#) per automatizzare il processo di mantenimento dei nodi gestiti in un determinato stato. L'utilizzo di State Manager garantisce che i nodi gestiti vengano avviati con un software specifico in fase di startup, aggiunti a un dominio Windows (solo nodi Windows Server) o con patch e con aggiornamenti software specifici.

Cambia gli strumenti di gestione

Automation

Utilizzare [Automation](#) per automatizzare le attività comuni di manutenzione e implementazione. È possibile utilizzare Automation (Automazione) per creare e aggiornare le Amazon Machine Images (AMIs) (AMI), applicare aggiornamenti di driver e agenti, reimpostare le password su un'istanza Windows Server, reimpostare chiavi SSH su istanze Linux e applicare patch dell'OS (del sistema operativo) o aggiornamenti delle applicazioni.

Modifica calendario

[Change Calendar](#) consente di impostare intervalli di data e ora quando le operazioni specificate (ad esempio, nei runbook di [Systems Manager Automation](#)) possono essere eseguite o meno nell' Account AWS. In Change Calendar, questi intervalli sono chiamati eventi. Quando si crea una voce Change Calendar, si sta creando un [documento Systems Manager](#) del tipo

ChangeCalendar. In Change Calendar, il documento memorizza i dati [iCalendar 2.0](#) in formato testo normale. Gli eventi aggiunti alla voce Change Calendar diventano parte del documento. È possibile aggiungere gli eventi manualmente nell'interfaccia Change Calendar o importare eventi da un calendario di terze parti supportato utilizzando un file .ics.

Change Manager

Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

[Change Manager](#) è un framework di gestione delle modifiche enterprise per la richiesta, l'approvazione, l'implementazione e la creazione di report sulle modifiche operative alla configurazione e all'infrastruttura delle applicazioni. Da un singolo account amministratore delegato, se lo utilizzi AWS Organizations, puoi gestire le modifiche su più Account AWS account. Regioni AWS In alternativa, utilizzando un account locale, è possibile gestire le modifiche di un singolo Account AWS. Utilizza Change Manager per la gestione delle modifiche a risorse AWS e risorse on-premises.

Documents

Un [documento di Systems Manager](#) (documento SSM) definisce le operazioni eseguite da Systems Manager. I tipi di documento SSM includono documenti Command (Comando), che vengono utilizzati da State Manager e Run Command, e runbook Automation, utilizzati da Systems Manager Automation. Systems Manager include decine di documenti preconfigurati che è possibile utilizzare specificando i parametri nel runtime (tempo di esecuzione). I documenti possono essere espressi in formato JSON o YAML e includono i passaggi e i parametri specificati dall'utente.

Intervallo di manutenzione

Utilizzare [Maintenance Windows](#) per impostare piani ricorrenti per le istanze gestite per l'esecuzione di attività amministrative, ad esempio l'installazione di patch e aggiornamenti senza interrompere operazioni business critical.

Configurazione rapida

Utilizzalo [Quick Setup](#) per configurare le funzionalità Servizi AWS e gli usi più frequenti con le best practice consigliate. Puoi Quick Setup utilizzarlo singolarmente Account AWS o in più Account AWS e Regioni AWS integrandoti con AWS Organizations. Quick Setup semplifica la configurazione dei servizi, incluso Systems Manager, automatizzando le attività comuni o consigliate. Queste attività includono, ad esempio, la creazione di ruoli di profilo delle istanze obbligatorie AWS Identity and Access Management (IAM) e l'impostazione di best practice operative, come scansioni periodiche delle patch e raccolta dell'inventario.

strumenti applicativi

AppConfig

[AppConfig](#) aiuta a creare, gestire e implementare configurazioni di applicazioni e flag di funzionalità. AppConfig supporta implementazioni controllate per applicazioni di qualsiasi dimensione. Puoi utilizzarlo AppConfig con applicazioni ospitate su istanze, AWS Lambda contenitori, applicazioni mobili o dispositivi edge di Amazon EC2. Per evitare errori durante l'implementazione delle configurazioni delle applicazioni, AppConfig include validatori. Un validatore fornisce un controllo sintattico o semantico per verificare che la configurazione da distribuire funzioni come previsto. Durante una distribuzione di configurazione, AppConfig monitora l'applicazione per verificare che la distribuzione abbia esito positivo. Se il sistema rileva un errore o se la distribuzione attiva un avviso, AppConfig ripristina la modifica per ridurre al minimo l'impatto per gli utenti dell'applicazione.

Application Manager

[Application Manager](#) aiuta DevOps gli ingegneri a indagare e risolvere i problemi con AWS le loro risorse nel contesto delle loro applicazioni e dei cluster. In Application Manager, un'applicazione è un gruppo logico di AWS risorse che si desidera utilizzare come un'unità. Questo gruppo logico può rappresentare diverse versioni di un'applicazione, limiti di proprietà per gli operatori o ambienti di sviluppo, solo per citarne alcuni. Application Manager il supporto per i cluster di container include sia i cluster Amazon Elastic Kubernetes Service (Amazon EKS) che Amazon Elastic Container Service (Amazon ECS). Application Manager aggrega le informazioni operative provenienti da più strumenti Servizi AWS e Systems Manager in un unico strumento. Console di gestione AWS

Parameter Store

[Parameter Store](#) consente di archiviare, organizzare e recuperare in modo sicuro i dati di configurazione su larga scala. Supporta un'ampia gamma di casi d'uso, dalla gestione dei valori di configurazione in testo normale, come le stringhe di connessione al database e le impostazioni delle applicazioni, alla gestione di dati sensibili come segreti per ambienti a basso rischio. Parameter Store è progettato per semplificare la gestione della configurazione tra gli ambienti, consentendo ai team di standardizzare il modo in cui le applicazioni accedono ai dati critici senza codificare i valori o affidarsi a soluzioni di storage frammentate.

Se gestisci credenziali che richiedono la rotazione automatica, l'accesso tra più account o una registrazione di controllo granulare, ti consigliamo di utilizzarle. [AWS Secrets Manager](#) Secrets Manager è stato creato appositamente per la gestione di informazioni segrete quali credenziali di database, chiavi API e informazioni segrete supportate da software di terze parti. Per ulteriori informazioni, vedi Che cos'è? [AWS Secrets Manager](#) nella Guida AWS Secrets Manager per l'utente.

Strumenti operativi

CloudWatch Dashboards

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Dashboards.html Le CloudWatch dashboard di Amazon sono pagine personalizzabili nella CloudWatch console che puoi utilizzare per monitorare le tue risorse in un'unica visualizzazione, anche quelle distribuite in diverse regioni. Puoi utilizzare i pannelli di controllo CloudWatch per creare viste personalizzate dei parametri e degli allarmi per le risorse AWS .

Explorer

[Explorer](#) è una dashboard operativa personalizzabile che riporta informazioni sulle tue AWS risorse. Explorer mostra una vista aggregata dei dati operativi (OpsData) per te Account AWS e per tutti Regioni AWS. In Explorer, OpsData include metadati sulle istanze Amazon EC2, dettagli sulla conformità delle patch e elementi di lavoro operativi (). OpsItems Explorer fornisce un contesto su come OpsItems sono distribuite tra le unità aziendali o le applicazioni, come si evolvono nel tempo e come variano in base alla categoria. È possibile raggruppare e filtrare le informazioni Explorer per concentrarti sugli elementi rilevanti e per cui è necessario prendere misure. Quando si identificano problemi ad alta priorità, è possibile utilizzarli OpsCenter per eseguire i runbook di Automation e risolverli.

Incident Manager

[Incident Manager](#) è una console di gestione degli incidenti che aiuta gli utenti a mitigare e ripristinare gli incidenti che interessano le loro AWS applicazioni ospitate.

Incident Manager aumenta la risoluzione degli incidenti notificando ai ricevitori l'effetto, evidenziando i dati pertinenti per la risoluzione dei problemi e fornendo strumenti di collaborazione per il ripristino e l'esecuzione dei servizi. Questa funzionalità automatizza inoltre i piani di risposta e consente l'escalation del team di ricevitori.

OpsCenter

[OpsCenter](#) fornisce una posizione centrale in cui ingegneri e IT professionisti operativi possono visualizzare, esaminare e risolvere gli elementi di lavoro operativi (OpsItems) relativi alle AWS risorse. OpsCenter è progettato per ridurre i tempi medi di risoluzione dei problemi che influiscono sulle AWS risorse. Questo strumento di Systems Manager aggrega e standardizza OpsItems su tutti i servizi fornendo al contempo dati investigativi contestuali su ogni OpsItem, OpsItems e risorse relativi. OpsCenter fornisce inoltre runbook di automazione di Systems Manager che è possibile utilizzare per risolvere problemi. È possibile specificare i dati ricercabili e personalizzati per ogni OpsItem. È inoltre possibile visualizzare i report di riepilogo generati automaticamente su OpsItems in base allo stato e all'origine.

Eseguire un'attività sul nodo con Systems Manager

Usa questo tutorial per iniziare AWS Systems Manager. Imparerai come avviare un'istanza Amazon Elastic Compute Cloud (Amazon EC2) gestita da Systems Manager e come connetterti all'istanza gestita.

Poiché Systems Manager è una raccolta di molteplici strumenti, nessuna singola procedura guidata o nessun singolo tutorial possono introdurre l'intero servizio. Questo tutorial fornisce un'introduzione ad alcuni strumenti.

Prerequisiti

Prima di iniziare, devi accertarti di aver completato le fasi in [Gestire le istanze EC2 con Systems Manager](#).

Avvia un'istanza utilizzando un AMI con Agente SSM preinstallato

Puoi avviare un'istanza Amazon 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 tua prima istanza gestita. 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. Dal pannello di controllo della console EC2, nella casella Launch instance (Avvia istanza), scegli Launch instance (Avvia istanza), quindi scegli Launch instance (Avvia istanza) dalle opzioni visualizzate.
3. In Nome e tag, per Nome inserisci un nome descrittivo per l'istanza.
4. In Immagini di applicazioni e sistema operativo (Amazon Machine Image), esegui le seguenti operazioni:
 - a. Scegli la scheda Avvio rapido, quindi scegli Amazon Linux. Questo è il sistema operativo (OS) per l'istanza.
 - b. In Amazon Machine Image (AMI), scegli una versione HVM di Amazon Linux 2.
5. In Tipo di istanza, dall'elenco Tipo di istanza scegli la configurazione hardware per l'istanza. Scegliere il tipo di istanza `t2.micro`, selezionato per impostazione di default. Il tipo di `t2.micro` istanza è idoneo per il piano AWS gratuito. Nelle Regioni AWS in cui `t2.micro` non è disponibile, è possibile utilizzare un'istanza `t3.micro` nell'ambito del Piano gratuito. Per ulteriori informazioni, consulta [Piano gratuito AWS](#).
6. Per Coppia di chiavi (login), per Nome della coppia di chiavi scegli una coppia di chiavi.
7. Per Impostazioni di rete, scegli Modifica. Per Nome del gruppo di sicurezza, osserva che la procedura guidata ha creato e selezionato un gruppo di sicurezza per tuo conto. È possibile utilizzare questo gruppo di sicurezza o, in alternativa, il gruppo di sicurezza creato durante la configurazione seguendo i passi descritti di seguito:
 - a. Scegli Select existing security group (Seleziona un gruppo di sicurezza esistente).
 - b. Da Common security groups (Gruppi di sicurezza comuni), scegli il gruppo di sicurezza dall'elenco dei gruppi di sicurezza esistenti.
8. Se non stai utilizzando la configurazione predefinita di gestione dell'host, espandi la sezione Dettagli avanzati. Per il profilo dell'istanza IAM, scegli il profilo di istanza in cui hai creato [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#).

9. Mantieni le selezioni di default per le altre impostazioni di configurazione dell'istanza.
10. Rivedi un riepilogo della configurazione dell'istanza nel riquadro Riepilogo. Al termine, scegli **Avvia istanza**.
11. Una pagina di conferma ti informa che l'istanza si sta avviando. Scegli **View Instances** (Visualizza istanze) per chiudere la pagina di conferma e tornare alla console.
12. Nella schermata **Instances** (Istanze), è possibile visualizzare lo stato dell'avvio. L'avvio di un'istanza richiede pochi minuti.
13. Possono essere necessari alcuni minuti prima che l'istanza venga mostrata come gestita e sia pronta per stabilire una connessione a essa. Controlla che l'istanza abbia superato i controlli relativi allo stato. Puoi visualizzare queste informazioni nella colonna **Verifica dello stato**.

Connessione all'istanza gestita tramite Systems Manager

Connessione all'istanza gestita

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli **Fleet Manager**.
3. Scegli il pulsante accanto all'istanza a cui ci si vuole connettere.
4. Nel menu **Operazioni del nodo**, scegli **Avvia sessione terminale**.
5. Seleziona **Connetti**.

Pulizia dell'istanza

Se hai finito di utilizzare l'istanza gestita che hai creato per questo tutorial, puoi terminarla. Se termini un'istanza, questa viene eliminata definitivamente.

Per terminare l'istanza

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, scegliere **Instances** (Istanze). Nell'elenco delle istanze, selezionare l'istanza.
3. Scegli **Instance state** (Stato istanza), **Terminate instance** (Termina istanza).
4. Quando viene richiesta la conferma, seleziona **Terminate** (Interrompi).

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 viene eliminata automaticamente. Non è possibile rimuovere in autonomia l'istanza terminata dal display della console.

AWS Systems Manager Strumenti per nodi

AWS Systems Manager fornisce i seguenti strumenti per accedere, gestire e configurare i nodi gestiti. Un nodo gestito è qualsiasi macchina configurata per l'uso con Systems Manager in un ambiente [ibrido e multicloud](#).

Argomenti

- [AWS Systems Manager Conformità](#)
- [AWS Systems Manager Distributor](#)
- [AWS Systems Manager Fleet Manager](#)
- [AWS Systems Manager Attivazioni ibride](#)
- [AWS Systems Manager Inventory](#)
- [AWS Systems Manager Patch Manager](#)
- [AWS Systems Manager Run Command](#)
- [AWS Systems Manager Session Manager](#)
- [AWS Systems Manager State Manager](#)

AWS Systems Manager Conformità

Puoi utilizzare Compliance per scansionare la tua flotta di nodi gestiti per verificare la conformità delle patch e le incoerenze di configurazione. Puoi raccogliere e aggregare dati da più regioni Account AWS e quindi analizzare in dettaglio le risorse specifiche che non sono conformi. Per impostazione predefinita, Conformità visualizza i dati di conformità correnti sull'applicazione di patch in Patch Manager e sulle associazioni in State Manager. (Patch Manager e State Manager sono strumenti di AWS Systems Manager.) Per iniziare a utilizzare Conformità, apri la [console di Systems Manager](#). Nel riquadro di navigazione, seleziona Conformità.

I dati sulla conformità delle patch da Patch Manager possono essere inviati a AWS Security Hub CSPM. Security Hub CSPM offre una visione completa degli avvisi di sicurezza ad alta priorità e dello

stato di conformità. Monitora anche lo stato di applicazione di patch del parco istanze. Per ulteriori informazioni, consulta [Integrazione Patch Manager con AWS Security Hub CSPM](#).

Conformità offre gli ulteriori vantaggi e funzionalità seguenti:

- Visualizzazione della cronologia della conformità e monitoraggio delle modifiche per i dati relativi alle patch di Patch Manager e alle associazioni State Manager utilizzando AWS Config.
- Personalizzazione di Conformità per creare tipi di conformità in base a requisiti aziendali o IT specifici.
- Risolvi i problemi utilizzando Run Command un altro strumento in AWS Systems Manager Amazon. State Manager EventBridge
- Trasferisci i dati su Amazon Athena e Amazon Quick per generare report a livello di flotta.

EventBridge supporto

Questo strumento Systems Manager è supportato come tipo di evento nelle EventBridge regole di Amazon. Per informazioni, consulta [Monitoraggio degli eventi di Systems Manager con Amazon EventBridge](#) e [Riferimento: modelli e tipi di EventBridge eventi Amazon per Systems Manager](#).

Chef InSpec integrazione

Systems Manager si integra con [Chef InSpec](#). InSpec è un framework di runtime open source che consente di creare profili leggibili dall'uomo su GitHub Amazon Simple Storage Service (Amazon S3). È quindi possibile utilizzare Systems Manager per eseguire analisi della conformità e visualizzare i nodi gestiti conformi e non conformi. Per ulteriori informazioni, consulta [Utilizzo Chef InSpec profili con Systems Manager Compliance](#).

Prezzi

Conformità è disponibile senza costi aggiuntivi. Paghi solo per le risorse che utilizzi. AWS

Indice

- [Nozioni di base su Conformità](#)
- [Configurazione delle autorizzazioni per la conformità](#)
- [Creazione di una sincronizzazione dei dati delle risorse per Conformità](#)
- [Scopri i dettagli sulla conformità](#)
- [Eliminazione di una sincronizzazione dei dati delle risorse per Compliance](#)

- [Risolvere i problemi di conformità utilizzando EventBridge](#)
- [Assegna metadati di conformità personalizzati utilizzando AWS CLI](#)

Nozioni di base su Conformità

Per iniziare con la conformità, completa le seguenti attività.

Processo	Ulteriori informazioni
Conformità opera con i dati delle patch in Patch Manager e le associazioni in State Manager. (Patch Manager e State Manager sono ugualmente strumenti di AWS Systems Manager.) Conformità funziona anche con i tipi di conformità personalizzati nei nodi gestiti tramite Systems Manager. Verifica di aver completato i requisiti di configurazione per le istanze Amazon Elastic Compute Cloud (Amazon EC2) e le macchine non EC2 in un ambiente ibrido e multicloud .	Configurazione della console unificata di Systems Manager per un'organizzazione
Aggiorna il ruolo AWS Identity and Access Management (IAM) utilizzato dai nodi gestiti per limitare le autorizzazioni di conformità.	Configurazione delle autorizzazioni per la conformità
Se intendi monitorare la conformità delle patch, verifica di aver configurato Patch Manager. Affinché Conformità possa visualizzare i dati di conformità delle patch, è prima necessario eseguire operazioni di applicazione di patch con Patch Manager.	AWS Systems Manager Patch Manager
Se intendi monitorare la conformità delle associazioni, verifica di aver creato associazioni State Manager. Affinché Conformità possa visualizzare i dati di conformità delle associazioni, è necessario creare prima associazioni.	AWS Systems Manager State Manager

Processo	Ulteriori informazioni
(Facoltativo) Configurazione del sistema per visualizzare la cronologia della conformità e il monitoraggio delle modifiche.	Visualizzazione della cronologia e del monitoraggio delle modifiche della configurazione di conformità
(Facoltativa) Creazione di tipi di conformità personalizzati.	Assegna metadati di conformità personalizzati utilizzando AWS CLI
(Facoltativo) Creazione di una sincronizzazione dei dati delle risorse per aggregare tutti i dati di conformità in un bucket Amazon Simple Storage Service (Amazon S3) di destinazione.	Creazione di una sincronizzazione dei dati delle risorse per Conformità

Configurazione delle autorizzazioni per la conformità

Come best practice, aggiorna il ruolo AWS Identity and Access Management (IAM) utilizzato dai nodi gestiti con le seguenti autorizzazioni. Ciò limita la capacità del nodo di utilizzare l'azione [PutComplianceItems](#) API, che registra un tipo di conformità e altri dettagli su una risorsa come un nodo gestito.

Se il tuo nodo è un'istanza Amazon EC2, devi aggiornare il profilo dell'istanza IAM utilizzato dall'istanza con le seguenti autorizzazioni. Per ulteriori informazioni sui profili dell'istanza per le istanze EC2 gestite da Systems Manager, consulta [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#). Per altri tipi di nodi gestiti, aggiorna il ruolo IAM utilizzato dal nodo con le seguenti autorizzazioni. Per ulteriori informazioni, consulta [Aggiornare autorizzazioni per un ruolo](#) nella Guida per l'utente IAM.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutComplianceItems"
      ],

```



```

        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "ec2:SourceInstanceARN": "${ec2:SourceInstanceARN}"
            }
        },
    },
    {
        "Effect": "Allow",
        "Action": [
            "ssm:PutComplianceItems"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "ssm:SourceInstanceARN": "${ssm:SourceInstanceARN}"
            }
        }
    }
}
]
}

```

Creazione di una sincronizzazione dei dati delle risorse per Conformità

Puoi utilizzare la funzionalità di sincronizzazione dei dati delle risorse AWS Systems Manager per inviare dati di conformità da tutti i nodi gestiti a un bucket Amazon Simple Storage Service (Amazon S3) di destinazione. Quando crei la sincronizzazione, puoi specificare nodi gestiti da più nodi e il tuo Account AWS ambiente Regioni AWS [ibrido e multicloud](#). La sincronizzazione dei dati delle risorse aggiorna quindi automaticamente i dati centralizzati quando vengono raccolti nuovi dati di conformità. Con tutti i dati di conformità archiviati in un bucket S3 di destinazione, puoi utilizzare servizi come Amazon Athena e Amazon Quick per interrogare e analizzare i dati aggregati. La configurazione della sincronizzazione dei dati delle risorse per Conformità è un'operazione una tantum.

Utilizza la procedura seguente per creare una sincronizzazione dei dati delle risorse per Conformità con la Console di gestione AWS.

Creazione e configurazione di un bucket S3 per la sincronizzazione dei dati della risorsa (console)

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>

2. Crea un bucket in cui archiviare i dati di conformità aggregati. Per ulteriori informazioni, consulta [Create a Bucket \(Creazione di un bucket\)](#) nella Guida per l'utente di Amazon Simple Storage Service. Prendi nota del nome del bucket e del Regione AWS luogo in cui lo hai creato.
3. Apri il bucket, scegli la scheda Autorizzazioni, quindi Policy di bucket.
4. Copia e incolla la policy di bucket seguente nell'editor di policy. Sostituisci `amzn-s3-demo-bucket` e `Account-ID` con il nome del bucket S3 che hai creato e un ID valido. Account AWS Facoltativamente, sostituirlo `Bucket-Prefix` con il nome di un prefisso Amazon S3 (sottodirectory). Se non hai creato un prefisso, rimuovi `Bucket-Prefix` dall'ARN nella policy.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSMBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    },
    {
      "Sid": "SSMBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket/Bucket-Prefix/*/"
accountid=111122223333/*"],
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Come creare una sincronizzazione dei dati delle risorse

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegliere Account management (Gestione account), Resource Data Syncs (Sincronizzazioni dei dati delle risorse) e quindi Create resource data sync (Crea sincronizzazione dati risorsa).
4. Nel campo Sync name (Nome sincronizzazione) digitare un nome per la configurazione di sincronizzazione.
5. Nel campo Nome del bucket, digita il nome del bucket Amazon S3 creato all'inizio di questa procedura.
6. (Facoltativo) Nel campo Prefisso bucket, inserisci il nome del prefisso di un bucket S3 (sottodirectory).
7. Nel campo Regione bucket, scegli Questa Regione, se il bucket S3 creato si trova nella Regione AWS corrente. Se il bucket si trova in un'altra regione Regione AWS, scegli Un'altra regione e inserisci il nome della regione.

Note

Se la sincronizzazione e il bucket S3 target si trovano in Regioni diverse, potrebbero essere applicati i prezzi per il trasferimento dei dati. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

8. Scegli Create (Crea).

Scopri i dettagli sulla conformità

La conformità raccoglie e riporta i dati sullo stato dell'applicazione delle Patch Manager patch e delle associazioni in. State Manager (Patch Manager State Manager sono anche entrambi gli strumenti in.) AWS Systems Manager Conformità riporta inoltre tipi di conformità personalizzati specificati per i nodi gestiti. Questa sezione contiene informazioni dettagliate su ognuno di questi tipi di conformità e su come visualizzare i dati di conformità di Systems Manager. Include inoltre informazioni su come visualizzare la cronologia della conformità e il monitoraggio delle modifiche.

 Note

Systems Manager si integra con [Chef InSpec](#). InSpec è un framework di runtime open source che consente di creare profili leggibili dall'uomo su GitHub Amazon Simple Storage Service (Amazon S3). È quindi possibile utilizzare Systems Manager per eseguire analisi della conformità e visualizzare le istanze conformi e non conformi. Per ulteriori informazioni, consulta [Utilizzo Chef InSpec profili con Systems Manager Compliance](#).

Informazioni sulla conformità delle patch

Dopo l'utilizzo di Patch Manager per l'installazione di patch nelle istanze, le informazioni sullo stato di conformità sono immediatamente disponibili nella console oppure in risposta a comandi AWS Command Line Interface (AWS CLI) o a operazioni API corrispondenti di Systems Manager.

Per informazioni sui valori dello stato di conformità delle patch, consulta [Valori dello stato di conformità delle patch](#).

Informazioni State Manager conformità delle associazioni

Dopo aver creato una o più State Manager associazioni, le informazioni sullo stato di conformità sono immediatamente disponibili nella console o in risposta ai AWS CLI comandi o alle corrispondenti operazioni dell'API di Systems Manager. Per le associazioni, Compliance mostra lo stato `Compliant` o `Non-compliant` e il livello di gravità assegnato all'associazione, ad esempio `Critical` o `Medium`.

Quando State Manager esegue un'associazione su un nodo gestito, attiva un processo di aggregazione della conformità, che aggiorna lo stato di conformità per tutte le associazioni su quel nodo. Il valore `ExecutionTime` nei report di conformità indica quando lo stato di conformità è stato acquisito da Systems Manager, non quando l'associazione è stata eseguita sul nodo gestito. Ciò significa che numerose associazioni potrebbero visualizzare valori `ExecutionTime` identici, anche se sono state eseguite in momenti diversi. Per determinare i tempi effettivi di esecuzione delle associazioni, fate riferimento alla cronologia di esecuzione dell'associazione utilizzando il AWS CLI comando [describe-association-execution-targets](#) o visualizzando i dettagli di esecuzione nella console.

Informazioni sulla personalizzazione della conformità

È possibile assegnare metadati di conformità a un nodo gestito. Tali metadati possono quindi essere aggregati ad altri dati di conformità per la creazione di report di conformità. Supponiamo ad esempio

che l'azienda esegua le versioni 2.0, 3.0 e 4.0 del software X nei nodi gestiti. Se l'azienda desidera standardizzare la versione 4.0, le istanze che eseguono le versioni 2.0 e 3.0 sono non conformi. È possibile utilizzare l'operazione [PutComplianceItems](#) API per annotare in modo esplicito quali nodi gestiti eseguono versioni precedenti del software X. È possibile assegnare i metadati di conformità solo utilizzando AWS CLI AWS Tools for Windows PowerShell, o gli SDK. Il comando di esempio riportato di seguito della CLI assegna metadati di conformità a un'istanza gestita e specifica il tipo di conformità nel formato obbligatorio Custom: . Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux & macOS

```
aws ssm put-compliance-items \  
  --resource-id i-1234567890abcdef0 \  
  --resource-type ManagedInstance \  
  --compliance-type Custom:SoftwareXCheck \  
  --execution-summary ExecutionTime=AnyStringToDenoteTimeOrDate \  
  --items  
  Id=Version2.0,Title=SoftwareXVersion,Severity=CRITICAL,Status=NON_COMPLIANT
```

Windows

```
aws ssm put-compliance-items ^  
  --resource-id i-1234567890abcdef0 ^  
  --resource-type ManagedInstance ^  
  --compliance-type Custom:SoftwareXCheck ^  
  --execution-summary ExecutionTime=AnyStringToDenoteTimeOrDate ^  
  --items  
  Id=Version2.0,Title=SoftwareXVersion,Severity=CRITICAL,Status=NON_COMPLIANT
```

Note

Il parametro `ResourceType` supporta solo `ManagedInstance`. Se si aggiunge la conformità personalizzata a un dispositivo core gestito AWS IoT Greengrass , è necessario specificare un `ResourceType` di `ManagedInstance`.

I gestori della conformità possono quindi visualizzare riepiloghi o creare report su quali nodi gestiti siano conformi e quali non lo siano. A un nodo è possibile assegnare un massimo di 10 diversi tipi di conformità personalizzati.

Per un esempio di come creare un tipo di conformità personalizzato e visualizzare i dati di conformità, consulta [Assegna metadati di conformità personalizzati utilizzando AWS CLI](#).

Visualizzazione dei dati di conformità correnti

Questa sezione illustra come visualizzare i dati di conformità nella console Systems Manager e mediante AWS CLI. Per informazioni su come visualizzare la cronologia della conformità e il monitoraggio delle modifiche di patch e associazioni, consulta [Visualizzazione della cronologia e del monitoraggio delle modifiche della configurazione di conformità](#).

Argomenti

- [Visualizzazione dei dati di conformità correnti \(console\)](#)
- [Visualizzazione dei dati di conformità correnti \(AWS CLI\)](#)

Visualizzazione dei dati di conformità correnti (console)

Per visualizzare i dati di conformità nella console Systems Manager, utilizza la procedura seguente.

Visualizzazione dei report di conformità correnti nella console Systems Manager

1. Apri la console all'indirizzo. AWS Systems Manager <https://console.aws.amazon.com/systems-manager/>
2. Nel riquadro di navigazione, seleziona Conformità.
3. Nella sezione Filtro del pannello di controllo di conformità, seleziona un'opzione per filtrare i dati di conformità. La sezione Riepilogo risorse di conformità mostra il numero di dati di conformità in base al filtro scelto.
4. Per eseguire il drill down in una risorsa per ulteriori informazioni, scorri verso il basso fino all'area Panoramica dettagliata delle risorse e scegli l'ID di un nodo gestito.
5. Nella pagina dei dettagli ID istanza o in Nome seleziona la scheda Conformità di configurazione per visualizzare il report dettagliato sulla conformità di configurazione del nodo gestito.

Note

Per informazioni sulla risoluzione dei problemi di conformità, consulta [Risolvere i problemi di conformità utilizzando EventBridge](#).

Visualizzazione dei dati di conformità correnti (AWS CLI)

È possibile visualizzare i riepiloghi dei dati di conformità per l'applicazione di patch, le associazioni e i tipi di conformità personalizzati in formato inthe AWS CLI utilizzando i seguenti AWS CLI comandi.

[list-compliance-summaries](#)

Restituisce un conteggio riepilogativo dello stato conforme e non conforme delle associazioni in base al filtro specificato. (API:) [ListComplianceSummaries](#)

[list-resource-compliance-summaries](#)

Restituisce un conteggio riepilogativo a livello di risorsa. Il riepilogo contiene informazioni sullo stato conforme e non conforme e conteggi dettagliati della gravità delle voci di conformità in base alle opzioni di filtro specificate. (API: [ListResourceComplianceSummaries](#))

È possibile visualizzare ulteriori dati di conformità per l'applicazione di patch utilizzando i comandi dell' AWS CLI riportati di seguito.

[describe-patch-group-state](#)

Restituisce lo stato di conformità aggregato generale delle patch di un gruppo di patch. (API: [DescribePatchGroupState](#))

[describe-instance-patch-states-for-patch-group](#)

Restituisce lo stato generale delle patch del gruppo di patch specificato per le istanze. (API: [DescribeInstancePatchStatesForPatchGroup](#))

Note

Per un'illustrazione di come configurare l'applicazione delle patch e visualizzare i dettagli sulla conformità delle patch utilizzando AWS CLI, vedere. [Tutorial: applicare patch a un ambiente server utilizzando AWS CLI](#)

Visualizzazione della cronologia e del monitoraggio delle modifiche della configurazione di conformità

Conformità di Systems Manager mostra i dati di conformità correnti relativi all'applicazione delle patch e alle associazioni per i nodi gestiti. È possibile visualizzare la cronologia della conformità delle patch e delle associazioni e il monitoraggio delle modifiche utilizzando. [AWS Config](#) AWS Config fornisce

una visualizzazione dettagliata della configurazione delle AWS risorse nel tuo Account AWS. Questo include le relazioni tra le risorse e la maniera in cui sono state configurate in passato, in modo che tu possa vedere come le configurazioni e le relazioni cambiano nel corso del tempo. Per visualizzare la cronologia della conformità e il monitoraggio delle modifiche per l'applicazione delle patch e le associazioni, è necessario abilitare le risorse seguenti in AWS Config:

- SSM:PatchCompliance
- SSM:AssociationCompliance

Per informazioni su come scegliere e configurare queste specifiche risorse in AWS Config, consulta [Scegli quali risorse deve registrare AWS Config](#) nella AWS Config Guida per gli sviluppatori.

Note

Per informazioni sui AWS Config prezzi, vedi [Prezzi](#).

Eliminazione di una sincronizzazione dei dati delle risorse per Compliance

Se non desideri più utilizzare AWS Systems Manager Compliance per visualizzare i dati sulla conformità, ti consigliamo di eliminare le sincronizzazioni dei dati delle risorse utilizzate per la raccolta dei dati sulla conformità.

Per eliminare una sincronizzazione dei dati delle risorse in Compliance

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegliere Gestione dell'account, Sincronizzazione dei dati delle risorse.
4. Scegliere un sync dall'elenco.

Important

Assicurati di scegliere la sincronizzazione utilizzata per Compliance. Systems Manager supporta la sincronizzazione dei dati delle risorse per molteplici strumenti. Se si sceglie la sincronizzazione errata, è possibile interrompere l'aggregazione dei dati per Systems Manager Explorer o l'Inventario di Systems Manager.

5. Scegli Elimina.
6. Elimina il bucket Amazon Simple Storage Service (Amazon S3) in cui sono stati memorizzati i dati. Per informazioni sull'eliminazione di un bucket S3, consulta la pagina [Eliminazione di un bucket](#).

Risolvere i problemi di conformità utilizzando EventBridge

È possibile risolvere rapidamente i problemi di conformità di patch e associazione utilizzando Run Command, uno strumento di AWS Systems Manager. Puoi scegliere come target gli ID o i tag dell'istanza o del dispositivo AWS IoT Greengrass principale ed eseguire il `AWS-RunPatchBaseline` documento o il `AWS-RefreshAssociation` documento. Se il problema di conformità non viene risolto aggiornando l'associazione o rieseguendo la baseline delle patch, è necessario esaminare le associazioni, le baseline delle patch o le configurazioni delle istanze per comprendere il motivo per cui le operazioni di Run Command non hanno risolto il problema.

Per ulteriori informazioni sull'applicazione di patch, consulta [AWS Systems Manager Patch Manager](#) e [Documento di comando SSM per l'applicazione di patch: AWS-RunPatchBaseline](#).

Per ulteriori informazioni sulle associazioni, consulta [Utilizzo delle associazioni in Systems Manager](#).

Per ulteriori informazioni sull'esecuzione di un comando, consulta [AWS Systems Manager Run Command](#).

Specifica la conformità come obiettivo di un EventBridge evento

Puoi anche configurare Amazon EventBridge per eseguire un'azione in risposta agli eventi di conformità di Systems Manager. Ad esempio, se i nodi non riescono a installare le patch critiche o a eseguire un'associazione anti-virus, puoi configurare l'esecuzione `AWS-RunPatchBaseline` o il momento EventBridge in `AWS-RefreshAssociation` cui si verifica l'evento Compliance.

Utilizzate la procedura seguente per configurare Compliance come obiettivo di un EventBridge evento.

Per configurare Compliance come destinazione di un EventBridge evento (console)

1. Apri la EventBridge console Amazon all'indirizzo <https://console.aws.amazon.com/events/>.
2. Nel pannello di navigazione, scegli Regole.
3. Scegli Crea regola.

4. Inserisci un nome e una descrizione per la regola.

Una regola non può avere lo stesso nome di un'altra regola nello stesso bus di eventi Regione AWS e sullo stesso bus.

5. Per Router di eventi, scegli quello che desideri associare a questa regola. Se desideri che questa regola risponda agli eventi corrispondenti che provengono dai tuoi Account AWS, seleziona predefinito. Quando un Servizio AWS utente del tuo account emette un evento, viene sempre indirizzato al bus eventi predefinito del tuo account.
6. Per Tipo di regola, scegli Regola con un modello di eventi.
7. Scegli Next (Successivo).
8. Per Origine degli eventi, scegli AWS eventi o eventi EventBridge partner.
9. Nella sezione Modello di eventi, scegli Modulo di modello di eventi.
10. Per Origine evento, scegli Servizi AWS .
11. Per AWS , scegli Systems Manager.
12. Nel campo Tipo di evento scegli Conformità.
13. Per Tipi di dettagli specifici, scegli Modifica dello stato di conformità della configurazione.
14. Scegli Next (Successivo).
15. Per Tipi di destinazione, scegli servizio AWS .
16. Per Select a target (Seleziona una destinazione), scegli Systems ManagerRun Command.
17. Nell'elenco Document (Documento), scegliere un documento Systems Manager (documento SSM) da eseguire quando viene richiamata la destinazione. Ad esempio, scegliere AWS-RunPatchBaselineper un evento di patch non conforme o AWS-RefreshAssociation per un evento di associazione non conforme.
18. Specificare le informazioni per i campi e i parametri rimanenti.

 Note

I campi e i parametri obbligatori sono contrassegnati da un asterisco (*) accanto al nome. Per creare un target, è necessario specificare un valore per ogni parametro o campo obbligatorio. In caso contrario, la regola viene creata dal sistema ma non verrà eseguita.

19. Scegli Next (Successivo).
20. (Facoltativo) Inserire uno o più tag per la regola. Per ulteriori informazioni, consulta [Tagging Your Amazon EventBridge Resources](#) nella Amazon EventBridge User Guide.

21. Scegli Next (Successivo).
22. Rivedi i dettagli della regola e scegli Crea regola.

Assegna metadati di conformità personalizzati utilizzando AWS CLI

La procedura seguente illustra il processo di utilizzo di AWS Command Line Interface (AWS CLI) per chiamare l'operazione AWS Systems Manager [PutComplianceItems](#) API per assegnare metadati di conformità personalizzati a una risorsa. Questa operazione API può anche essere utilizzata per assegnare manualmente metadati di conformità delle patch e delle associazioni a un nodo gestito, come illustrato nella procedura dettagliata seguente. Per ulteriori informazioni sulla personalizzazione della conformità, consulta [Informazioni sulla personalizzazione della conformità](#).

Per assegnare metadati di conformità personalizzati a un'istanza gestita (AWS CLI)

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Eseguire questo comando per assegnare metadati di conformità personalizzati a un nodo gestito. Sostituisci ogni *example resource placeholder* con le tue informazioni. Il parametro ResourceType supporta solo un valore di ManagedInstance. Specificate questo valore anche se state assegnando metadati di conformità personalizzati a un dispositivo AWS IoT Greengrass principale gestito.

Linux & macOS

```
aws ssm put-compliance-items \
  --resource-id instance_ID \
  --resource-type ManagedInstance \
  --compliance-type Custom:user-defined_string \
  --execution-summary ExecutionTime=user-defined_time_and/or_date_value \
  --items Id=user-defined_ID,Title=user-
defined_title,Severity=one_or_more_comma-separated_severities:CRITICAL, MAJOR,
MINOR, INFORMATIONAL, or UNSPECIFIED, Status=COMPLIANT or NON_COMPLIANT
```

Windows

```
aws ssm put-compliance-items ^
  --resource-id instance_ID ^
```

```
--resource-type ManagedInstance ^
--compliance-type Custom:user-defined_string ^
--execution-summary ExecutionTime=user-defined_time_and/or_date_value ^
--items Id=user-defined_ID,Title=user-
defined_title,Severity=one_or_more_comma-separated_severities:CRITICAL, MAJOR,
MINOR,INFORMATIONAL, or UNSPECIFIED,Status=COMPLIANT or NON_COMPLIANT
```

3. Ripetere il passaggio precedente per assegnare ulteriori metadati di conformità personalizzati a uno o più nodi. È anche possibile assegnare manualmente metadati di conformità delle patch o delle associazioni ai nodi gestiti utilizzando i comandi riportati di seguito:

Metadati di conformità delle associazioni

Linux & macOS

```
aws ssm put-compliance-items \
  --resource-id instance_ID \
  --resource-type ManagedInstance \
  --compliance-type Association \
  --execution-summary ExecutionTime=user-defined_time_and/or_date_value \
  --items Id=user-defined_ID,Title=user-
defined_title,Severity=one_or_more_comma-separated_severities:CRITICAL, MAJOR,
MINOR,INFORMATIONAL, or UNSPECIFIED,Status=COMPLIANT or NON_COMPLIANT
```

Windows

```
aws ssm put-compliance-items ^
  --resource-id instance_ID ^
  --resource-type ManagedInstance ^
  --compliance-type Association ^
  --execution-summary ExecutionTime=user-defined_time_and/or_date_value ^
  --items Id=user-defined_ID,Title=user-
defined_title,Severity=one_or_more_comma-separated_severities:CRITICAL, MAJOR,
MINOR,INFORMATIONAL, or UNSPECIFIED,Status=COMPLIANT or NON_COMPLIANT
```

Metadati di conformità delle patch

Linux & macOS

```
aws ssm put-compliance-items \
  --resource-id instance_ID \
```

```
--resource-type ManagedInstance \
--compliance-type Patch \
--execution-summary ExecutionTime=user-defined_time_and/
or_date_value,ExecutionId=user-defined_ID,ExecutionType=Command \
--items Id=for_example, KB12345,Title=user-
defined_title,Severity=one_or_more_comma-separated_severities:CRITICAL,
MAJOR, MINOR, INFORMATIONAL, or UNSPECIFIED,Status=COMPLIANT or
NON_COMPLIANT,Details="{PatchGroup=name_of_group,PatchSeverity=the_patch_severity,
for example, CRITICAL}"
```

Windows

```
aws ssm put-compliance-items ^
--resource-id instance_ID ^
--resource-type ManagedInstance ^
--compliance-type Patch ^
--execution-summary ExecutionTime=user-defined_time_and/
or_date_value,ExecutionId=user-defined_ID,ExecutionType=Command ^
--items Id=for_example, KB12345,Title=user-
defined_title,Severity=one_or_more_comma-separated_severities:CRITICAL,
MAJOR, MINOR, INFORMATIONAL, or UNSPECIFIED,Status=COMPLIANT or
NON_COMPLIANT,Details="{PatchGroup=name_of_group,PatchSeverity=the_patch_severity,
for example, CRITICAL}"
```

4. Eseguire questo comando per visualizzare un elenco delle voci di conformità per uno specifico nodo gestito. Utilizzare filtri per esplorare dati di conformità specifici.

Linux & macOS

```
aws ssm list-compliance-items \
--resource-ids instance_ID \
--resource-types ManagedInstance \
--filters one_or_more_filters
```

Windows

```
aws ssm list-compliance-items ^
--resource-ids instance_ID ^
--resource-types ManagedInstance ^
--filters one_or_more_filters
```

Gli esempi seguenti illustrano come utilizzare questo comando con i filtri.

Linux & macOS

```
aws ssm list-compliance-items \  
  --resource-ids i-02573cafcfEXAMPLE \  
  --resource-type ManagedInstance \  
  --filters Key=DocumentName,Values=AWS-RunPowerShellScript  
Key=Status,Values=NON_COMPLIANT,Type=NotEqual  
Key=Id,Values=cee20ae7-6388-488e-8be1-a88ccEXAMPLE  
Key=Severity,Values=UNSPECIFIED
```

Windows

```
aws ssm list-compliance-items ^  
  --resource-ids i-02573cafcfEXAMPLE ^  
  --resource-type ManagedInstance ^  
  --filters Key=DocumentName,Values=AWS-RunPowerShellScript  
Key=Status,Values=NON_COMPLIANT,Type=NotEqual  
Key=Id,Values=cee20ae7-6388-488e-8be1-a88ccEXAMPLE  
Key=Severity,Values=UNSPECIFIED
```

Linux & macOS

```
aws ssm list-resource-compliance-summaries \  
  --filters Key=OverallSeverity,Values=UNSPECIFIED
```

Windows

```
aws ssm list-resource-compliance-summaries ^  
  --filters Key=OverallSeverity,Values=UNSPECIFIED
```

Linux & macOS

```
aws ssm list-resource-compliance-summaries \  
  --filters Key=OverallSeverity,Values=UNSPECIFIED  
Key=ComplianceType,Values=Association Key=InstanceId,Values=i-02573cafcfEXAMPLE
```

Windows

```
aws ssm list-resource-compliance-summaries ^  
  --filters Key=OverallSeverity,Values=UNSPECIFIED  
  Key=ComplianceType,Values=Association Key=InstanceId,Values=i-02573cafcfEXAMPLE
```

5. Esegui questo comando per visualizzare un riepilogo degli stati di conformità. Utilizzare filtri per esplorare dati di conformità specifici.

```
aws ssm list-resource-compliance-summaries --filters One or more filters.
```

Gli esempi seguenti illustrano come utilizzare questo comando con i filtri.

Linux & macOS

```
aws ssm list-resource-compliance-summaries \  
  --filters Key=ExecutionType,Values=Command
```

Windows

```
aws ssm list-resource-compliance-summaries ^  
  --filters Key=ExecutionType,Values=Command
```

Linux & macOS

```
aws ssm list-resource-compliance-summaries \  
  --filters Key=AWS:InstanceInformation.PlatformType,Values=Windows  
  Key=OverallSeverity,Values=CRITICAL
```

Windows

```
aws ssm list-resource-compliance-summaries ^  
  --filters Key=AWS:InstanceInformation.PlatformType,Values=Windows  
  Key=OverallSeverity,Values=CRITICAL
```

6. Esegui questo comando per visualizzare un conteggio riepilogativo delle risorse conformi e non conformi per un tipo di conformità. Utilizzare filtri per esplorare dati di conformità specifici.

```
aws ssm list-compliance-summaries --filters One or more filters.
```

Gli esempi seguenti illustrano come utilizzare questo comando con i filtri.

Linux & macOS

```
aws ssm list-compliance-summaries \  
  --filters Key=AWS:InstanceInformation.PlatformType,Values=Windows  
  Key=PatchGroup,Values=TestGroup
```

Windows

```
aws ssm list-compliance-summaries ^  
  --filters Key=AWS:InstanceInformation.PlatformType,Values=Windows  
  Key=PatchGroup,Values=TestGroup
```

Linux & macOS

```
aws ssm list-compliance-summaries \  
  --filters Key=AWS:InstanceInformation.PlatformType,Values=Windows  
  Key=ExecutionId,Values=4adf0526-6aed-4694-97a5-14522EXAMPLE
```

Windows

```
aws ssm list-compliance-summaries ^  
  --filters Key=AWS:InstanceInformation.PlatformType,Values=Windows  
  Key=ExecutionId,Values=4adf0526-6aed-4694-97a5-14522EXAMPLE
```

AWS Systems Manager Distributor

Distributort aiuta a creare pacchetti e pubblicare software su nodi AWS Systems Manager gestiti. È possibile creare pacchetti e pubblicare il proprio software o utilizzare Distributor per trovare e pubblicare pacchetti software AWS forniti da agenti, come AmazonCloudWatchAgent, o pacchetti di terze parti come Trend Micro. La pubblicazione di un pacchetto pubblicizza versioni specifiche del documento del pacchetto ai nodi gestiti identificati tramite ID di nodo, Account AWS ID, tag o

un Regione AWS. Per cominciare a utilizzare Distributor, apri la [console di Systems Manager](#). Nel pannello di navigazione, scegli Distributor.

Dopo aver creato un pacchetto in Distributor, puoi installare il pacchetto in uno dei modi seguenti:

- Una sola volta con [AWS Systems Manager Run Command](#).
- In base a una pianificazione con [AWS Systems Manager State Manager](#).

Important

I pacchetti distribuiti da venditori terzi non sono gestiti AWS e vengono pubblicati dal fornitore del pacchetto. Consigliamo di condurre ulteriore due diligence per garantire il rispetto dei controlli di sicurezza interni. La sicurezza è una responsabilità condivisa tra te AWS e te. Questo è descritto come il modello di responsabilità condivisa. Per ulteriori informazioni consulta il [Modello di responsabilità condivisa](#).

Come può Distributor avvantaggiare la mia organizzazione?

Distributor offre questi vantaggi:

- Un solo pacchetto, molte piattaforme

Quando crei un pacchetto in Distributor, il sistema crea un documento AWS Systems Manager (documento SSM). È possibile allegare file con estensione zip a questo documento. Quando lanci Distributor, il sistema elabora le istruzioni nel documento SSM e installa il pacchetto software nel file .zip sulle destinazioni specificate. Distributor supporta più sistemi operativi, tra cui Windows, Ubuntu Server, Debian Server, e Red Hat Enterprise Linux. Per ulteriori informazioni sulle piattaforme supportate, consulta [Architetture e piattaforme dei pacchetti supportate](#).

- Controlla l'accesso ai pacchetti nei gruppi di istanze gestite

Puoi utilizzare Run Command o State Manager per controllare quali nodi gestiti ricevono un pacchetto e quale versione del pacchetto. Run Command e State Manager sono strumenti di AWS Systems Manager. Le istanze gestite possono essere raggruppate per istanza o ID di dispositivo, numeri di Account AWS, tag o Regioni AWS. Puoi utilizzare le associazioni di State Manager per distribuire diverse versioni di un pacchetto a diversi gruppi di istanze.

- Molti pacchetti di AWS agenti inclusi e pronti all'uso

Distributor include molti pacchetti di AWS agenti pronti per la distribuzione nei nodi gestiti. Cercare i pacchetti nella Distributor Packages che sono pubblicati da Amazon. A titolo di esempio si possono menzionare AmazonCloudWatchAgent e AWSPVDriver.

- Distribuzione automatica

Per mantenere aggiornato il tuo ambiente, utilizza State Manager per programmare i pacchetti per l'implementazione automatica nei nodi gestiti di destinazione quando vengono avviati per la prima volta.

Chi dovrebbe utilizzarlo Distributor?

- Qualsiasi AWS cliente che desideri creare nuovi pacchetti software o distribuire pacchetti software esistenti, inclusi i pacchetti AWS pubblicati, su più nodi gestiti da Systems Manager contemporaneamente.
- Sviluppatori software che creano pacchetti software.
- Gli amministratori responsabili dell'aggiornamento dei nodi gestiti di Systems Manager con i pacchetti software più recenti.

Quali sono le caratteristiche di Distributor?

- Implementazione dei pacchetti nelle istanze di Windows e Linux

Con Distributor, puoi distribuire pacchetti software su istanze Amazon Elastic Compute Cloud (Amazon EC2) e dispositivi AWS IoT Greengrass principali per Linux e Windows Server. Per un elenco dei tipi di sistema operativo dell'istanza supportati, consulta [the section called “Architetture e piattaforme dei pacchetti supportate”](#).

- Distribuisce i pacchetti una sola volta o in base a una pianificazione automatica

Puoi scegliere di distribuire i pacchetti una sola volta, in base a una pianificazione periodica o ogni volta che la versione del pacchetto predefinita viene modificata.

- Reinstallazione completa dei pacchetti o esecuzione di aggiornamenti in locale

Per installare una nuova versione del pacchetto, puoi disinstallare la versione corrente e installarne una nuova oppure aggiornare la versione corrente utilizzando uno script di aggiornamento. Il pacchetto non è disponibile durante la reinstallazione ma può rimanere disponibile durante un

aggiornamento in corso. In-place gli aggiornamenti sono utili per il monitoraggio della sicurezza o per altri scenari in cui è necessario evitare tempi di inattività.

- Accesso alle funzionalità tramite console PowerShell, CLI e SDK Distributor

Puoi lavorarci Distributor utilizzando la console di Systems Manager, AWS Command Line Interface (AWS CLI) o l' AWS SDK di tua scelta. AWS Strumenti per PowerShell

- Controllo degli accessi IAM

Utilizzando le policy AWS Identity and Access Management (IAM), puoi controllare quali membri dell'organizzazione possono creare, aggiornare, distribuire o eliminare pacchetti o versioni dei pacchetti. Ad esempio, potresti voler assegnare a un amministratore le autorizzazioni per distribuire i pacchetti, ma non per modificarli o per creare nuove versioni di pacchetti.

- Supporto delle funzionalità di registrazione e verifica

Puoi controllare e registrare le azioni Distributor degli utenti al tuo interno Account AWS attraverso l'integrazione con altri Servizi AWS. Per ulteriori informazioni, consulta [Controllo e registrazione Distributor activity](#).

In cosa consiste un pacchetto Distributor?

Un pacchetto è una raccolta di software o di risorse installabili che include quanto segue.

- Un file .zip del software per ogni piattaforma del sistema operativo di destinazione. Ogni file .zip deve includere quanto segue.
 - Una install e una uninstall sceneggiatura. Windows Serveri nodi gestiti basati su base richiedono PowerShell degli script (script denominati `install.ps1` e `uninstall.ps1`). Linux-based i nodi gestiti richiedono script di shell (script denominati `install.sh` e `uninstall.sh`). AWS Systems Manager SSM Agent legge ed esegue le istruzioni negli script `install` e `uninstall`.
 - Un file eseguibile. SSM Agent deve trovare questo eseguibile per installare il pacchetto nei nodi gestiti di destinazione.
- Un file JSON-formatted manifesto che descrive il contenuto del pacchetto. Il file manifest non è incluso nel file .zip, ma è archiviato nello stesso bucket Amazon Simple Storage Service (Amazon S3) dei file .zip che formano il pacchetto. Il manifest identifica la versione del pacchetto e mappa i file .zip del pacchetto agli attributi del nodo gestito di destinazione, ad esempio la versione del sistema operativo o l'architettura. Per informazioni su come creare il manifest, consulta [Fase 2: creazione del manifesto del pacchetto JSON](#).

Quando scegli la creazione del pacchetto Simple (Semplice) nella console Distributor, Distributor genera automaticamente gli script di installazione e disinstallazione, gli hash del file e il manifest del pacchetto JSON, in base al nome file dell'eseguibile software e alle piattaforme e architetture di destinazione.

Architetture e piattaforme dei pacchetti supportate

È possibile utilizzare Distributor per pubblicare pacchetti sulle seguenti piattaforme di nodi gestiti di Systems Manager. Il valore di una versione deve corrispondere esattamente alla versione della release dell'AMI del sistema operativo Amazon Machine Image (AMI) di destinazione. Per ulteriori informazioni su come determinare questa versione, consulta la fase 4 di [Fase 2: creazione del manifesto del pacchetto JSON](#).

Note

Systems Manager non supporta tutti i seguenti sistemi operativi per i dispositivi AWS IoT Greengrass principali. Per ulteriori informazioni, vedere [Configurazione dei dispositivi AWS IoT Greengrass principali](#) nella Guida per gli AWS IoT Greengrass Version 2 sviluppatori.

Platform (Piattaforma)	Valore del codice nel file manifest	Architetture supportate
AlmaLinux	almalinux	x86_64 ARM64
Amazon Linux 2 e Amazon Linux 2023	amazon	x86_64 o x86 ARM64 (Amazon Linux 2 e AL2023, tipi di istanza A1)
Bottlerocket	bottlerocket	x86_64 ARM64
Debian Server	debian	x86_64 o x86
Fedora Linux	fedora	x86_64

Platform (Piattaforma)	Valore del codice nel file manifest	Architetture supportate
		ARM64
macOS	mac_os_x	x86_64 ARM64
openSUSE	opensuse	x86_64
openSUSE Leap	opensuseleap	x86_64
Oracle Linux	oracle	x86_64
Red Hat Enterprise Linux (RHEL)	redhat	x86_64 ARM64 (RHEL 7.6 e versioni successive, tipi di istanza A1)
Rocky Linux	rocky	x86_64 ARM64
SUSE Linux Enterprise Server (SLES)	suse	x86_64
Ubuntu Server	ubuntu	x86_64 o x86 ARM64 (Ubuntu Server 16 e versioni successive, tipi di istanza A1)
Windows Server	windows	x86_64

Argomenti

- [Configurazione Distributor](#)
- [Lavorare con Distributor packages](#)
- [Controllo e registrazione Distributor activity](#)

- [Risoluzione dei problemi AWS Systems Manager Distributor](#)

Configurazione Distributor

Prima di utilizzare Distributor per creare, gestire e distribuire i pacchetti software, segui questa procedura.

Completa Distributor prerequisiti

Prima di utilizzare Distributor, verifica che il tuo ambiente soddisfi i requisiti seguenti.

Distributor prerequisiti

Requisito	Description
SSM Agent	<p>AWS Systems Manager SSM Agent la versione 2.3.274.0 o successiva deve essere installata nei nodi gestiti su cui si desidera eseguire la distribuzione o da cui si desidera rimuovere i pacchetti.</p> <p>Per installare o aggiornare SSM Agent, consulta Lavorare con Agente SSM.</p>
AWS CLI	<p>(Facoltativo) Per utilizzare la AWS Command Line Interface (AWS CLI) anziché la console di Systems Manager per creare e gestire i pacchetti, installate la versione più recente di sul AWS CLI computer locale.</p> <p>Per ulteriori informazioni su come installare e o aggiornare CLI, consulta Installazione di AWS Command Line Interface nella Guida per l'utente di AWS Command Line Interface .</p>
AWS Strumenti per PowerShell	<p>(Facoltativo) Per utilizzare Tools for PowerShell anziché la console Systems Manager per creare e gestire pacchetti, installate la versione più recente di Tools for PowerShell sul computer locale.</p>

Requisito	Description
	Per ulteriori informazioni su come installare o aggiornare Tools for PowerShell, vedere Configurazione di AWS Tools for Windows PowerShell o AWS Tools for PowerShell Core nella Guida per l'AWS Strumenti per PowerShell utente.

Note

Systems Manager non supporta la distribuzione di pacchetti ai nodi gestiti di Oracle Linux utilizzando Distributor.

Verifica o crea un profilo di istanza IAM con Distributor autorizzazioni

Per impostazione predefinita, AWS Systems Manager non è autorizzato a eseguire azioni sulle tue istanze. È necessario concedere l'accesso utilizzando un profilo di istanza AWS Identity and Access Management (IAM). Un profilo dell'istanza è un container che trasmette le informazioni sul ruolo IAM a un'istanza di Amazon Elastic Compute Cloud (Amazon EC2) all'avvio. Questo requisito si applica alle autorizzazioni per tutti gli strumenti di Systems Manager, non solo per Distributor.

Note

Quando configuri i dispositivi edge per eseguire il software AWS IoT Greengrass Core eSSM Agent, specifichi un ruolo del servizio IAM che consenta a Systems Manager di eseguire azioni su di esso. Non è necessario configurare dispositivi edge gestiti con un profilo dell'istanza.

Se già utilizzi altri strumenti di Systems Manager, ad esempio Run Command e State Manager, un profilo dell'istanza con le autorizzazioni richieste per Distributor è già associato alle tue istanze. Il modo più semplice per assicurarsi di disporre delle autorizzazioni per eseguire le Distributor attività consiste nell'allegare la `AmazonSSMManagedInstanceCore` policy al profilo dell'istanza. Per ulteriori informazioni, consulta la pagina [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#).

Controllo dell'accesso utenti ai pacchetti

Utilizzando le policy AWS Identity and Access Management (IAM), puoi controllare chi può creare, distribuire e gestire i pacchetti. Puoi anche controllare quali operazioni API di Run Command e State Manager possono eseguire sui nodi gestiti. Ad esempio Distributor, entrambi Run Command e State Manager sono strumenti di AWS Systems Manager.

Formato ARN

User-defined i pacchetti sono associati ai documenti Amazon Resource Names (ARN) e hanno il seguente formato.

```
arn:aws:ssm:region:account-id:document/document-name
```

Di seguito è riportato un esempio di :

```
arn:aws:ssm:us-west-1:123456789012:document/ExampleDocumentName
```

Puoi utilizzare un paio di policy IAM predefinite AWS fornite, una per gli utenti finali e una per gli amministratori, per concedere le autorizzazioni per le attività. Distributor In alternativa, puoi creare policy IAM personalizzate adatte ai tuoi specifici requisiti di autorizzazione.

Per ulteriori informazioni sull'utilizzo delle variabili nelle policy IAM, consulta [Elementi delle policy IAM: variabili](#).

Per informazioni su come creare policy e collegarle a utenti o gruppi, consulta le pagine [Creazione di policy IAM](#) e [Aggiunta e rimozione di policy IAM](#) nella Guida per l'utente di IAM.

Crea o scegli un bucket Amazon S3 da archiviare Distributor packages

Quando crei un pacchetto utilizzando il flusso di lavoro Semplice nella console AWS Systems Manager , scegli un bucket Amazon Simple Storage Service (Amazon S3) esistente in cui Distributor carica il software. Distributor è uno strumento di AWS Systems Manager. Nel flusso di lavoro Avanzato, è necessario caricare i file .zip del software o le risorse in un bucket Amazon S3 prima di iniziare. Sia che crei un pacchetto utilizzando i flussi di lavoro Semplice o Avanzato nella console o l'API, prima di iniziare a creare il pacchetto devi disporre di un bucket Amazon S3. Come parte del processo di creazione del pacchetto, Distributor copia il software installabile e le risorse da questo bucket in un archivio Systems Manager interno. Poiché le risorse vengono copiate in una memoria interna, puoi eliminare o riutilizzare il bucket Amazon S3 al termine della creazione del pacchetto.

Per ulteriori informazioni sulla creazione di un bucket, consulta la sezione relativa alla [creazione di un bucket](#) nella Guida alle operazioni di base di Amazon Simple Storage Service. Per ulteriori informazioni su come eseguire un AWS CLI comando per creare un bucket, consulta la sezione Command [mb](#) Reference. AWS CLI

Lavorare con Distributor packages

Puoi utilizzare la AWS Systems Manager console, gli strumenti a riga di AWS comando (AWS CLI e AWS Strumenti per PowerShell) e gli AWS SDK per aggiungere, gestire o distribuire pacchetti in. Distributor Distributore è uno strumento in. AWS Systems Manager Prima di aggiungere un pacchetto a Distributor:

- Crea e comprimi le risorse installabili.
- (Facoltativo) Crea un file manifest JSON per il pacchetto. Questa operazione non è necessaria per utilizzare il processo di creazione del pacchetto Simple (Semplice) nella console Distributor. La creazione del pacchetto semplice genera automaticamente un file manifest JSON.

È possibile utilizzare la AWS Systems Manager console o un editor di testo o JSON per creare il file manifest.

- Avere un bucket Amazon Simple Storage Service (Amazon S3) pronto per memorizzare le risorse o il software installabili. Se stai utilizzando il processo di creazione del pacchetto Advanced (Avanzato), carica le risorse nel bucket Amazon S3 prima di iniziare.

Note

Puoi eliminare o riutilizzare questo bucket al termine della creazione del pacchetto perché Distributor sposta i contenuti del pacchetto in un bucket interno Systems Manager come parte del processo di creazione del pacchetto.

AWS i pacchetti pubblicati sono già impacchettati e pronti per la distribuzione. Per distribuire un pacchetto pubblicato da AWS verso i nodi gestiti, consulta [Installa o aggiorna Distributor packages](#).

Puoi condividere pacchetti Distributor tra Account AWS. Quando usi un pacchetto condiviso da un altro account nei AWS CLI comandi, usa il pacchetto Amazon Resource Name (ARN) al posto del nome del pacchetto.

Argomenti

- [Visualizza i pacchetti in Distributor](#)
- [Crea un pacchetto in Distributor](#)
- [Modifica Distributor autorizzazioni dei pacchetti nella console](#)
- [Modifica Distributor etichette dei pacchetti nella console](#)
- [Aggiungere una versione a Distributor package](#)
- [Installa o aggiorna Distributor packages](#)
- [Disinstallazione di un pacchetto Distributor](#)
- [Eliminare un Distributor package](#)

Visualizza i pacchetti in Distributor

Per visualizzare i pacchetti disponibili per l'installazione, puoi utilizzare la AWS Systems Manager console o il tuo strumento da riga di AWS comando preferito. Distributor è uno strumento in AWS Systems Manager. Per accedere a Distributor, apri la AWS Systems Manager console e scegli Distributor nel riquadro di navigazione a sinistra. Visualizza tutti i pacchetti disponibili.

La sezione seguente descrive come visualizzare i pacchetti Distributor utilizzando lo strumento a riga di comando preferito.

Visualizzazione dei pacchetti utilizzando la riga di comando

Questa sezione contiene informazioni su come utilizzare lo strumento a riga di comando preferito per visualizzare Distributor utilizzando i comandi forniti.

Linux & macOS

Per visualizzare i pacchetti utilizzando AWS CLI su Linux

- Per visualizzare tutti i pacchetti, esclusi i pacchetti condivisi, esegui il comando seguente.

```
aws ssm list-documents \
  --filters Key=DocumentType,Values=Package
```

- Per visualizzare tutti i pacchetti di proprietà di Amazon, esegui il comando seguente.

```
aws ssm list-documents \
  --filters Key=DocumentType,Values=Package Key=Owner,Values=Amazon
```

- Per visualizzare tutti i pacchetti di proprietà di terze parti, esegui il comando seguente.

```
aws ssm list-documents \  
  --filters Key=DocumentType,Values=Package Key=Owner,Values=ThirdParty
```

Windows

Per visualizzare i pacchetti utilizzando AWS CLI su Windows

- Per visualizzare tutti i pacchetti, esclusi i pacchetti condivisi, esegui il comando seguente.

```
aws ssm list-documents ^  
  --filters Key=DocumentType,Values=Package
```

- Per visualizzare tutti i pacchetti di proprietà di Amazon, esegui il comando seguente.

```
aws ssm list-documents ^  
  --filters Key=DocumentType,Values=Package Key=Owner,Values=Amazon
```

- Per visualizzare tutti i pacchetti di proprietà di terze parti, esegui il comando seguente.

```
aws ssm list-documents ^  
  --filters Key=DocumentType,Values=Package Key=Owner,Values=ThirdParty
```

PowerShell

Per visualizzare i pacchetti utilizzando gli Strumenti per PowerShell

- Per visualizzare tutti i pacchetti, esclusi i pacchetti condivisi, esegui il comando seguente.

```
$filter = New-Object Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter  
$filter.Key = "DocumentType"  
$filter.Values = "Package"  
  
Get-SSMDocumentList `   
  -Filters @($filter)
```

- Per visualizzare tutti i pacchetti di proprietà di Amazon, esegui il comando seguente.

```
$typeFilter = New-Object  
Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter
```

```
$typeFilter.Key = "DocumentType"
$typeFilter.Values = "Package"

$ownerFilter = New-Object
    Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter
$ownerFilter.Key = "Owner"
$ownerFilter.Values = "Amazon"

Get-SSMDocumentList `
    -Filters @($typeFilter,$ownerFilter)
```

- Per visualizzare tutti i pacchetti di proprietà di terze parti, esegui il comando seguente.

```
$typeFilter = New-Object
    Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter
$typeFilter.Key = "DocumentType"
$typeFilter.Values = "Package"

$ownerFilter = New-Object
    Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter
$ownerFilter.Key = "Owner"
$ownerFilter.Values = "ThirdParty"

Get-SSMDocumentList `
    -Filters @($typeFilter,$ownerFilter)
```

Crea un pacchetto in Distributor

Per creare un pacchetto, prepara il software o le risorse installabili, un file per piattaforma del sistema operativo. Per creare un pacchetto è richiesto almeno un file.

A volte, piattaforme diverse potrebbero utilizzare lo stesso file, ma tutti i file collegati al pacchetto devono essere elencati nella sezione **Files** del manifesto. Se stai creando un pacchetto utilizzando il flusso di lavoro semplice nella console, il manifesto viene generato automaticamente. Il numero massimo di file che puoi collegare a un singolo documento è 20. La dimensione massima di ogni file è di 1 GB. Per ulteriori informazioni sulle piattaforme supportate, consulta [Architetture e piattaforme dei pacchetti supportate](#).

Quando crei un pacchetto, il sistema crea un nuovo [Documento SSM](#). Con questo documento, puoi distribuire il pacchetto nei nodi gestiti.

Solo a scopo dimostrativo, un pacchetto di esempio [ExamplePackage.zip](#), è disponibile per il download dal nostro sito Web. Il pacchetto di esempio include un manifest JSON completo e tre file .zip contenenti i programmi di installazione per la v7.0.0. PowerShell Gli script di installazione e disinstallazione non contengono comandi validi. Anche se è necessario comprimere ogni software installabile e gli script in un file .zip per creare un pacchetto nel flusso di lavoro Avanzato, le risorse installabili non vengono compresse nel flusso di lavoro Semplice.

Argomenti

- [Crea un pacchetto utilizzando il flusso di lavoro Semplice](#)
- [Creare un pacchetto utilizzando il flusso di lavoro Avanzato](#)

Crea un pacchetto utilizzando il flusso di lavoro Semplice

Questa sezione descrive come creare un pacchetto in Distributor scegliendo il flusso di lavoro di creazione del pacchetto Semplice nella console Distributor. Distributor è uno strumento di AWS Systems Manager. Per creare un pacchetto, prepara le risorse installabili, un file per ogni piattaforma del sistema operativo. Per creare un pacchetto è richiesto almeno un file. Il semplice processo di creazione del pacchetto genera automaticamente script di installazione e disinstallazione, hash di file e un manifest. JSON-formatted Il flusso di lavoro Semplice gestisce il processo di caricamento e compressione dei file installabili e la creazione di un nuovo pacchetto e del [documento SSM](#) associato. Per ulteriori informazioni sulle piattaforme supportate, consulta [Architetture e piattaforme dei pacchetti supportate](#).

Quando si utilizza il metodo semplice per creare un pacchetto, Distributor crea script `install` e `uninstall` per l'utente. Tuttavia, quando si crea un pacchetto per un aggiornamento in locale, è necessario fornire i propri contenuti dello script `update` nella scheda `Aggiorna script`. Quando si aggiungono comandi di input per uno script `update`, Distributor include questo script nel pacchetto.zip creato per l'utente, insieme agli script `install` e `uninstall`.

Note

Utilizza l'opzione di aggiornamento `In-place` per aggiungere file nuovi o aggiornati a un'installazione di pacchetti esistente senza disconnettere l'applicazione associata.

Creazione di un pacchetto tramite il flusso di lavoro semplice

1. Apri la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Distributor.
3. Nella home page Distributor, scegli Crea pacchetto, quindi seleziona Semplice.
4. Nella pagina Crea pacchetto, inserisci un nome per il pacchetto. I nomi dei pacchetti possono contenere lettere, numeri, punti, trattini e caratteri di sottolineatura. Il nome deve essere abbastanza generico da applicarsi a tutte le versioni degli allegati del pacchetto, ma abbastanza specifico da identificare lo scopo del pacchetto.
5. (Facoltativo) In Nome della versione, immetti un nome di versione. I nomi delle versioni possono essere composti da un massimo di 512 caratteri e non possono contenere caratteri speciali.
6. Per Posizione, scegli un bucket utilizzando il nome e il prefisso del bucket o utilizzandone l'URL.
7. Per Carica software, scegli Aggiungi software, quindi passa ai file software installabili con estensione .rpm, .msi o .deb. Se il nome del file contiene spazi, il caricamento non riesce. Puoi caricare più file del software in una singola operazione.
8. Per Piattaforma di destinazione, verifica che la piattaforma del sistema operativo di destinazione visualizzata per ogni file installabile sia corretta. Se il sistema operativo mostrato non è corretto, scegli il sistema operativo corretto nell'elenco a discesa.

Nel flusso di lavoro di creazione del pacchetto Semplice, poiché ogni file installabile viene caricato solo una volta, sono richieste fasi aggiuntive per indicare a Distributor di utilizzare un singolo file come destinazione di più sistemi operativi. Ad esempio, se carichi un file del software installabile denominato `Logtool_v1.1.1.rpm`, devi modificare alcune impostazioni predefinite nel flusso di lavoro Semplice, per indirizzare lo stesso software su versioni supportate sia dal sistema operativo di Amazon Linux che da quello di Ubuntu Server. Quando si utilizzano più piattaforme, esegui una delle seguenti operazioni.

- Utilizza il flusso di lavoro Avanzato, comprimi ogni file installabile in un file .zip prima di iniziare e creare manualmente il manifesto, in modo da poter destinare un file installabile a più piattaforme o versioni del sistema operativo. Per ulteriori informazioni, consulta [Creare un pacchetto utilizzando il flusso di lavoro Avanzato](#).
- Modifica manualmente il file manifest nel flusso di lavoro Semplice, in modo che il file .zip sia destinato a più piattaforme o versioni di sistema operativo. Per ulteriori informazioni su come eseguire questa operazione, consulta la fine della fase 4 in [Fase 2: creazione del manifesto del pacchetto JSON](#).

9. Per Versione della piattaforma, verifica che la versione della piattaforma del sistema operativo mostrata sia **_any** o una versione principale seguita da una wildcard (7.*) o l'esatta versione della release del sistema operativo specifico che deve essere valida per il software. Per ulteriori informazioni sulla specifica della versione della piattaforma del sistema operativo, consulta la fase 4 in [Fase 2: creazione del manifesto del pacchetto JSON](#).
10. Per Architettura, scegli l'architettura del processore corretta per ogni file installabile dall'elenco a discesa. Per ulteriori informazioni sulle architetture del processore supportate, consulta [Architetture e piattaforme dei pacchetti supportate](#).
11. (Facoltativo) Espandere Script ed esaminare gli script generati da Distributor per il software installabile.
12. (Facoltativo) Per fornire uno script di aggiornamento da utilizzare con gli aggiornamenti in locale, espandere Script, scegliere la scheda Aggiorna script e immettere i comandi di script di aggiornamento

Systems Manager non genera script di aggiornamento per conto dell'utente.
13. Per aggiungere altri file del software installabile, scegli Aggiungi software. Altrimenti, vai alla fase successiva.
14. (Facoltativo) Espandi Manifesto ed esamina il manifesto del pacchetto JSON generato da Distributor per il software installabile. Se hai modificato eventuali informazioni sul software da momento in cui hai avviato questa procedura, ad esempio versione della piattaforma o piattaforma di destinazione, scegli Genera manifesto per visualizzare il manifesto del pacchetto aggiornato.

Puoi modificare il manifesto manualmente, se desideri che un software installabile sia destinato a più di un sistema operativo, come descritto nella fase 8. Per ulteriori informazioni sulla modifica del manifesto, consulta [Fase 2: creazione del manifesto del pacchetto JSON](#).
15. Scegli Crea pacchetto.

Attendi che Distributor termini il caricamento del software e la creazione del pacchetto. Distributor mostra lo stato di caricamento per ogni file installabile. In base al numero e alla dimensione dei pacchetti che si stanno aggiungendo, questa operazione può richiedere alcuni minuti. Distributor esegue automaticamente il reindirizzamento alla pagina Dettagli del pacchetto per il nuovo pacchetto, ma puoi scegliere di aprire questa pagina personalmente dopo che il software è stato caricato. La pagina Dettagli del pacchetto non mostra tutte le informazioni sul pacchetto finché Distributor non termina il processo di creazione del pacchetto. Per interrompere il processo di caricamento e di creazione del pacchetto, scegli Annulla.

Se Distributor non è in grado di caricare i file installabili del software, visualizza un messaggio Caricamento non riuscito. Per riprovare a eseguire il caricamento, scegli Riprova caricamento. Per ulteriori informazioni su come risolvere gli errori di creazione del pacchetto, consulta [Risoluzione dei problemi AWS Systems Manager Distributor](#).

Creare un pacchetto utilizzando il flusso di lavoro Avanzato

In questa sezione, vengono fornite ulteriori informazioni su come utenti esperti possono creare un pacchetto in Distributor dopo il caricamento di risorse installabili compresse con script di installazione e disinstallazione e un file manifest JSON, in un bucket di Amazon S3.

Per creare un pacchetto, preparare i file .zip delle risorse installabili, un file .zip per ogni piattaforma del sistema operativo. Per creare un pacchetto è richiesto almeno un file .zip. Quindi, crea un manifesto JSON. Il manifesto include i puntatori per i file del codice del pacchetto. Dopo aver aggiunto i file del codice richiesti a una cartella o a una directory e dopo aver popolato il manifesto con i valori corretti, carica il pacchetto in un bucket S3.

Un pacchetto di esempio [ExamplePackage.zip](#), è disponibile per il download dal nostro sito Web. Il pacchetto di esempio include un manifesto JSON completato e tre file .zip.

Argomenti

- [Fase 1: creazione dei file ZIP](#)
- [Fase 2: creazione del manifesto del pacchetto JSON](#)
- [Fase 3: caricamento del pacchetto e del manifesto in un bucket Amazon S3](#)
- [Fase 4: Aggiungere un pacchetto a Distributor](#)

Fase 1: creazione dei file ZIP

La base del pacchetto è costituita da almeno un file .zip con software o risorse installabili. Un pacchetto include un file .zip per ogni sistema operativo da supportare, a meno che questo non possa essere installato su più sistemi operativi. Ad esempio, le versioni supportate delle istanze di Red Hat Enterprise Linux e di Amazon Linux, in genere, possono eseguire gli stessi file eseguibili .RPM, quindi è sufficiente collegare un solo file .zip al pacchetto per supportare entrambi i sistemi operativi.

File richiesti

Gli elementi seguenti sono obbligatori in ogni file .zip.

- Un install e uno uninstall script. Windows Server i nodi gestiti basati su base richiedono PowerShell degli script (script denominati `install.ps1` e `uninstall.ps1`). Linux-based i nodi gestiti richiedono script di shell (script denominati `install.sh` e `uninstall.sh`). SSM Agent esegue le istruzioni negli script `install` e `uninstall`.

Ad esempio, gli script di installazione potrebbero eseguire un programma di installazione, ad esempio `.rpm` o `.msi`, potrebbero copiare file o impostare opzioni di configurazione.

- Un file eseguibile, pacchetti di installazione (`.rpm`, `.deb`, `.msi` e così via), altri script o file di configurazione.

File facoltativi

Il seguente elemento è facoltativo in ogni file.zip:

- Uno script update. Fornire uno script di aggiornamento consente di utilizzare l'opzione `In-place update` per installare un pacchetto. Quando si desidera aggiungere file nuovi o aggiornati a un'installazione di pacchetto esistente, l'`In-place update` opzione non mette offline l'applicazione del pacchetto durante l'esecuzione dell'aggiornamento. Windows Server i nodi gestiti basati su base richiedono PowerShell uno script (script denominato `update.ps1`). Linux-based i nodi gestiti richiedono uno script di shell (script denominato `update.sh`). SSM Agent esegue le istruzioni nello script update.

Per ulteriori informazioni sull'installazione o sull'aggiornamento dei pacchetti, consulta [Installa o aggiorna Distributor packages](#).

Per esempi di file .zip, inclusi esempi install e uninstall script, scarica il pacchetto di esempio, [ExamplePackage.zip](#)

Fase 2: creazione del manifesto del pacchetto JSON

Dopo la preparazione e la compressione dei file installabili, crea un manifesto JSON. Di seguito è riportato il modello. Le parti del modello del manifesto sono descritte nella procedura in questa sezione. Puoi utilizzare un editor JSON per creare questo manifesto in un file separato. In alternativa, puoi creare il manifesto nella AWS Systems Manager console quando crei un pacchetto.

```
{
  "schemaVersion": "2.0",
  "version": "your-version",
  "publisher": "optional-publisher-name",
```

```
"packages": {
  "platform": {
    "platform-version": {
      "architecture": {
        "file": ".zip-file-name-1.zip"
      }
    }
  },
  "another-platform": {
    "platform-version": {
      "architecture": {
        "file": ".zip-file-name-2.zip"
      }
    }
  },
  "another-platform": {
    "platform-version": {
      "architecture": {
        "file": ".zip-file-name-3.zip"
      }
    }
  }
},
"files": {
  ".zip-file-name-1.zip": {
    "checksums": {
      "sha256": "checksum"
    }
  },
  ".zip-file-name-2.zip": {
    "checksums": {
      "sha256": "checksum"
    }
  }
}
}
```

Per creare un manifesto del pacchetto JSON

1. Aggiungi la versione dello schema al manifesto. In questo rilascio, la versione dello schema è sempre 2.0.

```
{ "schemaVersion": "2.0",
```

2. Aggiungi una versione del pacchetto definita dall'utente al manifesto. Questo è anche il valore di Nome versione specificato quando aggiungi il pacchetto a Distributor. Diventa parte del documento AWS Systems Manager che Distributor crea quando aggiungi il pacchetto. Questo valore viene anche fornito come input nel documento AWS-ConfigureAWSPackage per installare una versione del pacchetto diversa dall'ultima. Un valore `version` può contenere lettere, numeri, trattini bassi, trattini e punti e può avere una lunghezza massima di 128 caratteri. È consigliabile utilizzare una versione del pacchetto leggibile per semplificare a te e agli altri amministratori la specifica delle versioni esatte del pacchetto durante la distribuzione. Di seguito è riportato un esempio di :

```
"version": "1.0.1",
```

3. (Facoltativo) Aggiungi il nome di un publisher. Di seguito è riportato un esempio di :

```
"publisher": "MyOrganization",
```

4. Aggiungi pacchetti. La sezione "packages" descrive le piattaforme, le architetture e le versioni supportate dal file .zip nel pacchetto. Per ulteriori informazioni, consulta [Architetture e piattaforme dei pacchetti supportate](#).

platform-version Può essere il valore jolly, `_any`. Utilizzarlo per indicare che un file .zip supporta qualsiasi versione della piattaforma. È inoltre possibile specificare una versione principale seguita da un carattere jolly in modo che tutte le versioni secondarie siano supportate, ad esempio `7.*`. Se scegli di specificare un *platform-version* valore per una versione specifica del sistema operativo, assicurati che corrisponda all'esatta versione di rilascio del sistema operativo a AMI cui ti riferisci. Di seguito sono elencate le risorse consigliate per ottenere il valore corretto del sistema operativo.

- Su nodi gestiti basati su Windows Server, la versione di release è disponibile sotto forma di dati Windows Management Instrumentation (WMI). Puoi eseguire il seguente comando dal prompt dei comandi per ottenere le informazioni sulla versione, quindi puoi analizzare i risultati per `version`.

```
wmic OS get /format:list
```

- Su un nodo Linux-based gestito, recupera la versione eseguendo prima la ricerca della versione del sistema operativo (eseguendo il comando seguente). Cerca il valore di `VERSION_ID`.

```
cat /etc/os-release
```

Se non vengono restituiti i risultati richiesti, esegui il secondo comando per ottenere le informazioni di rilascio LSB dal file `/etc/lsb-release`, quindi cerca il valore di `DISTRIB_RELEASE`.

```
lsb_release -a
```

Se questi metodi non riescono, in genere è possibile individuare il rilascio in base alla distribuzione. Ad esempio, su Debian Server puoi analizzare il file `/etc/debian_version` oppure su Red Hat Enterprise Linux il `/etc/redhat-release`.

```
hostnamectl
```

```
"packages": {  
  "platform": {  
    "platform-version": {  
      "architecture": {  
        "file": ".zip-file-name-1.zip"  
      }  
    }  
  },  
  "another-platform": {  
    "platform-version": {  
      "architecture": {  
        "file": ".zip-file-name-2.zip"  
      }  
    }  
  },  
  "another-platform": {  
    "platform-version": {  
      "architecture": {  
        "file": ".zip-file-name-3.zip"  
      }  
    }  
  }  
}
```

```
}
}
```

Di seguito è riportato un esempio di : In questo esempio, la piattaforma del sistema operativo è amazon, la versione supportata è 2016.09, l'architettura è x86_64 e il file .zip che supporta questa piattaforma è test.zip.

```
{
  "amazon": {
    "2016.09": {
      "x86_64": {
        "file": "test.zip"
      }
    }
  }
},
```

Puoi aggiungere il valore jolly `_any` per indicare che il pacchetto supporta tutte le versioni dell'elemento padre. Ad esempio, per indicare che il pacchetto è supportato su qualsiasi versione di Amazon Linux, l'istruzione del pacchetto deve essere simile alla seguente. Puoi utilizzare il carattere jolly `_any` a livello di versione o di architettura per supportare tutte le versioni di una piattaforma, tutte le architetture di una versione oppure tutte le versioni e tutte le architetture di una piattaforma.

```
{
  "amazon": {
    "_any": {
      "x86_64": {
        "file": "test.zip"
      }
    }
  }
},
```

L'esempio seguente aggiunge `_any` per mostrare che il primo pacchetto, `data1.zip`, è supportato per tutte le architetture di Amazon Linux 2016.09. Il secondo pacchetto, `data2.zip`, è supportato per tutte le versioni di Amazon Linux, ma solo per i nodi gestiti con l'architettura `x86_64`. Entrambe le versioni `2023.8` e `_any` sono voci di `amazon`. Esiste una sola piattaforma (Amazon Linux)), ma diverse versioni, architetture e relativi file .zip supportati.

```
{
  "amazon": {
    "2023.8": {
      "_any": {
        "file": "data1.zip"
      }
    },
    "_any": {
      "x86_64": {
        "file": "data2.zip"
      }
    }
  }
}
```

È possibile fare riferimento a un file .zip più volte nella sezione "packages" del manifesto, se il file .zip supporta più di una piattaforma. Ad esempio, se un file .zip supporta sia le versioni 8.x di Red Hat Enterprise Linux che di Amazon Linux, la sezione "packages" contiene due voci che puntano allo stesso file .zip, come mostrato nell'esempio seguente.

```
{
  "amazon": {
    "2023.8.20250715 ": {
      "x86_64": {
        "file": "test.zip"
      }
    }
  },
  "redhat": {
    "8.*": {
      "x86_64": {
        "file": "test.zip"
      }
    }
  }
},
```

5. Aggiungere l'elenco dei file .zip che fanno parte di questo pacchetto dalla fase 4. Ogni voce di file richiede il nome del file e il checksum del valore hash sha256. I valori checksum nel manifesto devono corrispondere al valore hash sha256 nelle risorse compresse per evitare errori di installazione del pacchetto.

Per ottenere il checksum esatto dai file installabili, puoi eseguire i comandi riportati di seguito. In Linux, eseguire `shasum -a 256 file-name.zip` o `openssl dgst -sha256 file-name.zip`. In Windows, esegui il `Get-FileHash -Path path-to-.zip-file` cmdlet in [PowerShell](#).

La sezione "files" del manifesto include un riferimento a ciascuno dei file .zip nel pacchetto.

```
"files": {
  "test-agent-x86.deb.zip": {
    "checksums": {
      "sha256":
"EXAMPLE2706223c7616ca9fb28863a233b38e5a23a8c326bb4ae241dcEXAMPLE"
    }
  },
  "test-agent-x86_64.deb.zip": {
    "checksums": {
      "sha256":
"EXAMPLE572a745844618c491045f25ee6aae8a66307ea9bff0e9d1052EXAMPLE"
    }
  },
  "test-agent-x86_64.nano.zip": {
    "checksums": {
      "sha256":
"EXAMPLE63ccb86e830b63dfef46995af6b32b3c52ce72241b5e80c995EXAMPLE"
    }
  },
  "test-agent-rhel8-x86.nano.zip": {
    "checksums": {
      "sha256":
"EXAMPLE13df60aa3219bf117638167e5bae0a55467e947a363fff0a51EXAMPLE"
    }
  },
  "test-agent-x86.msi.zip": {
    "checksums": {
      "sha256":
"EXAMPLE12a4abb10315aa6b8a7384cc9b5ca8ad8e9ced8ef1bf0e5478EXAMPLE"
    }
  },
  "test-agent-x86_64.msi.zip": {
    "checksums": {
      "sha256":
"EXAMPLE63ccb86e830b63dfef46995af6b32b3c52ce72241b5e80c995EXAMPLE"
    }
  }
}
```

```

    }
  },
  "test-agent-rhel8-x86.rpm.zip": {
    "checksums": {
      "sha256":
"EXAMPLE13df60aa3219bf117638167e5bae0a55467e947a363fff0a51EXAMPLE"
    }
  }
}

```

6. Dopo aver aggiunto le informazioni sul pacchetto, salva e chiudi il file manifest.

Di seguito è riportato un esempio di un manifesto completato. Questo esempio mostra un file .zip, NewPackage_LINUX.zip, che supporta più di una piattaforma, ma viene indicato nella sezione "files" una sola volta.

```

{
  "schemaVersion": "2.0",
  "version": "1.7.1",
  "publisher": "Amazon Web Services",
  "packages": {
    "windows": {
      "_any": {
        "x86_64": {
          "file": "NewPackage_WINDOWS.zip"
        }
      }
    },
    "amazon": {
      "_any": {
        "x86_64": {
          "file": "NewPackage_LINUX.zip"
        }
      }
    },
    "ubuntu": {
      "_any": {
        "x86_64": {
          "file": "NewPackage_LINUX.zip"
        }
      }
    }
  }
},

```



```
{
  "files": {
    "NewPackage_WINDOWS.zip": {
      "checksums": {
        "sha256":
"EXAMPLEc2c706013cf8c68163459678f7f6daa9489cd3f91d52799331EXAMPLE"
      }
    },
    "NewPackage_LINUX.zip": {
      "checksums": {
        "sha256":
"EXAMPLE2b8b9ed71e86f39f5946e837df0d38aacdd38955b4b18ffa6fEXAMPLE"
      }
    }
  }
}
```

Esempio di pacchetto

Un pacchetto di esempio, [ExamplePackage.zip](#), è disponibile per il download dal nostro sito Web. Il pacchetto di esempio include un manifesto JSON completato e tre file .zip.

Fase 3: caricamento del pacchetto e del manifesto in un bucket Amazon S3

Preparare il pacchetto copiando o spostando tutti i file .zip in una cartella o una directory. Un pacchetto valido richiede il manifesto creato in [Fase 2: creazione del manifesto del pacchetto JSON](#) e tutti i file .zip identificati nel file manifest.

Per caricare il pacchetto e il manifesto in Amazon S3

1. Copiare o spostare tutti i file di archivio .zip specificati nel manifesto in una cartella o una directory. Non comprimere la cartella o la directory in cui si spostano i file di archivio .zip e il file manifest.
2. Creare un bucket o sceglierne uno esistente. Per ulteriori informazioni consulta la sezione relativa alla [creazione di un bucket](#) nella Guida alle operazioni di base di Amazon Simple Storage Service. Per ulteriori informazioni su come eseguire un AWS CLI comando per creare un bucket, consulta [mb](#) la sezione AWS CLI Command Reference.
3. Carica la cartella o la directory nel bucket. Per ulteriori informazioni, consulta [Aggiungi un oggetto in un bucket](#) nella Guida alle operazioni di base di Amazon Simple Storage Service. Se intendi incollare il manifesto JSON nella AWS Systems Manager console, non caricarlo. Per ulteriori informazioni su come eseguire un AWS CLI comando per caricare file in un bucket, consulta la sezione AWS CLI Command [mv](#) Reference.

4. Nella home page del bucket, scegli la cartella o la directory che hai caricato. Se hai caricato i file in una sottocartella in un bucket, prendi nota della sottocartella (nota anche come un prefisso). Il prefisso è necessario per aggiungere il pacchetto a Distributor.

Fase 4: Aggiungere un pacchetto a Distributor

Puoi utilizzare la AWS Systems Manager console, gli strumenti a riga di AWS comando (AWS CLI and AWS Strumenti per PowerShell) o gli AWS SDK per aggiungere un nuovo pacchetto. Distributor Quando aggiungi un pacchetto, stai aggiungendo un nuovo [documento SSM](#). Il documento consente di distribuire il pacchetto nei nodi gestiti.

Argomenti

- [Aggiunta di un pacchetto tramite la console](#)
- [Aggiungi un pacchetto usando il AWS CLI](#)

Aggiunta di un pacchetto tramite la console

È possibile utilizzare la AWS Systems Manager console per creare un pacchetto. Tieni pronto il nome del bucket in cui hai caricato il pacchetto in [Fase 3: caricamento del pacchetto e del manifesto in un bucket Amazon S3](#).

Per aggiungere un pacchetto a Distributor (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Distributor.
3. Nella home page Distributor, scegli Create package (Crea pacchetto) e seleziona Advanced (Avanzato).
4. Nella pagina Crea pacchetto, inserisci un nome per il pacchetto. I nomi dei pacchetti possono contenere lettere, numeri, punti, trattini e caratteri di sottolineatura. Il nome deve essere abbastanza generico da applicarsi a tutte le versioni degli allegati del pacchetto, ma abbastanza specifico da identificare lo scopo del pacchetto.
5. Per Nome della versione, immetti il valore esatto della voce `version` nel file manifest.
6. Per Nome del bucket S3, scegli il nome del bucket in cui sono stati caricati i file .zip e il manifesto in [the section called “Fase 3: caricamento del pacchetto e del manifesto in un bucket Amazon S3”](#).

7. Per Prefisso della chiave S3, immetti la sottocartella del bucket in cui sono archiviati i file .zip e il manifesto.
8. Per Manifesto, scegli Estrai dal pacchetto per utilizzare un manifesto caricato nel bucket Amazon S3 con i file .zip.

(Facoltativo) Se non è stato caricato il manifesto JSON nel bucket S3 in cui sono stati archiviati i file .zip, scegli Nuovo manifesto. Puoi creare o incollare l'intero manifesto nel campo Editor JSON. Per ulteriori informazioni su come creare il manifesto JSON, consulta [Fase 2: creazione del manifesto del pacchetto JSON](#).

9. Al termine, scegli Crea pacchetto.
10. Attendere che Distributor crei il pacchetto dai file .zip e manifest. In base al numero e alla dimensione dei pacchetti che si stanno aggiungendo, questa operazione può richiedere alcuni minuti. Distributor esegue automaticamente il reindirizzamento alla pagina Dettagli del pacchetto per il nuovo pacchetto, ma puoi scegliere di aprire questa pagina personalmente dopo che il software è stato caricato. La pagina Dettagli del pacchetto non mostra tutte le informazioni sul pacchetto finché Distributor non termina il processo di creazione del pacchetto. Per interrompere il processo di caricamento e di creazione del pacchetto, scegli Annulla.

Aggiungi un pacchetto usando il AWS CLI

È possibile utilizzare il AWS CLI per creare un pacchetto. Tieni pronto l'URL del bucket da cui hai caricato il pacchetto in [Fase 3: caricamento del pacchetto e del manifesto in un bucket Amazon S3](#).

Per aggiungere un pacchetto ad Amazon S3 utilizzando AWS CLI

1. AWS CLI Per creare un pacchetto, esegui il comando seguente, sostituendolo *package-name* con il nome del pacchetto e *path-to-manifest-file* con il percorso del file manifest JSON. `amzn-s3-demo-bucket` è l'URL del bucket Amazon S3 in cui è archiviato l'intero pacchetto. Quando esegui il comando `create-document` in Distributor, devi specificare il valore `Package` per `--document-type`.

Se non è stato aggiunto il file manifest al bucket Amazon S3, il valore del parametro `--content` è il percorso al file manifest JSON.

```
aws ssm create-document \  
  --name "package-name" \  
  --content file://path-to-manifest-file \  
  --attachments Key="SourceUrl",Values="amzn-s3-demo-bucket" \  
  --document-type Package
```

```
--version-name version-value-from-manifest \  
--document-type Package
```

Di seguito è riportato un esempio di :

```
aws ssm create-document \  
  --name "ExamplePackage" \  
  --content file://path-to-manifest-file \  
  --attachments Key="SourceUrl",Values="https://s3.amazonaws.com/amzn-s3-demo-  
bucket/ExamplePackage" \  
  --version-name 1.0.1 \  
  --document-type Package
```

2. Verifica che il pacchetto sia stato aggiunto e mostra il manifesto del pacchetto eseguendo il comando seguente, sostituendolo con il nome del pacchetto. *package-name* Per ottenere una versione specifica del documento (non la stessa di un pacchetto), puoi aggiungere il parametro `--document-version`.

```
aws ssm get-document \  
  --name "package-name"
```

Per informazioni sulle altre opzioni che puoi utilizzare con il comando `create-document`, consulta [create-document](#) nella sezione AWS Systems Manager Riferimento ai comandi AWS CLI . Per informazioni sulle altre opzioni che puoi utilizzare con il comando `get-document` , consulta [get-document](#).

Modifica Distributor autorizzazioni dei pacchetti nella console

Dopo aver aggiunto un pacchetto aDistributor, puoi modificare le autorizzazioni del pacchetto nella console di Systems Manager. È possibile aggiungerne altre Account AWS alle autorizzazioni di un pacchetto. I pacchetti possono essere condivisi con altri account Regione AWS solo nello stesso account. Cross-Region la condivisione non è supportata. Per impostazione predefinita, i pacchetti sono impostati su Privato, il che significa che solo chi ha accesso al creatore del pacchetto Account AWS può visualizzare le informazioni sui pacchetti e aggiornarli o eliminarli. Se le autorizzazioni Private (Privato) sono accettabili, puoi ignorare questa procedura.

 Note

È possibile aggiornare le autorizzazioni dei pacchetti condivisi con 20 o meno account.

Per modificare le autorizzazioni del pacchetto nella console

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Distributor.
3. Nella pagina Packages (Pacchetti) scegli il pacchetto di cui desideri modificare le autorizzazioni.
4. Nella scheda Package details (Dettagli pacchetto) scegli Edit permissions (Modifica autorizzazioni) per modificare le autorizzazioni.
5. Per Edit permissions (Modifica autorizzazioni), scegliere Shared with specific accounts (Condiviso con account specifici).
6. In Shared with specific accounts (Condiviso con account specifici) aggiungi i numeri degli account Account AWS , uno alla volta. Al termine, seleziona Salva.

Modifica Distributor etichette dei pacchetti nella console

Dopo aver aggiunto un pacchetto aDistributor, puoi modificare i tag del pacchetto nella console di Systems Manager. Questi tag vengono applicati al pacchetto e non sono connessi ai tag sui nodi gestiti in cui desideri implementare il pacchetto. I tag sono coppie chiave-valore che prevedono una distinzione tra lettere maiuscole e minuscole e che consentono di raggruppare e filtrare i pacchetti in base a criteri rilevanti per la tua organizzazione. Se non desideri aggiungere tag, puoi procedere con l'installazione del pacchetto o con l'aggiunta di una nuova versione.

Per modificare i tag del pacchetto nella console

1. Aprire la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Distributor.
3. Nella pagina Packages (Pacchetti) scegli il pacchetto di cui desideri modificare i tag.
4. Nella scheda Package details (Dettagli pacchetto in Tags, scegli Edit (Modifica).

5. Per Add tags (Aggiungi tag), inserire una chiave tag oppure una coppia chiave-valore del tag, quindi scegliere Add (Aggiungi). Ripeti se desideri aggiungere ulteriori tag. Per eliminare i tag, scegli X sul tag nella parte inferiore della finestra.
6. Dopo aver aggiunto i tag al pacchetto, scegli Save (Salva).

Aggiungere una versione a Distributor package

Per aggiungere una versione del pacchetto, [create un pacchetto](#) e quindi usate Distributor per aggiungere una versione del pacchetto aggiungendo una voce al documento AWS Systems Manager (SSM) già esistente per le versioni precedenti. Distributor è uno strumento in AWS Systems Manager. Per risparmiare tempo, aggiorna il manifesto di una versione precedente del pacchetto, modifica il valore della voce `version` nel manifesto (ad esempio da `Test_1.0` a `Test_2.0`) e salvalo come manifesto per la nuova versione. Il flusso di lavoro Aggiungi versione semplice nella console Distributor aggiorna automaticamente il file manifest.

Una nuova versione del pacchetto può:

- Sostituire almeno uno dei file installabili collegati alla versione corrente.
- Aggiungere nuovi file installabili per supportare piattaforme aggiuntive.
- Eliminare i file per interrompere il supporto per piattaforme specifiche.

Una versione più recente può utilizzare lo stesso bucket Amazon Simple Storage Service (Amazon S3), ma deve avere un URL con un nome file diverso indicato alla fine. Puoi utilizzare la console Systems Manager o l'opzione AWS Command Line Interface (AWS CLI) per aggiungere la nuova versione. Il caricamento di un file installabile con il nome esatto di un file installabile esistente nel bucket Amazon S3 sovrascrive il file esistente. Nessun file installabile viene copiato dalla versione precedente nella nuova versione; è necessario caricare i file installabili dalla versione precedente affinché siano parte di una nuova versione. Dopo che Distributor ha completato la creazione di una nuova versione del pacchetto, puoi eliminare o riutilizzare il bucket Amazon S3, perché Distributor copia il software in un bucket Systems Manager interno come parte del processo di controllo delle versioni.

Note

Ogni pacchetto è limitato a un massimo di 25 versioni. Puoi eliminare le versioni che non sono più necessarie.

Argomenti

- [Aggiunta di una versione del pacchetto utilizzando la console](#)
- [Aggiungere una versione del pacchetto utilizzando AWS CLI](#)

Aggiunta di una versione del pacchetto utilizzando la console

Prima di procedere, segui le istruzioni in [Crea un pacchetto in Distributor](#) per creare un nuovo pacchetto per la versione. Quindi, utilizza la console Systems Manager per aggiungere una nuova versione del pacchetto a Distributor.

Aggiunta di una versione del pacchetto utilizzando il flusso di lavoro Simple (Semplice)

Per aggiungere una versione del pacchetto utilizzando il flusso di lavoro Simple (Semplice), prepara file installabili aggiornati o aggiungi file installabili per supportare più piattaforme e architetture. Quindi, utilizza Distributor per caricare file installabili nuovi e aggiornati e aggiungere una versione del pacchetto. Il flusso di lavoro Aggiungi versione semplificato nella console Distributor aggiorna automaticamente il file manifest e il documento SSM associato.

Per aggiungere una versione del pacchetto utilizzando il flusso di lavoro Simple (Semplice)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Distributor.
3. Nella home page di Distributor, scegli il pacchetto a cui aggiungere un'altra versione.
4. Nella pagina Add version (Aggiungi versione), scegli Simple (Semplice).
5. Per Version name (Nome versione), immettere un nome della versione. Il nome della versione per la nuova versione deve essere diverso dai nomi delle versioni precedenti. I nomi delle versioni possono essere composti da un massimo di 512 caratteri e non possono contenere caratteri speciali.
6. Per Nome del bucket S3, scegli un bucket S3 esistente dall'elenco. Questo può essere lo stesso bucket utilizzato per archiviare i file installabili per versioni precedenti, ma i nomi dei file installabili devono essere diversi per evitare di sovrascrivere i file installabili esistenti nel bucket.
7. Per Prefisso della chiave S3, immetti la sottocartella del bucket in cui sono archiviate le risorse installabili.

8. Per Upload software, accedi ai file software installabili per la nuova versione. I file delle versioni esistenti non vengono copiati automaticamente nella nuova versione. Carica i file dalle versioni precedenti se li desideri nella nuova versione. Puoi caricare più di un file con una sola azione.
9. Per Piattaforma di destinazione, verifica che la piattaforma del sistema operativo di destinazione visualizzata per ogni file installabile sia corretta. Se il sistema operativo mostrato non è corretto, scegli il sistema operativo corretto nell'elenco a discesa.

Nel flusso di lavoro di controllo delle versioni Semplice, poiché ogni file installabile viene caricato solo una volta, sono richieste fasi aggiuntive per fare sì che un singolo file sia destinato a più sistemi operativi. Ad esempio, se carichi un file del software installabile denominato `Logtool_v1.1.1.rpm`, devi modificare alcune impostazioni predefinite nel flusso di lavoro Semplice, per istruire Distributor, affinché diriga lo stesso software sia sul sistema operativo di Amazon Linux che di Ubuntu Server. Per ovviare a questa limitazione puoi adottare una delle soluzioni riportate di seguito.

- Utilizza il flusso di lavoro di controllo delle versioni Avanzato, comprimi ogni file installabile in un file .zip prima di iniziare e creare manualmente il manifesto, in modo da poter destinare un file installabile a più piattaforme o versioni del sistema operativo. Per ulteriori informazioni, consulta [Aggiunta di una versione del pacchetto utilizzando il flusso di lavoro Avanzato](#).
 - Modifica manualmente il file manifest nel flusso di lavoro Semplice, in modo che il file .zip sia destinato a più piattaforme o versioni di sistema operativo. Per ulteriori informazioni su come eseguire questa operazione, consulta la fine della fase 4 in [Fase 2: creazione del manifesto del pacchetto JSON](#).
10. Per Versione della piattaforma, verifica che la versione della piattaforma del sistema operativo mostrata sia **_any** o una versione principale seguita da un carattere jolly (8.*) o l'esatta versione di rilascio del sistema operativo specifico, che deve essere valida per il software. Per ulteriori informazioni sulla specifica della versione della piattaforma, consulta la fase 4 in [Fase 2: creazione del manifesto del pacchetto JSON](#).
 11. Per Architecture (Architettura), scegli l'architettura del processore corretta per ogni file installabile dall'elenco a discesa. Per ulteriori informazioni sulle architetture supportate, consulta [Architetture e piattaforme dei pacchetti supportate](#).
 12. (Facoltativo) Espandere Scripts (Script) ed esaminare gli script di installazione e disinstallazione generati da Distributor per il software installabile.
 13. Per aggiungere altri file del software installabili nella versione, scegli Add software (Aggiungi software). Altrimenti, vai alla fase successiva.

14. (Facoltativo) Espandi Manifesto ed esamina il manifesto del pacchetto JSON generato da Distributor per il software installabile. Se hai modificato eventuali informazioni sul software installabile dal momento in cui hai avviato questa procedura, ad esempio versione della piattaforma o piattaforma di destinazione, scegli Genera manifesto per visualizzare il manifesto del pacchetto aggiornato.

Puoi modificare il manifesto manualmente se desideri che un software installabile sia la destinazione di più sistemi operativi, come descritto nella fase 9. Per ulteriori informazioni sulla modifica del manifesto, consulta [Fase 2: creazione del manifesto del pacchetto JSON](#).

15. Al termine dell'aggiunta del software e dell'esame della piattaforma di destinazione, della versione e dei dati dell'architettura, scegli Aggiungi versione.
16. Attendi che Distributor termini il caricamento del software e la creazione della nuova versione del pacchetto. Distributor mostra lo stato di caricamento per ogni file installabile. In base al numero e alla dimensione dei pacchetti che stai aggiungendo, questa operazione può richiedere alcuni minuti. Distributor esegue automaticamente il reindirizzamento alla pagina Dettagli del pacchetto per il pacchetto, ma puoi scegliere di aprire questa pagina personalmente dopo che il software è stato caricato. La pagina Dettagli del pacchetto non mostra tutte le informazioni sul pacchetto finché Distributor non termina la creazione della nuova versione del pacchetto. Per interrompere il caricamento e la creazione della versione del pacchetto, scegli Interrompi caricamento.
17. Se Distributor non è in grado di caricare i file installabili del software, visualizza un messaggio Caricamento non riuscito. Per riprovare a eseguire il caricamento, scegli Riprova caricamento. Per ulteriori informazioni su come risolvere errori di creazione della versione del pacchetto, consulta [Risoluzione dei problemi AWS Systems Manager Distributor](#).
18. Quando Distributor ha terminato la creazione della nuova versione del pacchetto, nella pagina Dettagli, nella scheda Versioni, visualizza la nuova versione nell'elenco delle versioni del pacchetto disponibili. Imposta una versione predefinita del pacchetto scegliendo una versione e selezionando Imposta versione predefinita.

Se non imposti una versione predefinita, verrà selezionata la versione più recente del pacchetto.

Aggiunta di una versione del pacchetto utilizzando il flusso di lavoro Avanzato

Per aggiungere una versione del pacchetto, [crea un pacchetto](#), quindi utilizza Distributor per aggiungere una versione del pacchetto aggiungendo una voce al documento SSM che esiste per versioni precedenti. Per risparmiare tempo, aggiorna il manifesto di una versione precedente del pacchetto, modifica il valore della voce `version` nel manifesto (ad esempio da `Test_1.0` a

Test_2.0) e salvalo come manifesto per la nuova versione. È necessario disporre di un manifesto aggiornato per aggiungere una nuova versione del pacchetto utilizzando il flusso di lavoro Avanzato.

Per aggiungere una versione del pacchetto utilizzando il flusso di lavoro Avanzato

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Distributor.
3. Nella home page di Distributor, scegli il pacchetto a cui aggiungere un'altra versione, quindi seleziona Aggiungi versione.
4. Per Nome versione, immetti il valore esatto nella voce version del proprio file manifest.
5. Per Nome del bucket S3, scegli un bucket S3 esistente dall'elenco. Questo può essere lo stesso bucket utilizzato per archiviare i file installabili per versioni precedenti, ma i nomi dei file installabili devono essere diversi per evitare di sovrascrivere i file installabili esistenti nel bucket.
6. Per Prefisso della chiave S3, immetti la sottocartella del bucket in cui sono archiviate le risorse installabili.
7. Per Manifesto, scegli Estrai dal pacchetto per utilizzare un manifesto caricato nel bucket S3 con i file .zip.

(Facoltativo) Se non è stato caricato il manifesto JSON rivisto nel bucket Amazon S3 in cui sono stati archiviati i file .zip, scegli Nuovo manifesto. Puoi creare o incollare l'intero manifesto nel campo Editor JSON. Per ulteriori informazioni su come creare il manifesto JSON, consulta [Fase 2: creazione del manifesto del pacchetto JSON](#).

8. Al completamento del manifesto, scegli Aggiungi versione del pacchetto.
9. Nella pagina Dettagli, nella scheda Versioni, visualizza la nuova versione nell'elenco delle versioni del pacchetto disponibili. Imposta una versione predefinita del pacchetto scegliendo una versione e selezionando Imposta versione predefinita.

Se non imposti una versione predefinita, verrà selezionata la versione più recente del pacchetto.

Aggiungere una versione del pacchetto utilizzando AWS CLI

È possibile utilizzare il AWS CLI per aggiungere una nuova versione del pacchetto a Distributor. Prima di eseguire questi comandi, devi creare una nuova versione del pacchetto e caricarla su S3, come descritto all'inizio di questo argomento.

Per aggiungere una versione del pacchetto utilizzando AWS CLI

1. Eseguite il comando seguente per modificare il AWS Systems Manager documento con una voce per una nuova versione del pacchetto. Sostituiscilo *document-name* con il nome del tuo documento. Sostituiscilo *amzn-s3-demo-bucket* con l'URL del manifesto JSON che hai copiato. [Fase 3: caricamento del pacchetto e del manifesto in un bucket Amazon S3](#) *S3-bucket-URL-of-package* è l'URL del bucket Amazon S3 in cui è archiviato l'intero pacchetto. Sostituisci *version-name-from-updated-manifest* con il valore di version nel manifest. Imposta il parametro `--document-version` su `$LATEST` per associare il documento a questa versione del pacchetto, la versione più recente del documento.

```
aws ssm update-document \  
  --name "document-name" \  
  --content "S3-bucket-URL-to-manifest-file" \  
  --attachments Key="SourceUrl",Values="amzn-s3-demo-bucket" \  
  --version-name version-name-from-updated-manifest \  
  --document-version $LATEST
```

Di seguito è riportato un esempio di :

```
aws ssm update-document \  
  --name ExamplePackage \  
  --content "https://s3.amazonaws.com/amzn-s3-demo-bucket/ExamplePackage/  
manifest.json" \  
  --attachments Key="SourceUrl",Values="https://s3.amazonaws.com/amzn-s3-demo-  
bucket/ExamplePackage" \  
  --version-name 1.1.1 \  
  --document-version $LATEST
```

2. Esegui il comando seguente per verificare che il pacchetto sia stato aggiornato e visualizzare il manifesto del pacchetto. Sostituiscilo *package-name* con il nome del pacchetto e, facoltativamente, *document-version* con il numero di versione del documento (diverso dalla versione del pacchetto) che hai aggiornato. Se questa versione del pacchetto è associata alla versione più recente del documento, puoi specificare `$LATEST` per il valore del parametro facoltativo `--document-version`.

```
aws ssm get-document \  
  --name "package-name" \  
  --document-version "document-version"
```

Per informazioni sulle altre opzioni che puoi usare con il `update-document` comando, vedi [update-document](#) nella AWS Systems Manager sezione del AWS CLI Command Reference.

Installa o aggiorna Distributor packages

È possibile distribuire pacchetti nei nodi AWS Systems Manager gestiti utilizzando Distributor uno strumento in AWS Systems Manager. Per distribuire i pacchetti, usa Console di gestione AWS o AWS Command Line Interface (AWS CLI). Al momento, puoi distribuire una sola versione di un pacchetto per ogni comando. È possibile installare nuovi pacchetti o aggiornare le installazioni esistenti in locale. Puoi scegliere di implementare una versione specifica oppure sempre quella più recente di un pacchetto per la distribuzione. Si consiglia di utilizzarlo State Manager per installare i pacchetti. L'utilizzo State Manager aiuta a garantire che i nodi gestiti eseguano sempre la versione più aggiornata del pacchetto.

Important

I pacchetti installati tramite Distributor devono essere disinstallati solo utilizzando Distributor. In caso contrario, Systems Manager può comunque registrare l'applicazione come INSTALLED e portare ad altri risultati indesiderati.

Preferenza	AWS Systems Manager azione	Ulteriori informazioni
Installare o aggiornare immediatamente un pacchetto.	Run Command	<ul style="list-style-type: none">• Installazione o aggiornamento di un pacchetto una tantum utilizzando la console• Installazione di un pacchetto una sola volta utilizzando AWS CLI• Aggiornamento di un pacchetto una sola volta utilizzando AWS CLI
Installare o aggiornare un pacchetto in base a una	State Manager	<ul style="list-style-type: none">• Pianificazione dell'installazione o dell'aggi

Preferenza	AWS Systems Manager azione	Ulteriori informazioni
pianificazione, in modo che l'installazione includa sempre la versione predefinita.		<p>ornamento di un pacchetto utilizzando la console</p> <ul style="list-style-type: none"> • Pianificazione dell'installazione di un pacchetto utilizzando AWS CLI • Pianificazione di un aggiornamento del pacchetto utilizzando AWS CLI
Installare automaticamente un pacchetto sui nuovi nodi gestiti che hanno un tag o set di tag specifico. Ad esempio, l'installazione dell' CloudWatch agente Amazon su nuove istanze.	State Manager	<p>Uno dei modi per farlo consiste nell'applicare i tag ai nuovi nodi gestiti, quindi specificare i tag come destinazioni nell'associazione di State Manager. State Manager installa automaticamente il pacchetto in un'associazione sui nodi gestiti che hanno tag corrispondenti. Consulta Comprendere gli obiettivi e i controlli delle tariffe in State Manager associati.</p>

Argomenti

- [Installazione o aggiornamento di un pacchetto una tantum utilizzando la console](#)
- [Pianificazione dell'installazione o dell'aggiornamento di un pacchetto utilizzando la console](#)
- [Installazione di un pacchetto una sola volta utilizzando AWS CLI](#)
- [Aggiornamento di un pacchetto una sola volta utilizzando AWS CLI](#)
- [Pianificazione dell'installazione di un pacchetto utilizzando AWS CLI](#)
- [Pianificazione di un aggiornamento del pacchetto utilizzando AWS CLI](#)

Installazione o aggiornamento di un pacchetto una tantum utilizzando la console

Puoi utilizzare la AWS Systems Manager console per installare o aggiornare un pacchetto una sola volta. Quando si configura un'installazione singola, Distributor utilizza [AWS Systems Manager Run Command](#), per eseguire l'installazione.

Per installare o aggiornare un pacchetto una tantum utilizzando la console

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Distributor.
3. Nella home page di Distributor, scegli il pacchetto da installare.
4. Scegli Install one time (Installa una tantum).

Questo comando apre Run Command con il documento del comando AWS-ConfigureAWSPackage e il pacchetto Distributor già selezionati.

5. Per Document version (Versione documento), selezionare la versione del documento AWS-ConfigureAWSPackage che si desidera eseguire.
6. Per Action (Operazione), selezionare Install (Installa).
7. Per Installation type (Tipo di installazione), scegliere una delle seguenti opzioni:
 - Uninstall and reinstall (Disinstalla e reinstalla): il pacchetto viene completamente disinstallato e quindi reinstallato. L'applicazione non è disponibile fino al completamento della reinstallazione.
 - In-place aggiornamento: solo i file nuovi o modificati vengono aggiunti all'installazione esistente in base alle istruzioni fornite in uno update script. L'applicazione rimane disponibile durante tutto il processo di aggiornamento. Questa opzione non è supportata per i pacchetti AWS pubblicati ad eccezione del AWSEC2Launch-Agent pacchetto.
8. Per Name (Nome), verificare che sia immesso il nome del pacchetto selezionato.
9. (Facoltativo) In Version (Versione), immettere il nome della versione del pacchetto. Se lasci vuoto questo campo, Run Command installa la versione predefinita selezionata in Distributor.
10. In Targets (Destinazioni), identificare i nodi gestiti in cui si desidera eseguire questa operazione specificando i tag, selezionando le istanze manualmente o indicando un gruppo di risorse.

 Note

Se nell'elenco non si visualizza un nodo gestito, vedi [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#).

11. In Altri parametri:

- In Commento, digita le informazioni su questo comando.
- In Timeout (secondi), specifica il numero di secondi che il sistema dovrà attendere prima di generare un errore per l'intera esecuzione del comando.

12. Per Rate control (Controllo velocità):

- In Concurrency (Simultaneità), specificare un numero o una percentuale di destinazioni su cui eseguire contemporaneamente il comando.

 Note

Se sono state selezionate le destinazioni specificando i tag o i gruppi di risorse, e se non si conosce con certezza il numero di nodi gestiti di destinazione, limitare il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- In Error threshold (Soglia di errore) specifica quando interrompere l'esecuzione del comando sulle altre destinazioni dopo un errore su un numero o una percentuale di nodi gestiti. Se ad esempio si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.

13. (Facoltativo) Nella sezione Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Scrivi l'output del comando in un bucket S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

 Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle](#)

[autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

14. Se vuoi che vengano inviate notifiche sullo stato dell'esecuzione del comando, nella sezione Notifiche SNS selezionare la casella di controllo Abilita notifiche SNS.

Per ulteriori informazioni, sulla configurazione delle notifiche Amazon SNS per Run Command consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

15. Quando si è pronti per installare il pacchetto, scegliere Run (Esegui).
16. L'area Command status (Stato del comando) segnala lo stato di avanzamento dell'esecuzione. Se il comando è ancora in corso, scegliere l'icona di aggiornamento nell'angolo in alto a sinistra della console finché la colonna Overall status (Stato generale) o Detailed status (Stato dettagliato) non mostra Success (Riuscito) o Failed (Non riuscito).
17. Nell'area Targets and outputs (Destinazioni e uscite), scegli il pulsante accanto al nome del nodo gestito e seleziona View output (Visualizza output).

La pagina di output del comando mostra i risultati di esecuzione del comando.

18. (Facoltativo) Se si sceglie di scrivere l'output dei comandi in un bucket Amazon S3, selezionare Amazon S3 per visualizzare i dati del log di output.

Pianificazione dell'installazione o dell'aggiornamento di un pacchetto utilizzando la console

È possibile utilizzare la AWS Systems Manager console per pianificare l'installazione o l'aggiornamento di un pacchetto. Quando pianifichi l'installazione o l'aggiornamento di un pacchetto, Distributor utilizza [AWS Systems Manager State Manager](#) per eseguire l'installazione o l'aggiornamento.

Per pianificare un'installazione del pacchetto utilizzando la console

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Distributor.
3. Nella home page di Distributor, scegliere il pacchetto da installare o aggiornare.

4. Per Install package (Installa pacchetto), scegliere Install on a schedule (Installa in base a una pianificazione).

Questo comando apre State Manager in una nuova associazione creata per te.

5. Per Name (Nome) immettere un nome (ad esempio **Deploy-test-agent-package**). Questo passaggio è facoltativo, ma è consigliato. Gli spazi non sono consentiti nel nome.
6. Nell'elenco Document (Documento), il nome del documento AWS-ConfigureAWSPackage è già selezionato.
7. Per Action (Operazione), verificare che sia selezionata l'opzione Install (Installa).
8. Per Installation type (Tipo di installazione), scegliere una delle seguenti opzioni:
 - Uninstall and reinstall (Disinstalla e reinstalla): il pacchetto viene completamente disinstallato e quindi reinstallato. L'applicazione non è disponibile fino al completamento della reinstallazione.
 - In-place aggiornamento: solo i file nuovi o modificati vengono aggiunti all'installazione esistente in base alle istruzioni fornite in uno update script. L'applicazione rimane disponibile durante tutto il processo di aggiornamento.
9. Per Name (Nome), verificare che sia inserito il nome del pacchetto.
10. Per Version (Versione), se si desidera installare una versione del pacchetto diversa dall'ultima versione pubblicata, immettere l'identificatore della versione.
11. In Targets (Destinazioni) scegliere Selecting all managed instances in this account (Selezione di tutte le istanze gestite in questo account), Specifying tags (Specifica tag) o Manually Selecting Instance (Selezione manuale dell'istanza). Se fai riferimento alle risorse con i tag, immetti una chiave e un valore del tag nei campi visualizzati.

Note

Puoi scegliere i dispositivi AWS IoT Greengrass principali gestiti scegliendo Selezione di tutte le istanze gestite in questo account o Selezione manuale dell'istanza.

12. In Specify schedule (Specifica pianificazione) scegliere On Schedule (In base a pianificazione) per eseguire l'associazione in base a una pianificazione regolare o No Schedule (Nessuna pianificazione) per eseguire l'associazione una sola volta. Per ulteriori informazioni su queste opzioni, consulta [Utilizzo delle associazioni in Systems Manager](#). Utilizza i controlli per creare una pianificazione cron o rate per l'associazione.
13. Scegli Crea associazione.

14. Nella pagina Association (Associazione), scegliere il pulsante accanto all'associazione creata e selezionare Apply association now (Applica associazione ora).

State Manager crea ed esegue immediatamente l'associazione sulle destinazioni specificate. Per ulteriori informazioni sui risultati dell'esecuzione delle associazioni, consulta [Utilizzo delle associazioni in Systems Manager](#) in questa guida.

Per ulteriori informazioni sull'utilizzo delle opzioni in Advanced options (Opzioni avanzate), Rate control (Controllo della velocità) e Output options (Opzioni di output), consulta [Utilizzo delle associazioni in Systems Manager](#).

Installazione di un pacchetto una sola volta utilizzando AWS CLI

È possibile eseguire send-command il comando AWS CLI per installare un Distributor pacchetto una sola volta. Se il pacchetto è già installato, l'applicazione verrà disconnessa mentre il pacchetto viene disinstallato e sostituito con la nuova versione.

Per installare un pacchetto una sola volta utilizzando AWS CLI

- Esegui il comando seguente nell' AWS CLI.

```
aws ssm send-command \  
  --document-name "AWS-ConfigureAWSPackage" \  
  --instance-ids "instance-IDs" \  
  --parameters '["action":["Install"],"installationType":["Uninstall and  
reinstall"],"name":["package-name (in same account) or package-ARN (shared from  
different account)"]]'
```

Note

Il comportamento predefinito per installationType è Uninstall and reinstall. È possibile omettere "installationType":["Uninstall and reinstall"] da questo comando quando si installa un pacchetto completo.

Di seguito è riportato un esempio di :

```
aws ssm send-command \  
  --document-name "AWS-ConfigureAWSPackage" \  
  --instance-ids "instance-IDs"
```

```
--instance-ids "i-0000000000000000" \  
--parameters '{"action":["Install"],"installationType":["Uninstall and  
reinstall"],"name":["ExamplePackage"]}'
```

Per informazioni sulle altre opzioni che puoi usare con il `send-command` comando, vedi [send-command](#) nella AWS Systems Manager sezione del AWS CLI Command Reference.

Aggiornamento di un pacchetto una sola volta utilizzando AWS CLI

È possibile eseguire `send-command` l'aggiornamento AWS CLI di un Distributor pacchetto senza mettere offline l'applicazione associata. Vengono sostituiti solo i file nuovi o aggiornati nel pacchetto.

Per aggiornare un pacchetto una sola volta utilizzando AWS CLI

- Esegui il comando seguente nell' AWS CLI.

```
aws ssm send-command \  
  --document-name "AWS-ConfigureAWSPackage" \  
  --instance-ids "instance-IDs" \  
  --parameters '{"action":["Install"],"installationType":["In-place  
update"],"name":["package-name (in same account) or package-ARN (shared from  
different account)"]}'
```

Note

Quando si aggiungono file nuovi o modificati, è necessario includere `"installationType":["In-place update"]` nel comando.

Di seguito è riportato un esempio di :

```
aws ssm send-command \  
  --document-name "AWS-ConfigureAWSPackage" \  
  --instance-ids "i-02573cafcfEXAMPLE" \  
  --parameters '{"action":["Install"],"installationType":["In-place  
update"],"name":["ExamplePackage"]}'
```

Per informazioni sulle altre opzioni che è possibile utilizzare con il `send-command` comando, vedere [send-command](#) nella AWS Systems Manager sezione del AWS CLI Command Reference.

Pianificazione dell'installazione di un pacchetto utilizzando AWS CLI

È possibile eseguire il comando AWS CLI per installare un Distributor pacchetto create-association in base a una pianificazione. Il valore `--name`, ossia il nome del documento, è sempre `AWS-ConfigureAWSPackage`. Il comando seguente utilizza la chiave `InstanceIds` per specificare i nodi gestiti di destinazione. Se il pacchetto è già installato, l'applicazione verrà disconnessa mentre il pacchetto viene disinstallato e sostituito con la nuova versione.

```
aws ssm create-association \
  --name "AWS-ConfigureAWSPackage" \
  --parameters '{"action":["Install"],"installationType":["Uninstall and
reinstall"],"name":["package-name (in same account) or package-ARN (shared from
different account)"]}' \
  --targets [{"Key\":\"InstanceIds\",\"Values\":[\"instance-ID1\",\"instance-
ID2\"]}]
```

Note

Il comportamento predefinito per `installationType` è `Uninstall and reinstall`. È possibile omettere `"installationType":["Uninstall and reinstall"]` da questo comando quando si installa un pacchetto completo.

Di seguito è riportato un esempio di :

```
aws ssm create-association \
  --name "AWS-ConfigureAWSPackage" \
  --parameters '{"action":["Install"],"installationType":["Uninstall and
reinstall"],"name":["Test-ConfigureAWSPackage"]}' \
  --targets [{"Key\":\"InstanceIds\",\"Values\":[\"i-02573cafcfEXAMPLE\",
\"i-0471e04240EXAMPLE\"]}]
```

Per informazioni sulle altre opzioni che è possibile utilizzare con il `create-association` comando, vedere [create-association](#) la AWS Systems Manager sezione del AWS CLI Command Reference.

Pianificazione di un aggiornamento del pacchetto utilizzando AWS CLI

È possibile eseguire l'aggiornamento AWS CLI di un Distributor pacchetto create-association in base a una pianificazione senza mettere offline l'applicazione associata. Vengono sostituiti solo i file

nuovi o aggiornati nel pacchetto. 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":["In-place update"],"name":  
["package-name (in same account) or package-ARN (shared from different account)"]}' \  
  --targets [{"Key\":\"InstanceIds\",\"Values\":[\"instance-ID1\",\"instance-ID2\"]}]]
```

Note

Quando si aggiungono file nuovi o modificati, è necessario includere `"installationType":["In-place update"]` nel comando.

Di seguito è riportato un esempio di :

```
aws ssm create-association \  
  --name "AWS-ConfigureAWSPackage" \  
  --parameters '{"action":["Install"],"installationType":["In-place update"],"name":  
["Test-ConfigureAWSPackage"]}' \  
  --targets [{"Key\":\"InstanceIds\",\"Values\":[\"i-02573cafcfEXAMPLE\",  
\"i-0471e04240EXAMPLE\"]]}}
```

Per informazioni sulle altre opzioni che è possibile utilizzare con il `create-association` comando, vedere [create-association](#) nella AWS Systems Manager sezione del AWS CLI Command Reference.

Disinstallazione di un pacchetto Distributor

Puoi usare Console di gestione AWS o il AWS Command Line Interface (AWS CLI) per disinstallare Distributor i pacchetti dai tuoi nodi AWS Systems Manager gestiti utilizzando `Run Command`. Distributore `Run Command` sono strumenti in AWS Systems Manager. In questa versione, puoi disinstallare una sola versione di un pacchetto per ogni comando. Puoi disinstallare una versione specifica oppure la versione predefinita.

 Important

I pacchetti installati tramite Distributor devono essere disinstallati solo utilizzando Distributor. In caso contrario, Systems Manager può comunque registrare l'applicazione come INSTALLED e portare ad altri risultati indesiderati.

Argomenti

- [Disinstallazione di un pacchetto utilizzando la console](#)
- [Disinstallazione di un pacchetto utilizzando AWS CLI](#)

Disinstallazione di un pacchetto utilizzando la console

Puoi utilizzare Run Command nella console Systems Manager per disinstallare un pacchetto una sola volta. Distributor utilizza [AWS Systems Manager Run Command](#) per disinstallare i pacchetti.

Per disinstallare un pacchetto utilizzando la console

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Run Command.
3. Nella home page di Run Command, scegli Run command (Esegui comando).
4. Scegli il documento del comando AWS-ConfigureAWSPackage.
5. In Action (Operazione) scegli Uninstall (Disinstalla)
6. In Name (Nome) digita il nome del pacchetto da disinstallare.
7. Per Targets (Obiettivi), scegli il metodo di destinazione dei file utilizzato dai tuoi nodi gestiti. È possibile specificare una chiave di tag e valori condivisi dalle destinazioni. È inoltre possibile specificare le destinazioni scegliendo attributi, ad esempio un>ID, una piattaforma e una versione SSM Agent.
8. Puoi utilizzare le opzioni avanzate per aggiungere commenti sull'operazione, modificare i valori Concurrency (Concorrenza) ed Error threshold (Soglia errore) in Rate control (Controllo frequenza), specificare le opzioni di output oppure configurare le notifiche di Amazon Simple Notification Service (Amazon SNS). Per ulteriori informazioni, consulta [Esecuzione di comandi dalla console](#) in questa guida.

9. Quando sei pronto a disinstallare il pacchetto, scegli Run (Esegui), quindi View results (Visualizza risultati).
10. Nell'elenco di comandi scegli il comando AWS-ConfigureAWSPackage che hai eseguito. Se il comando è ancora in corso, scegli l'icona di aggiornamento nell'angolo in alto a destra della console.
11. Quando la colonna Status (Stato) mostra Success (Riuscito) o Failed (Non riuscito), scegli la scheda Output.
12. Scegli View output (Visualizza output). La pagina di output del comando mostra i risultati di esecuzione del comando.

Disinstallazione di un pacchetto utilizzando AWS CLI

È possibile utilizzare AWS CLI per disinstallare un Distributor pacchetto dai nodi gestiti utilizzando Run Command.

Per disinstallare un pacchetto utilizzando il AWS CLI

- Esegui il comando seguente nell' AWS CLI.

```
aws ssm send-command \  
  --document-name "AWS-ConfigureAWSPackage" \  
  --instance-ids "instance-IDs" \  
  --parameters '["action":["Uninstall"],"name":["package-name (in same account)  
or package-ARN (shared from different account)"]]'
```

Di seguito è riportato un esempio di :

```
aws ssm send-command \  
  --document-name "AWS-ConfigureAWSPackage" \  
  --instance-ids "i-02573cafcfEXAMPLE" \  
  --parameters '["action":["Uninstall"],"name":["Test-ConfigureAWSPackage"]]'
```

Per informazioni sulle altre opzioni che è possibile utilizzare con il send-command comando, vedere [send-command](#) la AWS Systems Manager sezione della Guida di riferimento ai AWS CLI comandi.

Eliminare un Distributor package

In questa sezione viene descritto come eliminare un pacchetto. Non è possibile eliminare una versione di un pacchetto, ma solo l'intero pacchetto.

Eliminazione di un pacchetto utilizzando la console

È possibile utilizzare la AWS Systems Manager console per eliminare un pacchetto o una versione del pacchetto da Distributor. L'eliminazione di un pacchetto cancella tutte le relative versioni da Distributor.

Per eliminare un pacchetto utilizzando la console

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Distributor.
3. Nella home page di Distributor, scegliere il pacchetto da eliminare.
4. Nella pagina dei dettagli del pacchetto, scegli Delete package (Elimina pacchetto).
5. Quando viene richiesto di confermare l'eliminazione, scegli Delete package (Elimina pacchetto).

Eliminazione di una versione del pacchetto utilizzando la console

Puoi utilizzare la console Systems Manager per eliminare una versione del pacchetto da Distributor.

Per eliminare una versione del pacchetto utilizzando la console

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Distributor.
3. Nella home page di Distributor, scegliere il pacchetto di cui eliminare la versione.
4. Nella pagina delle versioni del pacchetto, scegliere la versione da eliminare e scegliere Delete version (Elimina versione).
5. Quando viene richiesto di confermare l'eliminazione, scegliere Delete package version (Elimina versione del pacchetto).

Eliminazione di un pacchetto utilizzando la riga di comando

Puoi utilizzare lo strumento a riga di comando preferito per eliminare un pacchetto da Distributor.

Linux & macOS

Per eliminare un pacchetto utilizzando il AWS CLI

1. Esegui il comando seguente per elencare i documenti per i pacchetti specifici. Nei risultati di questo comando, cerca il pacchetto da eliminare.

```
aws ssm list-documents \  
  --filters Key=Name,Values=package-name
```

2. Eseguire il comando seguente per eliminare un pacchetto. Sostituisci *package-name* con il nome del pacchetto.

```
aws ssm delete-document \  
  --name "package-name"
```

3. Eseguire di nuovo il comando list-documents per verificare che il pacchetto sia stato eliminato. Il pacchetto che hai eliminato non viene incluso nell'elenco.

```
aws ssm list-documents \  
  --filters Key=Name,Values=package-name
```

Windows

Per eliminare un pacchetto utilizzando il AWS CLI

1. Esegui il comando seguente per elencare i documenti per i pacchetti specifici. Nei risultati di questo comando, cerca il pacchetto da eliminare.

```
aws ssm list-documents ^  
  --filters Key=Name,Values=package-name
```

2. Eseguire il comando seguente per eliminare un pacchetto. Sostituisci *package-name* con il nome del pacchetto.

```
aws ssm delete-document ^  
  --name "package-name"
```

3. Eseguire di nuovo il comando list-documents per verificare che il pacchetto sia stato eliminato. Il pacchetto che hai eliminato non viene incluso nell'elenco.

```
aws ssm list-documents ^  
  --filters Key=Name,Values=package-name
```

PowerShell

Per eliminare un pacchetto utilizzando Tools for PowerShell

1. Esegui il comando seguente per elencare i documenti per i pacchetti specifici. Nei risultati di questo comando, cerca il pacchetto da eliminare.

```
$filter = New-Object  
  Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter  
$filter.Key = "Name"  
$filter.Values = "package-name"  
  
Get-SSMDocumentList `  
  -Filters @($filter)
```

2. Eseguire il comando seguente per eliminare un pacchetto. Sostituisci *package-name* con il nome del pacchetto.

```
Remove-SSMDocument `  
  -Name "package-name"
```

3. Eseguire di nuovo il comando Get-SSMDocumentList per verificare che il pacchetto sia stato eliminato. Il pacchetto che hai eliminato non viene incluso nell'elenco.

```
$filter = New-Object  
  Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter  
$filter.Key = "Name"  
$filter.Values = "package-name"  
  
Get-SSMDocumentList `  
  -Filters @($filter)
```

Eliminazione di una versione del pacchetto utilizzando la riga di comando

Puoi utilizzare lo strumento a riga di comando preferito per eliminare una versione del pacchetto da Distributor.

Linux & macOS

Per eliminare una versione del pacchetto utilizzando il AWS CLI

1. Eseguire il comando seguente per elencare le versioni del pacchetto. Nei risultati di questo comando, cercare la versione del pacchetto da eliminare.

```
aws ssm list-document-versions \  
  --name "package-name"
```

2. Per eliminare la versione del pacchetto, esegui il comando seguente. Sostituire *package-name* con il nome del pacchetto e *version* con il numero di versione.

```
aws ssm delete-document \  
  --name "package-name" \  
  --document-version version
```

3. Eseguire il comando list-document-versions per verificare che la versione del pacchetto sia stata eliminata. La versione del pacchetto eliminata non è più presente nell'elenco.

```
aws ssm list-document-versions \  
  --name "package-name"
```

Windows

Per eliminare una versione del pacchetto utilizzando il AWS CLI

1. Eseguire il comando seguente per elencare le versioni del pacchetto. Nei risultati di questo comando, cercare la versione del pacchetto da eliminare.

```
aws ssm list-document-versions ^  
  --name "package-name"
```

2. Per eliminare la versione del pacchetto, esegui il comando seguente. Sostituire *package-name* con il nome del pacchetto e *version* con il numero di versione.

```
aws ssm delete-document ^  
  --name "package-name" ^  
  --document-version version
```

3. Eseguire il comando `list-document-versions` per verificare che la versione del pacchetto sia stata eliminata. La versione del pacchetto eliminata non è più presente nell'elenco.

```
aws ssm list-document-versions ^  
  --name "package-name"
```

PowerShell

Per eliminare una versione del pacchetto utilizzando Tools for PowerShell

1. Eseguire il comando seguente per elencare le versioni del pacchetto. Nei risultati di questo comando, cercare la versione del pacchetto da eliminare.

```
Get-SSMDocumentVersionList `  
  -Name "package-name"
```

2. Per eliminare la versione del pacchetto, esegui il comando seguente. Sostituisci *package-name* con il nome del pacchetto e *version* con il numero di versione.

```
Remove-SSMDocument `  
  -Name "package-name" `  
  -DocumentVersion version
```

3. Eseguire il comando `Get-SSMDocumentVersionList` per verificare che la versione del pacchetto sia stata eliminata. La versione del pacchetto eliminata non è più presente nell'elenco.

```
Get-SSMDocumentVersionList `  
  -Name "package-name"
```

Per informazioni sulle altre opzioni che puoi usare con il `list-documents` comando, vedi [list-documents](#) nella AWS Systems Manager sezione del AWS CLI Command Reference. Per informazioni sulle altre opzioni che puoi utilizzare con il comando `delete-document`, consulta [delete-document](#).

Controllo e registrazione Distributor activity

Puoi utilizzarlo AWS CloudTrail per controllare le attività relative aDistributor. Per ulteriori informazioni sulle opzioni di verifica e registrazione per Systems Manager, consulta [Registrazione e monitoraggio AWS Systems Manager](#).

Audit Distributor attività utilizzando CloudTrail

CloudTrail acquisisce le chiamate API effettuate nella AWS Systems Manager console, nel AWS Command Line Interface (AWS CLI) e nel Systems Manager SDK. Puoi visualizzare queste informazioni nella CloudTrail console o archivarle in un bucket Amazon Simple Storage Service (Amazon S3). Viene utilizzato un bucket per tutti i CloudTrail log del tuo account.

I log di Run Command e le azioni di State Manager mostrano l'attività di creazione di documenti, installazione e disinstallazione di pacchetti. Run Command e State Manager sono strumenti di AWS Systems Manager. Per ulteriori informazioni sulla visualizzazione e l'utilizzo dei CloudTrail registri delle attività di Systems Manager, vedere[Registrazione dei log AWS Systems Manager Chiamate API con AWS CloudTrail](#).

Risoluzione dei problemi AWS Systems Manager Distributor

Le informazioni seguenti consentono di risolvere i problemi che potrebbero verificarsi durante l'uso di Distributor.

Argomenti

- [È installato un pacchetto errato con lo stesso nome](#)
- [Errore: non è stato possibile recuperare il manifesto. Non è stato possibile trovare la versione più recente del pacchetto](#)
- [Errore: non è stato possibile recuperare il manifesto. Eccezione per convalida](#)
- [Il pacchetto non è supportato \(manca l'azione di installazione\)](#)
- [Errore: impossibile scaricare il manifesto, Il documento con nome non esiste](#)
- [Caricamento non riuscito.](#)
- [Errore: impossibile trovare la piattaforma. Nessun manifesto trovato per la piattaforma: Oracle, versione 8.9, architettura x86_64](#)

È installato un pacchetto errato con lo stesso nome

Problema: hai installato un pacchetto, ma Distributor ha installato un pacchetto diverso.

Causa: durante l'installazione, Systems Manager rileva tra i risultati i pacchetti pubblicati da AWS prima dei pacchetti esterni definiti dall'utente. Se il nome del pacchetto definito dall'utente è lo stesso di un nome di pacchetto AWS pubblicato, il AWS pacchetto viene installato al posto del pacchetto.

Soluzione: per evitare questo problema, assegna al pacchetto un nome diverso dal nome di un pacchetto AWS pubblicato.

Errore: non è stato possibile recuperare il manifesto. Non è stato possibile trovare la versione più recente del pacchetto

Problema: hai ricevuto un errore simile al seguente.

```
Failed to retrieve manifest: ResourceNotFoundException: Could not find the latest
version of package
arn:aws:ssm::package/package-name status code: 400, request id: guid
```

Causa: stai utilizzando una versione di SSM Agent con Distributor precedente alla versione 2.3.274.0.

Soluzione: aggiorna la versione di SSM Agent alla versione 2.3.274.0 o successiva. Per ulteriori informazioni, consulta [Aggiornamento di SSM Agent utilizzando Run Command](#) o [Procedura dettagliata: aggiorna SSM Agent automaticamente con AWS CLI](#).

Errore: non è stato possibile recuperare il manifesto. Eccezione per convalida

Problema: hai ricevuto un errore simile al seguente.

```
Failed to retrieve manifest: ValidationException: 1 validation error detected: Value
'documentArn'
at 'packageName' failed to satisfy constraint: Member must satisfy regular expression
pattern:
arn:aws:ssm:region-id:account-id:package/package-name
```

Causa: stai utilizzando una versione di SSM Agent con Distributor precedente alla versione 2.3.274.0.

Soluzione: aggiorna la versione di SSM Agent alla versione 2.3.274.0 o successiva. Per ulteriori informazioni, consulta [Aggiornamento di SSM Agent utilizzando Run Command](#) o [Procedura dettagliata: aggiorna SSM Agent automaticamente con AWS CLI](#).

Il pacchetto non è supportato (manca l'azione di installazione)

Problema: hai ricevuto un errore simile al seguente.

```
Package is not supported (package is missing install action)
```

Causa: la struttura della directory del pacchetto non è corretta.

Soluzione: non comprimere una directory padre contenente il software e gli script richiesti. Invece, crea un file .zip di tutti i contenuti richiesti direttamente nel percorso assoluto. Per verificare che il file .zip è stato creato correttamente, decomprimere la directory della piattaforma di destinazione ed esaminare la struttura della directory. Ad esempio, il percorso assoluto dello script di installazione dovrebbe essere `/ExamplePackage_targetPlatform/install.sh`.

Errore: impossibile scaricare il manifesto, Il documento con nome non esiste

Problema: hai ricevuto un errore simile al seguente.

```
Failed to download manifest - failed to retrieve package document description:  
InvalidDocument: Document with name filename does not exist.
```

Causa 1: Distributor non riesce a trovare il pacchetto in base al nome del pacchetto quando si condivide un pacchetto Distributor da un altro account.

Soluzione 1: quando viene condiviso un pacchetto da un altro account, utilizzare il nome della risorsa Amazon (ARN) completo per il pacchetto e non solo il nome.

Causa 2: quando usi un VPC, non hai fornito al tuo profilo di istanza IAM l'accesso al bucket S3 AWS gestito che contiene il documento AWS-ConfigureAWSPackage per il quale Regione AWS ti stai rivolgendo.

Soluzione 2: assicurati che il profilo della tua istanza IAM SSM Agent fornisca l'accesso al bucket S3 AWS gestito che contiene il documento relativo al destinatario AWS-ConfigureAWSPackage, come spiegato Regione AWS in [Agente SSM comunicazioni con AWS bucket S3 gestiti](#)

Caricamento non riuscito.

Problema: hai ricevuto un errore simile al seguente.

```
Upload failed. At least one of your files was not successfully uploaded to your S3  
bucket.
```

Causa: il nome del pacchetto software include uno spazio. Ad esempio, Hello World.msi non verrebbe caricato.

Errore: impossibile trovare la piattaforma. Nessun manifesto trovato per la piattaforma: Oracle, versione 8.9, architettura x86_64

Problema: hai ricevuto un errore simile al seguente.

```
Failed to find platform: no manifest found for platform: oracle, version 8.9,  
architecture x86_64
```

Causa: l'errore indica che il manifesto del pacchetto JSON non ha alcuna definizione per quella piattaforma, in questo caso, Oracle Linux.

Soluzione: scarica il pacchetto che si desidera distribuire dal sito [Trend Micro Deep Security Software](#). Crea un pacchetto software .rpm utilizzando il [the section called "Crea un pacchetto utilizzando il flusso di lavoro Semplice"](#). Imposta i seguenti valori per il pacchetto e completa il pacchetto software di caricamento utilizzando Distributor:

```
Platform version: _any  
Target platform: oracle  
Architecture: x86_64
```

AWS Systems Manager Fleet Manager

Fleet Manager è un'esperienza di interfaccia utente (UI) unificata che consente di gestire in remoto i nodi in esecuzione on o on premise. AWS Con Fleet Manager è possibile visualizzare lo stato di integrità e delle prestazioni dell'intero parco istanze server da un'unica console. È inoltre possibile raccogliere dati da singoli nodi per eseguire processi comuni di risoluzione dei problemi e gestione dalla console. Ciò include la connessione alle istanze di Windows tramite Remote Desktop Protocol (RDP), la visualizzazione del contenuto di cartelle e file, la gestione del registro di Windows, la gestione degli utenti del sistema operativo e altro ancora.

Questa sezione contiene gli argomenti seguenti.

- [Configurazione Fleet Manager](#)
- [Monitoraggio delle prestazioni dei nodi gestiti](#)
- [Connessione a un Windows Server istanza gestita utilizzando Remote Desktop \(Desktop remoto\)](#)
- [Gestione dei volumi Amazon EBS all'interno di un'istanza gestita](#)
- [Accesso al portale Red Hat Knowledge base](#)

- [Visualizzazione dei log sui nodi gestiti](#)
- [Lavorare con i processi](#)
- [Gestione degli account utente e dei gruppi del sistema operativo sui nodi gestiti utilizzando Fleet Manager](#)
- [Risoluzione dei problemi di disponibilità dei nodi gestiti tramite `ssm-cli`](#)

Per cominciare a utilizzare Fleet Manager, apri la [console di Systems Manager](#). Nel pannello di navigazione, scegli Fleet Manager.

Chi dovrebbe utilizzarlo Fleet Manager?

Qualsiasi AWS cliente che desideri un modo centralizzato per gestire la propria flotta di nodi dovrebbe Fleet Manager utilizzarlo.

Come può Fleet Manager avvantaggiare la mia organizzazione?

Fleet Manager offre questi vantaggi:

- Eseguire una serie di attività comuni di amministrazione dei sistemi senza dover connettersi manualmente ai nodi gestiti.
- Gestire nodi in esecuzione su più piattaforme da un'unica console unificata.
- Gestire nodi che eseguono sistemi operativi diversi da un'unica console unificata.
- Migliorare l'efficienza dell'amministrazione dei sistemi.

Quali sono le caratteristiche di Fleet Manager?

Le funzionalità principali di Fleet Manager comprendono:

- Accedere al portale della Knowledgebase Red Hat

Accedere a binari, conoscenze condivisione e forum di discussione nel portale della Knowledgebase di Red Hat tramite istanze Red Hat Enterprise Linux (RHEL).

- Stato del nodo gestito

Visualizza quali istanze gestite sono `running` e quali istanze sono `stopped`. Per ulteriori informazioni sulle istanze arrestate, consulta [Arrestare e avviare un'istanza](#) nella Guida per l'utente

di Amazon EC2. Per i dispositivi AWS IoT Greengrass principali, puoi visualizzare quali sono online o mostrare uno stato di `Connection lost`. offline

Note

Se l'istanza è stata interrotta prima del 12 luglio 2021, non verrà visualizzata la proprietà evidenziatore `stopped`. Per mostrare l'evidenziatore, avvia e arresta l'istanza.

- Visualizzazione delle informazioni sull'istanza

Visualizza le informazioni sui dati delle cartelle e dei file archiviati nei volumi collegati alle istanze gestite, i dati sulle prestazioni delle istanze in tempo reale e i dati di log archiviati nelle istanze.

- Visualizzare le informazioni dei dispositivi edge

Visualizza il nome dell' AWS IoT Greengrass oggetto per il dispositivo, lo stato e la versione del SSM Agent ping e altro ancora.

- Gestione account e registro

Gestisci gli account utente del sistema operativo (OS) nelle istanze e il registro nelle istanze di Windows.

- Controlla l'accesso alle caratteristiche

Controlla l'accesso alle Fleet Manager funzionalità utilizzando le policy AWS Identity and Access Management (IAM). Con queste policy, puoi controllare quali utenti singoli o gruppi della tua organizzazione possono utilizzare diverse caratteristiche Fleet Manager e quali nodi gestiti possono gestire.

Configurazione Fleet Manager

Prima che gli utenti del tuo Account AWS account possano Fleet Manager utilizzare i tuoi nodi gestiti per monitorare e gestire i tuoi nodi gestiti, devono disporre delle autorizzazioni necessarie. Inoltre, è necessario che qualsiasi istanza Amazon Elastic Compute Cloud (Amazon EC2); dispositivo core AWS IoT Greengrass , server on-premises, dispositivo edge e macchina virtuale (VM) da monitorare e gestire utilizzando Fleet Manager, siano nodi gestiti da Systems Manager. Un nodo gestito è qualsiasi macchina configurata per l'uso con Systems Manager in ambienti [ibridi e multicloud](#).

Ciò significa che i nodi devono soddisfare determinati prerequisiti ed essere configurati con AWS Systems Manager Agent (SSM Agent).

A seconda del tipo di computer, fate riferimento a uno dei seguenti argomenti per assicurarvi che i computer soddisfino i requisiti per i nodi gestiti.

- Istanze Amazon EC2: [Gestire le istanze EC2 con Systems Manager](#)

 Tip

Puoi anche utilizzarlo Quick Setup per aiutarti a configurare rapidamente le tue istanze Amazon EC2 come istanze gestite in un singolo account. Se la tua azienda o organizzazione utilizza AWS Organizations, puoi anche configurare le istanze su più unità organizzative (OU) e. Regioni AWS Per ulteriori informazioni sull'utilizzo di Quick Setup per la configurazione delle istanze gestite, consulta [Configura la gestione degli host di Amazon EC2 utilizzando Configurazione rapida](#).

- On-premises e altri tipi di server nel cloud: [Gestione dei nodi in ambienti ibridi e multicloud con Systems Manager](#)
- AWS IoT Greengrass dispositivi (edge): [Gestione dei dispositivi edge con Systems Manager](#)

Policy di esempio

- [Controllo dell'accesso a Fleet Manager](#)

Controllo dell'accesso a Fleet Manager

Per utilizzarlo Fleet Manager, l'utente o il ruolo AWS Identity and Access Management (IAM) deve disporre delle autorizzazioni richieste. Puoi creare una policy IAM che fornisca accesso a tutti le funzionalità Fleet Manager oppure modifica il criterio per concedere l'accesso alle caratteristiche scelte. Quindi concedi queste autorizzazioni agli utenti o alle identità del tuo account.

Attività 1: crea policy IAM per definire le autorizzazioni di accesso

Segui uno dei metodi illustrati nel seguente argomento della Guida per l'utente IAM per creare un IAM che fornisca alle identità (utenti, ruoli o gruppi di utenti) l'accesso a Fleet Manager:

- [Definisci le autorizzazioni IAM personalizzate con le policy gestite dal cliente](#)

È possibile utilizzare una delle policy di esempio fornita di seguito o modificarle in base alle autorizzazioni che si desidera concedere. Forniamo policy di esempio di accesso completo a Fleet Manager e di accesso in sola lettura.

Attività 2: collega le policy IAM agli utenti per concedere le autorizzazioni

Dopo aver creato la policy o le policy IAM che definiscono le autorizzazioni di accesso a Fleet Manager, utilizza una delle seguenti procedure nella Guida per l'utente IAM per concedere queste autorizzazioni alle identità dell'account:

- [Aggiunta di autorizzazioni per identità IAM \(console\)](#)
- [Aggiunta di autorizzazioni per identità IAM \(AWS CLI\)](#)
- [Aggiunta di autorizzazioni per identità IAM \(API AWS\)](#)

Esempio di politica per Fleet Manager accesso amministratore

La seguente policy fornisce le autorizzazioni per tutte le funzionalità di Fleet Manager. Ciò significa che un utente può creare ed eliminare utenti e gruppi locali, modificare l'appartenenza ai gruppi per qualsiasi gruppo locale e modificare le chiavi o i valori del registro di Windows Server. Sostituisci ogni *example resource placeholder* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EC2",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2>DeleteTags",
        "ec2:DescribeInstances",
        "ec2:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Sid": "General",
      "Effect": "Allow",
      "Action": [
        "ssm:AddTagsToResource",
        "ssm:DescribeInstanceAssociationsStatus",
        "ssm:DescribeInstancePatches",
        "ssm:DescribeInstancePatchStates",
```

```

        "ssm:DescribeInstanceProperties",
        "ssm:GetCommandInvocation",
        "ssm:GetServiceSetting",
        "ssm:GetInventorySchema",
        "ssm:ListComplianceItems",
        "ssm:ListInventoryEntries",
        "ssm:ListTagsForResource",
        "ssm:ListCommandInvocations",
        "ssm:ListAssociations",
        "ssm:RemoveTagsFromResource"
    ],
    "Resource": "*"
},
{
    "Sid": "DefaultHostManagement",
    "Effect": "Allow",
    "Action": [
        "ssm:ResetServiceSetting",
        "ssm:UpdateServiceSetting"
    ],
    "Resource": "arn:aws:ssm:us-east-1:111122223333:servicesetting/ssm/managed-instance/default-ec2-instance-management-role"
},
{
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": "arn:aws:iam::111122223333:role/service-role/AWSSystemsManagerDefaultEC2InstanceManagementRole",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": [
                "ssm.amazonaws.com"
            ]
        }
    }
},
{
    "Sid": "SendCommand",
    "Effect": "Allow",
    "Action": [
        "ssm:GetDocument",
        "ssm:SendCommand",

```

```

        "ssm:StartSession"
    ],
    "Resource": [
        "arn:aws:ec2:*:111122223333:instance/*",
        "arn:aws:ssm:*:111122223333:managed-instance/*",
        "arn:aws:ssm:*:111122223333:document/SSM-SessionManagerRunShell",
        "arn:aws:ssm:*:*:document/AWS-PasswordReset",
        "arn:aws:ssm:*:*:document/AWSFleetManager-AddUsersToGroups",
        "arn:aws:ssm:*:*:document/AWSFleetManager-CopyFileSystemItem",
        "arn:aws:ssm:*:*:document/AWSFleetManager-CreateDirectory",
        "arn:aws:ssm:*:*:document/AWSFleetManager-CreateGroup",
        "arn:aws:ssm:*:*:document/AWSFleetManager-CreateUser",
        "arn:aws:ssm:*:*:document/AWSFleetManager-CreateUserInteractive",
        "arn:aws:ssm:*:*:document/AWSFleetManager-
CreateWindowsRegistryKey",
        "arn:aws:ssm:*:*:document/AWSFleetManager-DeleteFileSystemItem",
        "arn:aws:ssm:*:*:document/AWSFleetManager-DeleteGroup",
        "arn:aws:ssm:*:*:document/AWSFleetManager-DeleteUser",
        "arn:aws:ssm:*:*:document/AWSFleetManager-
DeleteWindowsRegistryKey",
        "arn:aws:ssm:*:*:document/AWSFleetManager-
DeleteWindowsRegistryValue",
        "arn:aws:ssm:*:*:document/AWSFleetManager-GetDiskInformation",
        "arn:aws:ssm:*:*:document/AWSFleetManager-GetFileContent",
        "arn:aws:ssm:*:*:document/AWSFleetManager-GetFileSystemContent",
        "arn:aws:ssm:*:*:document/AWSFleetManager-GetGroups",
        "arn:aws:ssm:*:*:document/AWSFleetManager-
GetPerformanceCounters",
        "arn:aws:ssm:*:*:document/AWSFleetManager-GetProcessDetails",
        "arn:aws:ssm:*:*:document/AWSFleetManager-GetUsers",
        "arn:aws:ssm:*:*:document/AWSFleetManager-GetWindowsEvents",
        "arn:aws:ssm:*:*:document/AWSFleetManager-
GetWindowsRegistryContent",
        "arn:aws:ssm:*:*:document/AWSFleetManager-MountVolume",
        "arn:aws:ssm:*:*:document/AWSFleetManager-MoveFileSystemItem",
        "arn:aws:ssm:*:*:document/AWSFleetManager-RemoveUsersFromGroups",
        "arn:aws:ssm:*:*:document/AWSFleetManager-RenameFileSystemItem",
        "arn:aws:ssm:*:*:document/AWSFleetManager-
SetWindowsRegistryValue",
        "arn:aws:ssm:*:*:document/AWSFleetManager-StartProcess",
        "arn:aws:ssm:*:*:document/AWSFleetManager-TerminateProcess"
    ]
},
{

```

```

        "Sid": "TerminateSession",
        "Effect": "Allow",
        "Action": [
            "ssm:TerminateSession"
        ],
        "Resource": "*",
        "Condition": {
            "StringLike": {
                "ssm:resourceTag/aws:ssmmessages:session-id": [
                    "${aws:userid}"
                ]
            }
        }
    }
}

```

Esempio di politica per Fleet Manager accesso in sola lettura

La seguente policy fornisce le autorizzazioni per le funzionalità di Fleet Manager di sola lettura. Sostituisci ogni *example resource placeholder* con le tue informazioni.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeTags"
            ],
            "Resource": "*"
        },
        {
            "Sid": "General",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeInstanceAssociationsStatus",
                "ssm:DescribeInstancePatches",

```

```

        "ssm:DescribeInstancePatchStates",
        "ssm:DescribeInstanceProperties",
        "ssm:GetCommandInvocation",
        "ssm:GetServiceSetting",
        "ssm:GetInventorySchema",
        "ssm:ListComplianceItems",
        "ssm:ListInventoryEntries",
        "ssm:ListTagsForResource",
        "ssm:ListCommandInvocations",
        "ssm:ListAssociations"
    ],
    "Resource": "*"
},
{
    "Sid": "SendCommand",
    "Effect": "Allow",
    "Action": [
        "ssm:GetDocument",
        "ssm:SendCommand",
        "ssm:StartSession"
    ],
    "Resource": [
        "arn:aws:ec2:*:111122223333:instance/*",
        "arn:aws:ssm:*:111122223333:managed-instance/*",
        "arn:aws:ssm:*:111122223333:document/SSM-SessionManagerRunShell",
        "arn:aws:ssm:*:*:document/AWSFleetManager-GetDiskInformation",
        "arn:aws:ssm:*:*:document/AWSFleetManager-GetFileContent",
        "arn:aws:ssm:*:*:document/AWSFleetManager-GetFileSystemContent",
        "arn:aws:ssm:*:*:document/AWSFleetManager-GetGroups",
        "arn:aws:ssm:*:*:document/AWSFleetManager-
GetPerformanceCounters",
        "arn:aws:ssm:*:*:document/AWSFleetManager-GetProcessDetails",
        "arn:aws:ssm:*:*:document/AWSFleetManager-GetUsers",
        "arn:aws:ssm:*:*:document/AWSFleetManager-GetWindowsEvents",
        "arn:aws:ssm:*:*:document/AWSFleetManager-
GetWindowsRegistryContent"
    ]
},
{
    "Sid": "TerminateSession",
    "Effect": "Allow",
    "Action": [
        "ssm:TerminateSession"
    ],

```



```
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "ssm:resourceTag/aws:ssmmessages:session-id": [
          "${aws:userid}"
        ]
      }
    }
  ]
}
```

Utilizzo dei nodi gestiti

Un nodo gestito è qualsiasi macchina configurata per AWS Systems Manager. Puoi configurare i seguenti tipi di macchine come nodi gestiti:

Questa sezione contiene gli argomenti seguenti.

- [Reimpostazione delle password nei nodi gestiti.](#)
- [Gestione del registro di Windows sui nodi gestiti](#)
- Istanze Amazon Elastic Compute Cloud (Amazon EC2)
- Server presso la propria sede (server on-premises)
- AWS IoT Greengrass dispositivi principali
- AWS IoT e dispositivi non AWS periferici
- Macchine virtuali (VM), incluse le macchine virtuali in altri ambienti cloud

Nella console di Systems Manager, qualsiasi macchina con prefisso "mi-" è stata configurata come nodo gestito utilizzando un'[attivazione ibrida](#). I dispositivi Edge visualizzano il nome dell' AWS IoT oggetto.

Note

L'unica funzionalità supportata per le istanze di macOS è la visualizzazione del file system.

 Note

Importante: a partire dal 30 giugno 2026, il livello di istanze avanzate è stato rimosso. Non esiste più un limite di 1.000 istanze per i nodi gestiti ibridi e non è più necessario abilitare un livello a pagamento da utilizzare su macchine non EC2. Session Manager Invece, a partire dal 30 settembre 2026, utilizza i prezzi Session Manager pay-as-you-go se Run Command utilizzati su nodi gestiti ibridi.

Per ulteriori informazioni sui prezzi, consulta [Prezzi di AWS Systems Manager](#).

Visualizza i nodi gestiti

Se i propri nodi gestiti non sono elencati nella console, procedi come segue:

1. Verifica che la console sia aperta nel luogo in cui hai creato i nodi gestiti Regione AWS. È possibile passare da una Regione all'altra utilizzando l'elenco nell'angolo in alto a destra della console.
2. Verifica che la procedura di configurazione per i nodi gestiti soddisfi i requisiti di Systems Manager. Per informazioni, consulta [Configurazione dei nodi gestiti per AWS Systems Manager](#).
3. Per le macchine non EC2, verifica di aver completato il processo di attivazione ibrida. Per ulteriori informazioni, consulta [Gestione dei nodi in ambienti ibridi e multicloud con Systems Manager](#).

Prendi nota della seguenti informazioni aggiuntive:

- La console di Fleet Manager non visualizza i nodi Amazon EC2 che sono stati terminati.
- Systems Manager richiede riferimenti temporali accurati per eseguire operazioni sui computer. Se la data e l'ora non sono impostate correttamente nei nodi gestiti, tali informazioni potrebbero non corrispondere alla data di firma delle richieste API. Per ulteriori informazioni, consulta [Casi d'uso e best practice](#).
- Quando crei o modifichi tag, potrebbe volerci fino a un'ora affinché il sistema mostri le modifiche nel filtro della tabella.
- Se lo stato di un nodo gestito è rimasto `Connection Lost` per almeno 30 giorni, il nodo potrebbe non essere più elencato nella console Fleet Manager. Per inserirlo nuovamente nell'elenco, è necessario risolvere il problema che ha causato la perdita della connessione. Per suggerimenti sulla risoluzione dei problemi, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#).

Verifica del supporto di Systems Manager su un nodo gestito

AWS Config fornisce AWS Managed Rules, regole predefinite e personalizzabili che vengono AWS Config utilizzate per valutare se le configurazioni AWS delle risorse sono conformi alle best practice più comuni. AWS Config Le regole gestite includono la regola <https://docs.aws.amazon.com/config/latest/developerguide/ec2-instance-managed-by-systems-manager.html> ec2-instance-managed-by-systems-manager. Questa regola verifica se le istanze Amazon EC2 dell'account sono gestite da Systems Manager. Per ulteriori informazioni, consulta [Regole gestite di AWS Config](#).

Maggiore sicurezza nei nodi gestiti

Per informazioni su come aumentare la posizione di sicurezza rispetto ai comandi non autorizzati a livello di root nei nodi gestiti, consulta [Limitare l'accesso ai comandi a livello di root tramite SSM Agent](#)

Annullare registrazione dei nodi gestiti

Puoi annullare la registrazione dei nodi gestiti in qualsiasi momento. Ad esempio, se gestisci più nodi con lo stesso ruolo AWS Identity and Access Management (IAM) e noti qualsiasi tipo di comportamento dannoso, puoi annullare la registrazione di un numero qualsiasi di macchine in qualsiasi momento. (Per registrare nuovamente la stessa macchina, è necessario utilizzare un codice di attivazione ibrido e un ID di attivazione diversi da quelli utilizzati in precedenza per la registrazione.) Per ulteriori informazioni sull'annullamento delle registrazioni dei nodi gestiti, consulta [Annullamento della registrazione dei nodi gestiti in un ambiente ibrido e multicloud](#).

Reimpostazione delle password nei nodi gestiti.

Puoi ripristinare la password per qualsiasi utente su un nodo gestito. Ciò include le istanze Amazon Elastic Compute Cloud (Amazon EC2), i dispositivi AWS IoT Greengrass principali e i server locali, i dispositivi edge e le macchine virtuali (VM) gestiti da AWS Systems Manager La funzionalità di reimpostazione della password è integrata. Session Manager Puoi usare questa funzionalità per connetterti a nodi gestiti senza aprire porte in entrata, mantenendo host bastione o gestendo chiavi SSH.

Il ripristino della password è utile quando un utente ha dimenticato una password o quando desidera aggiornare rapidamente una password senza effettuare una connessione RDP o SSH al nodo gestito.

Prerequisiti

Prima di ripristinare la password in un nodo gestito, è necessario soddisfare i seguenti requisiti:

- Il nodo gestito su cui desideri modificare una password deve essere un nodo gestito di Systems Manager. Inoltre, la versione SSM Agent 2.3.668.0 o successiva deve essere installata sul nodo gestito.) Per informazioni sull'installazione o l'aggiornamento di SSM Agent, consulta [Lavorare con Agente SSM](#).
- La funzione di ripristino della password utilizza la configurazione Session Manager impostata per l'account per connettersi al nodo gestito. Pertanto, i prerequisiti per l'utilizzo di Session Manager devono essere stati completati per il tuo account nella Regione AWS corrente. Per ulteriori informazioni, consulta [Configurazione di Session Manager](#).
- L' AWS utente che modifica la password deve disporre dell'ssm: SendCommand autorizzazione per il nodo gestito. Per ulteriori informazioni, consulta [Limitazione Run Command accesso basato su tag](#).

Limitazione dell'accesso

Puoi limitare la capacità di un utente di ripristinare le password a istanze specifiche. Questo avviene mediante policy basate sull'identità per l'operazione Session Manager `ssm:StartSession` con il documento SSM AWS-PasswordReset. Per ulteriori informazioni, consulta [Controllo dell'accesso della sessione utente alle istanze](#).

Crittografia dei dati

Attiva AWS Key Management Service (AWS KMS) la crittografia completa per Session Manager i dati per utilizzare l'opzione di reimpostazione della password per i nodi gestiti. Per ulteriori informazioni, consulta [Attiva la crittografia delle chiavi KMS per i dati delle sessioni \(console\)](#).

Reimpostazione di una password su un nodo gestito

È possibile reimpostare una password su un nodo gestito da Systems Manager utilizzando la Fleet Manager console Systems Manager o AWS Command Line Interface (AWS CLI).

Per modificare la password su un nodo gestito (console)

1. Aprire la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli il pulsante accanto al nodo che richiede una nuova password.
4. Scegli Operazioni istanza, Reimposta password.

5. Per User name (Nome utente), inserisci il nome dell'utente per il quale stai modificando la password. Può essere qualsiasi nome utente che dispone di un account sul nodo.
6. Seleziona Invia.
7. Segui i prompt nella finestra di comando Enter new password (Inserisci nuova password) per specificare la nuova password.

Note

Se la versione di SSM Agent sul nodo gestito non supporta la reimpostazione della password, ti verrà richiesto di installare una versione supportata utilizzando. Run Command

Per reimpostare la password su un nodo gestito (AWS CLI)

1. Per ripristinare la password per un utente su un nodo gestito, esegui il comando seguente. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Note

Per utilizzare il AWS CLI per reimpostare una password, il Session Manager plug-in deve essere installato sul computer locale. Per informazioni, consulta [Installa il Session Manager plugin per AWS CLI](#).

Linux & macOS

```
aws ssm start-session \  
  --target instance-id \  
  --document-name "AWS-PasswordReset" \  
  --parameters '{"username": ["user-name"]}'
```

Windows

```
aws ssm start-session ^  
  --target instance-id ^  
  --document-name "AWS-PasswordReset" ^  
  --parameters username="user-name"
```

2. Segui i prompt nella finestra di comando Enter new password (Inserisci nuova password) per specificare la nuova password.

Risoluzione dei problemi di reimpostazione della password su nodi gestiti.

Molti problemi di reimpostazione password possono essere risolti assicurando di aver completato i [prerequisiti di reimpostazione della password](#). Per altri problemi, utilizza le informazioni seguenti per risolvere i problemi di reimpostazione della password.

Nodo gestito non disponibile

Problema: desideri reimpostare la password per un nodo gestito nella pagina della console Managed instances (Istanze gestite), ma il nodo non è nell'elenco.

- Soluzione: il nodo gestito a cui connettersi potrebbe non essere configurato per Systems Manager. Per utilizzare un'istanza EC2 con Systems Manager, è necessario allegare all'istanza un profilo di istanza AWS Identity and Access Management (IAM) che consenta a Systems Manager di eseguire azioni sulle istanze. Per informazioni, consulta la pagina [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#).

Per usare una macchina non EC2 con Systems Manager, crea un ruolo di servizio IAM che fornisca a Systems Manager l'autorizzazione per eseguire operazioni sui nodi gestiti. Per ulteriori informazioni, consulta [Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud](#).

Agente SSM non aggiornato (console)

Problema: un messaggio segnala che la versione di SSM Agent non supporta la funzionalità di reimpostazione della password.

- Soluzione: è necessario installare la versione 2.3.668.0 o successiva per SSM Agent eseguire la reimpostazione della password. Nella console, puoi aggiornare l'agente sul nodo gestito scegliendo Update SSM Agent (Aggiorna agente SSM).

Una versione aggiornata di SSM Agent viene distribuita ogni volta che vengono aggiunti nuovi strumenti a Systems Manager o eseguiti aggiornamenti degli strumenti esistenti. Il mancato utilizzo della versione più recente dell'agente può impedire al nodo gestito di utilizzare vari strumenti e funzionalità di Systems Manager. Per questo motivo, ti consigliamo di automatizzare il processo di aggiornamento di SSM Agent sulle macchine. Per informazioni, consulta [Automatizzazione degli](#)

[aggiornamenti a Agente SSM](#). Iscriviti alla pagina [Note di rilascio di SSM Agent](#) su GitHub per ricevere notifiche sugli aggiornamenti di SSM Agent.

Le opzioni di reimpostazione della password non sono fornite (AWS CLI)

Problema: ci si connette correttamente a un nodo gestito utilizzando il AWS CLI [start-session](#) comando. Hai specificato il documento SSM AWS-PasswordReset e fornito un nome utente valido, ma le richieste di modifica della password non vengono visualizzate.

- Soluzione: la versione di SSM Agent sul nodo gestito non è aggiornata. Per eseguire la reimpostazione delle password è richiesta la versione 2.3.668.0 o successiva.

Una versione aggiornata di SSM Agent viene distribuita ogni volta che vengono aggiunti nuovi strumenti a Systems Manager o eseguiti aggiornamenti agli strumenti esistenti. Il mancato utilizzo della versione più recente dell'agente può impedire al nodo gestito di utilizzare vari strumenti e funzionalità di Systems Manager. Per questo motivo, ti consigliamo di automatizzare il processo di aggiornamento di SSM Agent sulle macchine. Per informazioni, consulta [Automatizzazione degli aggiornamenti a Agente SSM](#). Iscriviti alla pagina [Note di rilascio di SSM Agent](#) su GitHub per ricevere notifiche sugli aggiornamenti di SSM Agent.

Nessuna autorizzazione per eseguire **ssm: SendCommand**

Problema: tenti di connetterti a un nodo gestito per modificarne la password, ma ricevi un messaggio di errore che indica che non sei autorizzato a eseguire `ssm: SendCommand` sul nodo gestito.

- Soluzione: la policy IAM deve includere l'autorizzazione per eseguire il comando `ssm: SendCommand`. Per informazioni, consulta [Limitazione Run Command accesso basato su tag](#).

Session Manager messaggio di errore

Problema: ricevi un messaggio di errore correlato a Session Manager.

- Soluzione: il supporto della reimpostazione della password richiede che Session Manager sia configurato correttamente. Per informazioni, consulta [Configurazione di Session Manager](#) e [Risoluzione dei problemi relativi a Session Manager](#).

Annullamento della registrazione dei nodi gestiti in un ambiente ibrido e multicloud

Se non desideri più gestire un server locale, un dispositivo edge o una macchina virtuale (VM) utilizzando AWS Systems Manager, puoi annullare la registrazione. L'annullamento della registrazione di un nodo attivato in modalità ibrida lo rimuove dall'elenco dei nodi gestiti in Systems Manager. AWS Systems Manager L'agente (SSM Agent) in esecuzione sul nodo attivato da sistemi ibridi non sarà in grado di aggiornare il token di autorizzazione perché non è più registrato. SSM Agent verrà ibernato e riduce la sua frequenza di ping a Systems Manager nel cloud a una volta all'ora. Systems Manager gestisce la cronologia dei comandi per un nodo gestito di cui è stata annullata la registrazione per 30 giorni.

Note

Puoi registrare nuovamente un server on-premises, un dispositivo periferico o una macchina virtuale locale utilizzando lo stesso codice di attivazione e lo stesso ID, purché non sia stato raggiunto il limite di istanze per il codice di attivazione e l'ID designati. Puoi verificare il limite di istanze nella console scegliendo Strumenti per i nodi, quindi scegli Attivazioni ibride. Se il valore delle istanze registrate è inferiore al limite di registrazione, puoi registrare nuovamente una macchina utilizzando lo stesso codice di attivazione e lo stesso ID. Se è maggiore, è necessario utilizzare un codice di attivazione e un ID diversi.

Nella procedura seguente viene descritto come annullare la registrazione di un nodo attivato da sistemi ibridi utilizzando la console di Systems Manager. Per informazioni su come eseguire questa operazione utilizzando l' AWS Command Line Interface, consulta [deregister-managed-instance](#).

Per le relative informazioni, consultare i seguenti argomenti:

- [Annullamento della registrazione e nuova registrazione di un nodo gestito \(Linux\)](#) (Linux)
- [Annullare la registrazione e ri-registrare un nodo gestito \(Windows Server\)](#) (Windows Server)

Per annullare la registrazione di un nodo (console) attivato in modalità ibrida

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Selezionare la casella di controllo accanto al nodo gestito di cui si desidera annullare la registrazione.

4. Scegliere Operazioni del nodo, Strumenti, Annulla la registrazione di questo nodo gestito.
5. Esaminare le informazioni nella finestra di dialogo Annulla la registrazione di questo nodo gestito. in caso di approvazione, scegliere Annulla registrazione.

Lavorare con i file system del sistema operativo utilizzando Fleet Manager

È possibile Fleet Manager utilizzarlo per lavorare con il file system sui nodi gestiti. Utilizzando Fleet Manager è possibile visualizzare le informazioni sulla directory e i dati dei file memorizzati nei volumi collegati ai nodi gestiti. Ad esempio, è possibile visualizzare il nome, le dimensioni, l'estensione, il proprietario e le autorizzazioni per le directory e i file. È possibile visualizzare in anteprima fino a 10.000 righe di dati di file come testo dalla console Fleet Manager. Puoi utilizzare questa funzionalità anche per i file `tail`. Quando utilizzi `tail` per visualizzare i dati di file, le ultime 10 righe del file vengono visualizzate all'inizio. Man mano che nuove righe di dati vengono scritte nel file, la visualizzazione viene aggiornata in tempo reale. Di conseguenza, è possibile esaminare i dati di registro dalla console, in modo da migliorare l'efficienza della risoluzione dei problemi e dell'amministrazione dei sistemi. Inoltre è possibile creare directory e copiare, tagliare, incollare, rinominare o eliminare file e directory.

Questa sezione contiene gli argomenti seguenti.

- [Visualizzazione del file system del sistema operativo tramite Fleet Manager](#)
- [Visualizzazione in anteprima dei file del sistema operativo utilizzando Fleet Manager](#)
- [Tailing dei file del sistema operativo utilizzando Fleet Manager](#)
- [Copiare, tagliare e incollare file o directory del sistema operativo utilizzando Fleet Manager](#)
- [Rinominare file e directory del sistema operativo utilizzando Fleet Manager](#)
- [Eliminazione di file e directory del sistema operativo utilizzando Fleet Manager](#)
- [Creazione di directory del sistema operativo utilizzando Fleet Manager](#)
- [Tagliare, copiare e incollare le directory del sistema operativo utilizzando Fleet Manager](#)

Consigliamo di creare backup regolari o di fare snapshot dei volumi Amazon Elastic Block Store (Amazon EBS) collegati ai nodi gestiti. Quando vengono copiati, tagliati o incollati i file, vengono sostituiti i file e le directory esistenti nel percorso di destinazione con lo stesso nome dei nuovi file o directory. Se si sostituiscono o si modificano file e directory di sistema, possono verificarsi seri problemi. AWS non garantisce che questi problemi possano essere risolti. Modificare i file di sistema

a proprio rischio. L'utente è responsabile di tutte le modifiche ai file e alle directory e garantisce di disporre di backup. L'eliminazione o la sostituzione di file e directory non può essere annullata.

Note

Fleet Manager utilizza Session Manager per visualizzare anteprime di testo e `tail` file. Per le istanze di Amazon Elastic Compute Cloud (Amazon EC2), il profilo dell'istanza associato alle istanze gestite deve fornire le autorizzazioni per Session Manager in modo da poter utilizzare questa funzionalità. Per ulteriori informazioni sull'aggiunta delle autorizzazioni Session Manager a un profilo dell'istanza, consulta [Aggiunta di autorizzazioni Session Manager per un ruolo IAM esistente](#).

Visualizzazione del file system del sistema operativo tramite Fleet Manager

Utilizza Fleet Manager per visualizzare il file system del sistema operativo su un nodo gestito da Systems Manager.

Per visualizzare il file system del sistema operativo utilizzando Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Seleziona il collegamento del nodo gestito con il file system che desideri visualizzare.
4. Scegli Strumenti, File system.

Visualizzazione in anteprima dei file del sistema operativo utilizzando Fleet Manager

Utilizza Fleet Manager per visualizzare in anteprima i file di testo su un sistema operativo.

Per visualizzare le anteprime di testo dei file utilizzando Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Seleziona il collegamento del nodo gestito con i file che desideri visualizzare in anteprima.
4. Scegli Strumenti, File system.
5. Seleziona il Nome del file della directory contenente il file da visualizzare in anteprima.

6. Scegli il pulsante accanto al file di cui si desidera visualizzare in anteprima il contenuto.
7. Scegli Operazioni, Anteprima come testo.

Tailing dei file del sistema operativo utilizzando Fleet Manager

Utilizza Fleet Manager per eseguire il tailing di un file su un nodo gestito.

Per eseguire il tailing dei file con Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Seleziona il collegamento del nodo gestito con i file che desideri controllare.
4. Scegli Strumenti, File system.
5. Seleziona il File name (Nome del file) della directory contenente il file da controllare.
6. Scegli il pulsante accanto al file di cui si desidera eseguire la coda del contenuto.
7. Scegli Operazioni, File di coda.

Copiare, tagliare e incollare file o directory del sistema operativo utilizzando Fleet Manager

Utilizza Fleet Manager per copiare, tagliare e incollare file del sistema operativo su un nodo gestito.

Per copiare o tagliare e incollare file o directory utilizzando Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Selezionare il collegamento del nodo gestito con i file che si desidera copiare o tagliare e incollare.
4. Scegli Strumenti, File system.
5. Per copiare o tagliare un file, selezionare il Nome file della directory che contiene il file che si desidera copiare o tagliare. Per copiare o tagliare una cartella, scegli il pulsante accanto alla cartella che desideri copiare o tagliare. Procedete quindi al passaggio 8.
6. Scegli il pulsante accanto al file che si desidera copiare o tagliare.
7. Nel menu Actions (Operazioni) scegli Copy (Copia) o Cut (Taglia).

8. Nella schermata File system, scegli il pulsante accanto alla directory in cui incollare il file.
9. Nel menu Actions (Operazioni), scegli Paste (Incolla).

Rinominare file e directory del sistema operativo utilizzando Fleet Manager

Utilizza Fleet Manager per rinominare file e directory su nodo gestito nell'account.

Per rinominare file o directory con Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Selezionare il collegamento del nodo gestito con i file o le directory che si desidera rinominare.
4. Scegli Strumenti, File system.
5. Per rinominare un file, selezionare il Nome file della directory che contiene il file che si desidera rinominare. Per rinominare una directory, scegliere il pulsante accanto alla directory che si desidera rinominare e quindi procedere al passaggio 8.
6. Scegli il pulsante accanto al file che desideri rinominare.
7. Scegli Operazioni, Rinomina.
8. Nel campo Nome file, inserisci il nuovo nome per il file e seleziona Rinomina.

Eliminazione di file e directory del sistema operativo utilizzando Fleet Manager

Utilizza Fleet Manager per eliminare file e directory su un nodo gestito nell'account.

Per eliminare file o directory utilizzando Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Seleziona il collegamento del nodo gestito con i file o le directory che desideri eliminare.
4. Scegli Strumenti, File system.
5. Per eliminare un file, seleziona il Nome file della directory che contiene il file che desideri eliminare. Per eliminare una directory, scegli il pulsante accanto alla directory da eliminare e procedere al passaggio 7.

6. Scegli il pulsante accanto al file che desideri eliminare.
7. Scegli Operazioni, Elimina.

Creazione di directory del sistema operativo utilizzando Fleet Manager

Utilizza Fleet Manager per creare directory su nodo gestito nell'account.

Per creare una directory utilizzando Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Seleziona il collegamento del nodo gestito in cui desideri creare una directory.
4. Scegli Strumenti, File system.
5. Seleziona il File Name (Nome file) della directory in cui desideri creare una nuova directory.
6. Seleziona CREATE DIRECTORY.
7. Nel campo Nome directory, inserisci il nome per la nuova directory e seleziona Crea directory.

Tagliare, copiare e incollare le directory del sistema operativo utilizzando Fleet Manager

Utilizza Fleet Manager per tagliare, copiare e incollare le directory su un nodo gestito nell'account.

Per copiare o tagliare e incollare le directory con Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Selezionare il collegamento del nodo gestito con i file che si desidera copiare o tagliare e incollare.
4. Scegli Strumenti, File system.
5. Scegliere il pulsante accanto alla directory che si desidera copiare o tagliare e quindi procedere al passaggio 8.
6. Nel menu Actions (Operazioni) scegli Copy (Copia) o Cut (Taglia).
7. Nella schermata File system, scegli il pulsante accanto alla directory in cui incollare il file.
8. Nel menu Actions (Operazioni), scegli Paste (Incolla).

Monitoraggio delle prestazioni dei nodi gestiti

Puoi utilizzarlo Fleet Manager per visualizzare i dati sulle prestazioni dei tuoi nodi gestiti in tempo reale. I dati sulle prestazioni vengono recuperati dalle unità di conteggio delle prestazioni.

Le seguenti unità di conteggio delle prestazioni sono disponibili in Fleet Manager:

- Utilizzo CPU
- Utilizzo di Disk input/output (I/O)
- Traffico di rete
- Utilizzo della memoria

Note

Fleet Manager utilizza Session Manager per recuperare i dati sulle prestazioni. Per le istanze di Amazon Elastic Compute Cloud (Amazon EC2), il profilo dell'istanza associato alle istanze gestite deve fornire le autorizzazioni per Session Manager in modo da poter utilizzare questa funzionalità. Per ulteriori informazioni sull'aggiunta delle autorizzazioni Session Manager a un profilo dell'istanza, consulta [Aggiunta di autorizzazioni Session Manager per un ruolo IAM esistente](#).

Per visualizzare i dati sulle prestazioni con Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli il pulsante accanto al nodo gestito di cui desideri monitorare le prestazioni.
4. Seleziona Visualizza dettagli.
5. Scegli Strumenti, Contatori delle prestazioni.

Lavorare con i processi

Puoi usarlo Fleet Manager per lavorare con i processi sui tuoi nodi gestiti. Utilizzando Fleet Manager, puoi visualizzare le informazioni relative ai processi. Ad esempio, è possibile visualizzare l'utilizzo della CPU e della memoria dei processi oltre ai relativi handle e thread. Con Fleet Manager, è possibile avviare e terminare i processi dalla console.

Questa sezione contiene gli argomenti seguenti.

- [Visualizzazione dei dettagli sui processi del sistema operativo utilizzando Fleet Manager](#)
- [Avvio di un processo del sistema operativo su un nodo gestito utilizzando Fleet Manager](#)
- [Interruzione di un processo del sistema operativo utilizzando Fleet Manager](#)

 Note

Fleet Manager utilizza Session Manager per recuperare i dati di processo. Per le istanze di Amazon Elastic Compute Cloud (Amazon EC2), il profilo dell'istanza associato alle istanze gestite deve fornire le autorizzazioni per Session Manager in modo da poter utilizzare questa funzionalità. Per ulteriori informazioni sull'aggiunta delle autorizzazioni Session Manager a un profilo dell'istanza, consulta [Aggiunta di autorizzazioni Session Manager per un ruolo IAM esistente](#).

Visualizzazione dei dettagli sui processi del sistema operativo utilizzando Fleet Manager

Utilizza Fleet Manager per visualizzare i dettagli sui processi sui nodi gestiti.

Per visualizzare i dettagli relativi ai processi con Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Selezionare il collegamento del nodo di cui si desidera visualizzare i processi.
4. Scegli Strumenti, Processi.

Avvio di un processo del sistema operativo su un nodo gestito utilizzando Fleet Manager

Utilizza Fleet Manager per avviare un processo su un nodo gestito.

Per avviare un processo con Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.

3. Seleziona il collegamento del nodo gestito su cui desideri avviare un processo.
4. Scegli Strumenti, Processi.
5. Seleziona Start new process (Avvia un nuovo processo).
6. Nel campo Nome del processo o percorso completo, inserisci il nome del processo o il percorso completo dell'eseguibile.
7. (Facoltativo) Nel campo Directory di lavoro, immetti il percorso della directory in cui desideri eseguire il processo.

Interruzione di un processo del sistema operativo utilizzando Fleet Manager

Per interrompere un processo del sistema operativo utilizzando Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Seleziona il collegamento del nodo gestito su cui desideri avviare un processo.
4. Scegli Strumenti, Processi.
5. Scegliere il pulsante accanto al processo che si desidera terminare.
6. Scegli Operazioni, Terminare il processo oppure Operazioni, Terminare la struttura del processo.

Note

La chiusura di un albero di processo termina anche tutti i processi e le applicazioni che utilizzano tale processo.

Visualizzazione dei log sui nodi gestiti

È possibile Fleet Manager utilizzarlo per visualizzare i dati di registro archiviati nei nodi gestiti. Per i nodi gestiti di Windows, è possibile visualizzare i log eventi Windows e copiare i relativi dettagli dalla console. Per facilitare la ricerca degli eventi, filtrare i registri eventi di Windows in base al livello dell'evento, all'ID evento, all'origine evento e all'ora di creazione. È inoltre possibile visualizzare altri dati di registro utilizzando la procedura descritta per visualizzare il file system. Per ulteriori informazioni sulla visualizzazione del file system con Fleet Manager consulta [Lavorare con i file system del sistema operativo utilizzando Fleet Manager](#).

Per visualizzare i registri degli eventi di Windows con Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli il pulsante accanto al nodo gestito di cui si desidera visualizzare i registri di eventi.
4. Seleziona Visualizza dettagli.
5. Scegli Strumenti, Log eventi di Windows.
6. Seleziona il Log name (Nome log) che contiene gli eventi che si desidera visualizzare.
7. Selezionare il pulsante accanto al Log name (Nome log) che si desidera visualizzare, quindi selezionare View events (Visualizza eventi).
8. Seleziona il pulsante accanto all'evento che desideri visualizzare, quindi seleziona View event details (Visualizza dettagli evento).
9. (Opzionale) Seleziona Copy as JSON (Copia come JSON) per copiare i dettagli dell'evento negli appunti.

Gestione degli account utente e dei gruppi del sistema operativo sui nodi gestiti utilizzando Fleet Manager

Puoi utilizzarlo Fleet Manager per gestire gli account utente e i gruppi del sistema operativo (OS) sui nodi gestiti. Ad esempio, è possibile creare ed eliminare utenti e gruppi. Inoltre, è possibile visualizzare dettagli quali l'appartenenza al gruppo, i ruoli utente e lo stato.

Questa sezione contiene gli argomenti seguenti.

- [Creazione di un utente o gruppo del sistema operativo utilizzando Fleet Manager](#)
- [Aggiornamento dell'appartenenza di un utente o di un gruppo utilizzando Fleet Manager](#)
- [Eliminazione di un utente o gruppo del sistema operativo utilizzando Fleet Manager](#)

Important

Fleet Manager utilizza Run Command e Session Manager, strumenti AWS Systems Manager, per varie operazioni di gestione degli utenti. Di conseguenza, un utente potrebbe concedere autorizzazioni a un account utente del sistema operativo che altrimenti non sarebbe possibile. Questo perché AWS Systems Manager Agent (SSM Agent) viene eseguito su istanze

Amazon Elastic Compute Cloud (Amazon EC2) utilizzando i permessi di root (Linux) o i permessi SYSTEM (). Windows Server Per ulteriori informazioni su come limitare l'accesso ai comandi di livello root tramite SSM Agent, consulta [Limitare l'accesso ai comandi a livello di root tramite SSM Agent](#). Per limitare l'accesso a questa funzionalità, ti consigliamo di creare policy AWS Identity and Access Management (IAM) per i tuoi utenti che consentano l'accesso solo alle azioni che definisci. Per ulteriori informazioni sulla creazione di policy IAM per Fleet Manager, consulta [Controllo dell'accesso a Fleet Manager](#).

Creazione di un utente o gruppo del sistema operativo utilizzando Fleet Manager

Note

Fleet Manager utilizza Session Manager per impostare le password per i nuovi utenti. Per le istanze Amazon EC2, il profilo istanza associato alle tue istanze gestite deve fornire le autorizzazioni per Session Manager in modo da poter utilizzare questa funzionalità. Per ulteriori informazioni sull'aggiunta delle autorizzazioni Session Manager a un profilo dell'istanza, consulta [Aggiunta di autorizzazioni Session Manager per un ruolo IAM esistente](#).

Invece di accedere direttamente a un server per creare un account utente o un gruppo, è possibile utilizzare la console Fleet Manager per eseguire le stesse attività.

Per creare un account utente del sistema operativo utilizzando Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli il pulsante accanto al nodo gestito su cui si desidera creare un nuovo utente.
4. Seleziona Visualizza dettagli.
5. Scegli Strumenti, Utenti e gruppi.
6. Seleziona la scheda Users (Utenti), quindi scegli Create user (Creazione dell'utente).
7. Inserire un valore per Name (Nome) del nuovo utente.
8. (Consigliato) Seleziona la casella di controllo accanto a Set password (Imposta password). Al termine della procedura viene richiesto di fornire una password per il nuovo utente.

9. Seleziona **Create user** (Crea utente). Se è stata selezionata la casella di controllo per creare una password per il nuovo utente, viene richiesto di immettere un valore per la password e selezionare **Fine**. Se la password specificata non soddisfa i requisiti specificati dalle policy locali o di dominio del nodo gestito, viene restituito un errore.

Per creare un gruppo di sistemi operativi utilizzando Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli **Fleet Manager**.
3. Scegli il pulsante accanto al nodo gestito in cui si desidera creare un gruppo.
4. Seleziona **Visualizza dettagli**.
5. Scegli **Strumenti, Utenti e gruppi**.
6. Scegliere la scheda **Gruppi** quindi scegliere **Crea gruppo**.
7. Inserire un valore per **Name** (Nome) del nuovo gruppo.
8. (Opzionale) inserire un valore per **Description** (Descrizione) del nuovo gruppo.
9. (Opzionale) Seleziona gli utenti da aggiungere a **Group members** (Membri del gruppo) per il nuovo gruppo.
10. Seleziona **Create group** (Crea gruppo).

Aggiornamento dell'appartenenza di un utente o di un gruppo utilizzando Fleet Manager

Non è necessario accedere direttamente a un server per aggiornare un account utente o un gruppo. È possibile utilizzare la Fleet Manager console per eseguire queste attività.

Per aggiungere un account utente del sistema operativo a un nuovo gruppo utilizzando Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli **Fleet Manager**.
3. Scegli il pulsante accanto al nodo gestito in cui esiste l'account utente che desideri aggiornare.
4. Seleziona **Visualizza dettagli**.
5. Scegli **Strumenti, Utenti e gruppi**.

6. Scegli la scheda Users (Utenti);
7. Scegli il pulsante accanto all'utente che si desidera aggiornare.
8. Scegli Operazioni, Aggiungi utente al gruppo.
9. Scegli il gruppo a cui aggiungere l'utente in Add to group (Aggiungi a gruppo).
10. Seleziona Add user to group (Aggiungi utente al gruppo).

Per modificare l'appartenenza di un gruppo di sistemi operativi utilizzando Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli il pulsante accanto al nodo gestito in cui esiste il gruppo che desideri aggiornare.
4. Seleziona Visualizza dettagli.
5. Scegli Strumenti, Utenti e gruppi.
6. Scegliere la scheda Groups (Gruppi).
7. Scegli il pulsante accanto al gruppo che si desidera aggiornare.
8. Scegli Operazioni, Modifica gruppo.
9. Scegli gli utenti che desideri aggiungere o rimuovere in Group members (Membri del gruppo).
10. Seleziona Modify group (Modifica gruppo).

Eliminazione di un utente o gruppo del sistema operativo utilizzando Fleet Manager

Non è necessario accedere direttamente a un server per eliminare un account utente o un gruppo. È possibile utilizzare la Fleet Manager console per eseguire queste attività.

Per eliminare un account utente del sistema operativo utilizzando Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli il pulsante accanto al nodo gestito in cui esiste l'account utente che desideri eliminare.
4. Seleziona Visualizza dettagli.
5. Scegli Utenti e gruppi.
6. Scegli la scheda Users (Utenti);

7. Scegli il pulsante accanto all'utente che si desidera eliminare.
8. Scegli Operazioni, Elimina utente locale.

Per eliminare un gruppo di sistemi operativi utilizzando Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli il pulsante accanto al nodo gestito in cui esiste il gruppo che desideri eliminare.
4. Seleziona Visualizza dettagli.
5. Scegli Strumenti, Utenti e gruppi.
6. Scegli la scheda Group (Gruppo).
7. Scegli il pulsante accanto al gruppo che si desidera aggiornare.
8. Scegli Operazioni, Elimina gruppo locale.

Gestione del registro di Windows sui nodi gestiti

È possibile Fleet Manager utilizzarlo per gestire il registro sui nodi Windows Server gestiti. Dalla console Fleet Manager è possibile creare, copiare, aggiornare ed eliminare voci e valori del registro.

 Important

Ti consigliamo di creare un backup del registro o di acquisire uno snapshot del volume principale Amazon Elastic Block Store (Amazon EBS) allegato al tuo nodo gestito, prima di modificare il registro. Possono verificarsi problemi gravi se si modifica il registro in modo errato. Questi problemi potrebbero richiedere la reinstallazione del sistema operativo o il ripristino del volume principale del nodo da un'istantanea. AWS non garantisce che questi problemi possano essere risolti. Modifica il registro a proprio rischio e pericolo. L'utente è responsabile di tutte le modifiche al registro e garantisce di disporre di backup.

Crea una chiave o voce del registro di Windows

Per creare una chiave di registro di Windows con Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli il pulsante accanto al nodo gestito in cui desideri creare una chiave di registro.
4. Seleziona Visualizza dettagli.
5. Scegli Strumenti, Registro di Windows.
6. Scegli l'hive in cui si desidera creare una nuova chiave di registro selezionando il Registry name (Nome del registro).
7. Scegli Crea, Crea chiave di registro.
8. Scegli il pulsante accanto alla voce di registro in cui si desidera creare una chiave nuova.
9. Scegli Create registry key (Crea chiave di registro).
10. Inserisci un valore per Name (Nome) della nuova chiave di registro e seleziona Submit (Invia).

Per creare una voce di registro di Windows con Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli il pulsante accanto all'istanza in cui si desidera creare una voce di registro.
4. Seleziona Visualizza dettagli.
5. Scegli Strumenti, Registro di Windows.
6. Scegli l'hive e la chiave di registro seguente in cui si desidera creare una nuova chiave di registro selezionando il Registry name (Nome del registro).
7. Scegli Crea, Crea voce di registro.
8. Inserisci un valore per Name (Nome) della nuova voce di registro.
9. Scegli Type (Tipo) di valore che si desidera creare per la voce di registro. Per ulteriori informazioni sui tipi di valore del registro, consulta [Registry value types \(Tipi di valori del registro\)](#).
10. Inserisci un valore per Value (Valore) della nuova voce di registro.

Aggiorna una voce di registro di Windows

Per aggiornare una voce del registro di Windows con Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli il pulsante accanto al nodo gestito in cui desideri aggiornare una voce di registro.
4. Seleziona Visualizza dettagli.
5. Scegli Strumenti, Registro di Windows.
6. Scegli l'hive e la chiave di registro seguente che si desidera aggiornare selezionando il Registry name (Nome del registro).
7. Scegli il pulsante accanto alla voce di registro che si desidera aggiornare.
8. Scegli Operazioni, Aggiorna voce di registro.
9. Inserisci un nuovo valore per Value (Valore) della voce di registro.
10. Scegliere Aggiorna.

Elimina una chiave o voce del registro di Windows

Per eliminare una chiave di registro di Windows con Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli il pulsante accanto al nodo gestito in cui desideri eliminare una chiave di registro.
4. Scegli Strumenti, Registro di Windows.
5. Scegli l'hive e la chiave di registro seguente che si desidera eliminare selezionando il Registry name (Nome del registro).
6. Scegli il pulsante accanto alla chiave di registro che si desidera eliminare.
7. Scegli Operazioni, Elimina chiave di registro.

Per eliminare una voce del registro di Windows con Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli il pulsante accanto al nodo gestito in cui desideri eliminare una voce di registro.
4. Seleziona Visualizza dettagli.
5. Scegli Strumenti, Registro di Windows.
6. Scegli l'hive e la chiave di registro seguente contenente la voce che si desidera eliminare selezionando il Registry name (Nome del registro).
7. Scegli il pulsante accanto alla voce di registro che si desidera eliminare.
8. Scegli Operazioni, Elimina voce di registro.

Gestione automatica delle istanze EC2 con la configurazione di gestione host predefinita

L'impostazione predefinita di configurazione di gestione degli host consente di AWS Systems Manager gestire automaticamente le istanze Amazon EC2 come istanze gestite. Un'istanza gestita è un'istanza EC2 configurata per l'uso con Systems Manager.

I vantaggi della gestione delle istanze con Systems Manager includono:

- Connettersi in modo sicuro alle istanze EC2 utilizzando Session Manager.
- Eseguire le scansioni automatiche delle patch utilizzando Patch Manager.
- Visualizzare informazioni dettagliate sulle istanze utilizzando Inventario di Systems Manager Inventory.
- Tieni traccia delle istanze e gestiscile utilizzando Fleet Manager.
- Mantenere SSM Agent aggiornato automaticamente.

Fleet Manager, Inventory, Patch Manager e Session Manager sono strumenti di Systems Manager.

Utilizzando la configurazione predefinita di gestione degli host, puoi gestire le istanze EC2 senza dover creare manualmente un profilo di istanza AWS Identity and Access Management (IAM). Invece, la configurazione predefinita di gestione dell'host crea e applica un ruolo IAM predefinito per

assicurarsi che Systems Manager disponga delle autorizzazioni per gestire tutte le istanze presenti Account AWS e in Regione AWS cui è attivato.

Se le autorizzazioni fornite non sono sufficienti per il tuo caso d'uso, è possibile anche aggiungere policy al ruolo IAM predefinito creato dalla configurazione di gestione host predefinita. In alternativa, se non hai bisogno di autorizzazioni per tutte le funzionalità fornite dal ruolo IAM predefinito, è possibile creare ruoli e policy personalizzati. Qualsiasi modifica apportata al ruolo IAM scelto per la configurazione di gestione host predefinita si applica a tutte le istanze Amazon EC2 gestite nella Regione e nell'account.

Per ulteriori informazioni sulla policy utilizzata dalla configurazione di gestione host predefinita, consulta la pagina [AWS politica gestita: AmazonSSMManagedEC2InstanceDefaultPolicy](#).

Implementazione dell'accesso con privilegi minimi

La procedura in questo argomento deve essere eseguita solo dagli amministratori. Pertanto, consigliamo di implementare l'accesso con i privilegi minimi per impedire agli utenti non amministrativi di configurare o modificare la configurazione predefinita di gestione degli host. Per visualizzare esempi di policy che limitano l'accesso alla funzionalità Configurazione di gestione host predefinita, consulta [Esempi di policy con privilegi minimi per la funzionalità Configurazione di gestione host predefinita](#) più avanti in questo argomento.

Important

Le informazioni di registrazione delle istanze registrate utilizzando la configurazione di gestione host predefinita sono archiviate localmente nelle directory `var/lib/amazon/ssm` o `C:\ProgramData\Amazon`. La rimozione di tali directory o dei relativi file impedirà all'istanza di acquisire le credenziali necessarie per connettersi a Systems Manager utilizzando la configurazione di gestione host predefinita. In questi casi, è necessario utilizzare un profilo dell'istanza IAM per fornire le autorizzazioni richieste all'istanza o ricreare l'istanza.

Prerequisiti

Per utilizzare la configurazione predefinita di gestione dell'host nel Regione AWS punto in Account AWS cui si attiva l'impostazione, è necessario soddisfare i seguenti requisiti.

- Un'istanza da gestire deve utilizzare Instance Metadata Service Versione 2 (IMDSv2).

La configurazione di gestione host predefinita non supporta Instance Metadata Service versione 1. Per ulteriori informazioni sul passaggio a IMDSv2, consulta la pagina [Passaggio all'utilizzo del servizio di metadati dell'istanza versione 2](#) nella Guida per l'utente di Amazon EC2

- Per poter essere gestito, SSM Agent versione 3.2.582.0 o successiva deve essere installato sull'istanza.

Per informazioni sulla verifica della versione di SSM Agent installata sull'istanza, consulta [Verifica del Agente SSM numero di versione](#).

Per informazioni sull'aggiornamento di SSM Agent, consulta [Aggiornamento automatico Agente SSM](#).

- L'utente, in qualità di amministratore che esegue le attività descritte in questo argomento, deve disporre delle autorizzazioni per le operazioni [GetServiceSetting](#), [ResetServiceSetting](#), e [UpdateServiceSetting](#) API. Inoltre, è necessario disporre delle autorizzazioni per l'autorizzazione `iam:PassRole` del ruolo IAM `AWSSystemsManagerDefaultEC2InstanceManagementRole`. Quello seguente è un esempio di policy che concede queste autorizzazioni. Sostituisci ogni *example resource placeholder* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetServiceSetting",
        "ssm:ResetServiceSetting",
        "ssm:UpdateServiceSetting"
      ],
      "Resource": "arn:aws:ssm:us-east-1:111122223333:servicesetting/ssm/managed-instance/default-ec2-instance-management-role"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::111122223333:role/service-role/AWSSystemsManagerDefaultEC2InstanceManagementRole",
```

```
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": [
          "ssm.amazonaws.com"
        ]
      }
    }
  }
}
```

- Se un profilo dell'istanza IAM è già collegato a un'istanza EC2 da gestire utilizzando Systems Manager, devi rimuoverne tutte le autorizzazioni che consentono l'operazione `ssm:UpdateInstanceInformation`. SSM Agent tenta di utilizzare le autorizzazioni del profilo dell'istanza prima di utilizzare le autorizzazioni della configurazione di gestione host predefinita. Se consenti l'operazione `ssm:UpdateInstanceInformation` nel profilo dell'istanza IAM, l'istanza non utilizzerà le autorizzazioni della configurazione di gestione host predefinita.

Attivazione dell'impostazione di Configurazione di gestione host predefinita

È possibile attivare la configurazione predefinita di gestione dell'host dalla Fleet Manager console o utilizzando il pulsante AWS Command Line Interface o AWS Tools for Windows PowerShell.

È necessario attivare l'impostazione di Configurazione di gestione host predefinita in ciascuna Regione nella quale si desidera che gestisca le istanze Amazon EC2.

Dopo aver attivato la Configurazione di gestione host predefinita, le istanze potrebbero impiegare fino a 30 minuti per utilizzare le credenziali del ruolo scelto nel Passaggio 5 della seguente procedura.

Per attivare la funzionalità Configurazione di gestione host predefinita (console)

1. Aprire la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli Gestione account, Configura la Configurazione di gestione host predefinita.
4. Attiva Abilita la configurazione di gestione host predefinita.
5. Scegli il ruolo AWS Identity and Access Management (IAM) utilizzato per abilitare gli strumenti di Systems Manager per le tue istanze. Ti consigliamo di utilizzare il ruolo predefinito fornito dalla configurazione di gestione host predefinita. Contiene il set minimo di autorizzazioni necessario

per gestire le istanze Amazon EC2 utilizzando Systems Manager. Se preferisci utilizzare un ruolo personalizzato, la policy di attendibilità del ruolo deve riconoscere Systems Manager come un'entità attendibile.

6. Scegli Configura per completare la configurazione.

Per attivare la funzionalità Configurazione di gestione host predefinita (riga di comando)

1. Crea un file JSON sul tuo computer locale contenente la seguente policy di attendibilità.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Apri AWS CLI o Tools for Windows PowerShell ed esegui uno dei seguenti comandi, a seconda del tipo di sistema operativo del tuo computer locale, per creare un ruolo di servizio nel tuo account. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux & macOS

```
aws iam create-role \
--role-name AWSSystemsManagerDefaultEC2InstanceManagementRole \
--path /service-role/ \
--assume-role-policy-document file://trust-policy.json
```

Windows

```
aws iam create-role ^
--role-name AWSSystemsManagerDefaultEC2InstanceManagementRole ^
```

```
--path /service-role/ ^
--assume-role-policy-document file://trust-policy.json
```

PowerShell

```
New-IAMRole `
-RoleName "AWSSystemsManagerDefaultEC2InstanceManagementRole" `
-Path "/service-role/" `
-AssumeRolePolicyDocument "file://trust-policy.json"
```

3. Esegui il comando seguente per collegare la policy gestita AmazonSSMManagedEC2InstanceDefaultPolicy al ruolo appena creato. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux & macOS

```
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy \
--role-name AWSSystemsManagerDefaultEC2InstanceManagementRole
```

Windows

```
aws iam attach-role-policy ^
--policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy ^
--role-name AWSSystemsManagerDefaultEC2InstanceManagementRole
```

PowerShell

```
Register-IAMRolePolicy `
-PolicyArn "arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy" `
-RoleName "AWSSystemsManagerDefaultEC2InstanceManagementRole"
```

4. Apri AWS CLI o Tools for Windows PowerShell ed esegui il comando seguente. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux & macOS

```
aws ssm update-service-setting \
--setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/
default-ec2-instance-management-role \
```

```
--setting-value service-role/AWSSystemsManagerDefaultEC2InstanceManagementRole
```

Windows

```
aws ssm update-service-setting ^  
--setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/  
default-ec2-instance-management-role ^  
--setting-value service-role/AWSSystemsManagerDefaultEC2InstanceManagementRole
```

PowerShell

```
Update-SSMServiceSetting `  
-SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/  
default-ec2-instance-management-role" `  
-SettingValue "service-role/AWSSystemsManagerDefaultEC2InstanceManagementRole"
```

Se il comando va a buon fine, non viene generato output.

5. Esegui il comando seguente per visualizzare le impostazioni correnti del servizio per la configurazione predefinita di gestione dell'host nell'attuale Account AWS e Regione AWS.

Linux & macOS

```
aws ssm get-service-setting \  
--setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/  
default-ec2-instance-management-role
```

Windows

```
aws ssm get-service-setting ^  
--setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/  
default-ec2-instance-management-role
```

PowerShell

```
Get-SSMServiceSetting `  
-SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/  
default-ec2-instance-management-role"
```

Il comando restituisce informazioni simili alle seguenti.

```
{
  "ServiceSetting": {
    "SettingId": "/ssm/managed-instance/default-ec2-instance-management-role",
    "SettingValue": "service-role/
AWSSystemsManagerDefaultEC2InstanceManagementRole",
    "LastModifiedDate": "2022-11-28T08:21:03.576000-08:00",
    "LastModifiedUser": "System",
    "ARN": "arn:aws:ssm:us-east-2:-123456789012:servicesetting/ssm/managed-
instance/default-ec2-instance-management-role",
    "Status": "Custom"
  }
}
```

Disattivazione dell'impostazione di Configurazione di gestione host predefinita

È possibile disattivare la configurazione predefinita di gestione dell'host dalla Fleet Manager console o utilizzando il pulsante AWS Command Line Interface o AWS Tools for Windows PowerShell.

Devi disattivare l'impostazione di Configurazione di gestione host predefinita in ciascuna Regione nella quale si desidera impedire che gestisca le istanze Amazon EC2. La disattivazione in una Regione non comporta la disattivazione in tutte le Regioni.

Se disattivi la funzionalità Configurazione di gestione host predefinita e non hai collegato un profilo dell'istanza alle istanze Amazon EC2 che consenta l'accesso a Systems Manager, queste non saranno più gestite da Systems Manager.

Per disattivare la funzionalità Configurazione di gestione host predefinita (console)

1. Aprire la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli Gestione account, Configurazione di gestione host predefinita.
4. Disattiva Abilita configurazione di gestione host predefinita.
5. Scegli Configura per disabilitare la configurazione di gestione host predefinita.

Per disattivare la funzionalità Configurazione di gestione host predefinita (riga di comando)

- Apri AWS CLI o Tools for Windows PowerShell ed esegui il seguente comando. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux & macOS

```
aws ssm reset-service-setting \  
--setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/  
default-ec2-instance-management-role
```

Windows

```
aws ssm reset-service-setting ^  
--setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/  
default-ec2-instance-management-role
```

PowerShell

```
Reset-SSMServiceSetting `  
-SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/  
default-ec2-instance-management-role"
```

Esempi di policy con privilegi minimi per la funzionalità Configurazione di gestione host predefinita

Le seguenti policy di esempio mostrano come impedire ai membri dell'organizzazione di apportare modifiche all'impostazione della funzionalità Configurazione di gestione host predefinita nell'account.

Politica di controllo del servizio per AWS Organizations

La seguente politica illustra come impedire ai membri non amministrativi dell'azienda di aggiornare l'impostazione predefinita della configurazione di gestione dell'host. AWS Organizations Sostituisci ogni *example resource placeholder* con le tue informazioni.

JSON

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



```

        "Action": [
            "ssm:UpdateServiceSetting",
            "ssm:ResetServiceSetting"
        ],
        "Resource": "arn:aws:ssm:*:*:servicesetting/ssm/managed-instance/
default-ec2-instance-management-role",
        "Condition": {
            "StringNotEqualsIgnoreCase": {
                "aws:PrincipalTag/job-function": [
                    "administrator"
                ]
            }
        }
    },
    {
        "Effect": "Deny",
        "Action": [
            "iam:PassRole"
        ],
        "Resource": "arn:aws:iam:*:*:role/service-role/
AWSSystemsManagerDefaultEC2InstanceManagementRole",
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": "ssm.amazonaws.com"
            },
            "StringNotEqualsIgnoreCase": {
                "aws:PrincipalTag/job-function": [
                    "administrator"
                ]
            }
        }
    },
    {
        "Effect": "Deny",
        "Resource": "arn:aws:iam:*:*:role/service-role/
AWSSystemsManagerDefaultEC2InstanceManagementRole",
        "Action": [
            "iam:AttachRolePolicy",
            "iam>DeleteRole"
        ],
        "Condition": {
            "StringNotEqualsIgnoreCase": {
                "aws:PrincipalTag/job-function": [
                    "administrator"
                ]
            }
        }
    }
]

```

```

    ]
  }
}
]
}

```

Policy per i principali IAM

La seguente politica dimostra come impedire ai gruppi, ai ruoli o agli utenti IAM dell'azienda di aggiornare l'impostazione predefinita AWS Organizations della configurazione di gestione dell'host. Sostituisci ogni *example resource placeholder* con le tue informazioni.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ssm:UpdateServiceSetting",
        "ssm:ResetServiceSetting"
      ],
      "Resource": "arn:aws:ssm:us-east-1:111122223333:servicesetting/ssm/managed-instance/default-ec2-instance-management-role"
    },
    {
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam>DeleteRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::111122223333:role/service-role/AWSSystemsManagerDefaultEC2InstanceManagementRole"
    }
  ]
}

```

Connessione a un Windows Server istanza gestita utilizzando Remote Desktop (Desktop remoto)

Puoi utilizzarlo Fleet Manager per connetterti alle tue istanze Windows Server Amazon Elastic Compute Cloud (Amazon EC2) utilizzando (RDP). Remote Desktop Protocol Fleet Manager Remote Desktop, basato [su Amazon DCV](#), offre una connettività sicura alle Windows Server istanze direttamente dalla console di Systems Manager. È possibile avere fino a quattro connessioni simultanee in un'unica finestra del browser.

L'API Fleet Manager Remote Desktop è denominata AWS Systems Manager GUI Connect Per informazioni sull'utilizzo dell'API Systems Manager GUI Connect, consulta il [Documento di riferimento dell'API AWS Systems Manager GUI Connect](#).

Attualmente, è possibile utilizzare Desktop remoto solo con istanze che eseguono Windows Server 2012 RTM o versioni successive. Desktop remoto supporta solo input in lingua inglese.

Fleet Manager Remote Desktop è un servizio solo per console e non supporta connessioni da riga di comando alle istanze gestite. Per connettersi a un'istanza gestita Windows Server tramite una shell, è possibile utilizzare Session Manager, un altro strumento di AWS Systems Manager. Per ulteriori informazioni, consulta [AWS Systems Manager Session Manager](#).

Note

La durata di una connessione RDP non è determinata dalla durata delle credenziali AWS Identity and Access Management (IAM) dell'utente. Al contrario, la connessione persiste invece fino al raggiungimento della sua durata massima o del limite di inattività, a seconda dell'evento che si verifica per primo. Per ulteriori informazioni, consulta [Durata e simultaneità della connessione remota](#).

Per informazioni sulla configurazione delle autorizzazioni AWS Identity and Access Management (IAM) per consentire alle istanze di interagire con Systems Manager, consulta [Configurare le autorizzazioni delle istanze per Systems Manager](#).

Configurazione dell'ambiente

Prima di utilizzare Desktop remoto, verifica che il tuo ambiente soddisfi i requisiti seguenti:

- Configurazione di nodi gestiti

Assicurati che le istanze Amazon EC2 siano configurate come [nodi gestiti](#) in Systems Manager.

- Versione minima di SSM Agent

Verifica che i nodi eseguano SSM Agent versione 3.0.222.0 o successiva. Per informazioni su come verificare la versione dell'agente in esecuzione su un nodo, consulta [Verifica del Agente SSM numero di versione](#). Per informazioni sull'installazione o l'aggiornamento di SSM Agent, consulta [Lavorare con Agente SSM](#).

- Configurazione della porta RDP

Per accettare connessioni remote, il servizio Remote Desktop Services sui nodi Windows Server deve utilizzare la porta RDP 3389 predefinita. Questa è la configurazione predefinita su Amazon Machine Images () AMIs fornita da. AWS Non è richiesto esplicitamente di aprire alcuna porta in entrata per utilizzare Desktop remoto.

- Versione del modulo PSReadLine per la funzionalità della tastiera

Per assicurarti che la tastiera funzioni correttamente in PowerShell, verifica che nei nodi che eseguono Windows Server 2022 sia installata la versione del PSReadLine modulo 2.2.2 o successiva. Se i nodi utilizzano una versione precedente, è possibile installare la versione richiesta utilizzando i seguenti comandi.

```
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
```

Dopo aver installato il provider NuGet del pacchetto, esegui il comando seguente.

```
Install-Module `
  -Name PSReadLine `
  -Repository PSGallery `
  -MinimumVersion 2.2.2 -Force
```

- Configurazione di Session Manager

Prima di utilizzare Desktop remoto, è necessario completare i prerequisiti per l'installazione di Session Manager. Quando ti connetti a un'istanza tramite Remote Desktop, Regione AWS vengono applicate tutte le preferenze di sessione definite per il tuo Account AWS e. Per ulteriori informazioni, consulta [Configurazione di Session Manager](#).

 Note

Se registri l'attività di Session Manager utilizzando Amazon Simple Storage Service (Amazon S3), le connessioni Desktop remoto genereranno l'errore seguente in `bucket_name/Port/stderr`. Questo errore è previsto e può essere ignorato.

```
Setting up data channel with id SESSION_ID failed: failed to create websocket
for datachannel with error: CreateDataChannel failed with no output or
error: createDataChannel request failed: unexpected response from the service
<BadRequest>
<ClientErrorMessage>Session is already terminated</ClientErrorMessage>
</BadRequest>
```

Configurazione delle autorizzazioni IAM per Desktop remoto

Oltre alle autorizzazioni IAM richieste per Systems Manager e Session Manager, all'utente o al ruolo utilizzato devono essere consentite le autorizzazioni per l'avvio delle connessioni.

Autorizzazioni per l'avvio delle connessioni

Per effettuare connessioni RDP alle istanze EC2 nella console, sono necessarie le seguenti autorizzazioni:

- `ssm-guiconnect:CancelConnection`
- `ssm-guiconnect:GetConnection`
- `ssm-guiconnect:StartConnection`

Autorizzazioni per elencare le connessioni

Per visualizzare gli elenchi di connessioni nella console, è richiesta la seguente autorizzazione:

`ssm-guiconnect:ListConnections`

Di seguito sono riportati alcuni esempi di policy IAM che è possibile collegare a un utente o a un ruolo per consentire diversi tipi di interazione con Desktop remoto. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Policy standard per la connessione alle istanze EC2

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EC2",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:GetPasswordData"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSM",
      "Effect": "Allow",
      "Action": [
        "ssm:DescribeInstanceProperties",
        "ssm:GetCommandInvocation",
        "ssm:GetInventorySchema"
      ],
      "Resource": "*"
    },
    {
      "Sid": "TerminateSession",
      "Effect": "Allow",
      "Action": [
        "ssm:TerminateSession"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ssm:resourceTag/aws:ssmmessages:session-id": [
            "${aws:userid}"
          ]
        }
      }
    },
    {
      "Sid": "SSMStartSession",
```

```

    "Effect": "Allow",
    "Action": [
        "ssm:StartSession"
    ],
    "Resource": [
        "arn:aws:ec2:*:111122223333:instance/*",
        "arn:aws:ssm:*:111122223333:managed-instance/*",
        "arn:aws:ssm:*::document/AWS-StartPortForwardingSession"
    ],
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "ssm-guiconnect.amazonaws.com"
        }
    }
},
{
    "Sid": "SSMMessages",
    "Effect": "Allow",
    "Action": [
        "ssmmessages:OpenDataChannel"
    ],
    "Resource": [
        "arn:aws:ssm:*:111122223333:session/*"
    ],
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "ssm-guiconnect.amazonaws.com"
        }
    }
},
{
    "Sid": "GuiConnect",
    "Effect": "Allow",
    "Action": [
        "ssm-guiconnect:CancelConnection",
        "ssm-guiconnect:GetConnection",
        "ssm-guiconnect:StartConnection",
        "ssm-guiconnect:ListConnections"
    ],
    "Resource": "*"
}
]
}

```

Policy per la connessione a istanze EC2 con tag specifici

Note

Nella seguente policy IAM, la sezione `SSMStartSession` richiede un nome della risorsa Amazon (ARN) per l'azione `ssm:StartSession`. Come mostrato, l'ARN specificato non richiede un Account AWS ID. Se si specifica un ID account, Fleet Manager restituisce `AccessDeniedException`.

La sezione `AccessTaggedInstances`, che si trova nella parte inferiore della policy di esempio, richiede ARN anche per `ssm:StartSession`. Per questi ARN, è necessario specificare gli ID Account AWS.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EC2",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:GetPasswordData"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSM",
      "Effect": "Allow",
      "Action": [
        "ssm:DescribeInstanceProperties",
        "ssm:GetCommandInvocation",
        "ssm:GetInventorySchema"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSMStartSession",
      "Effect": "Allow",
      "Action": [
```



```

        "ssm:StartSession"
    ],
    "Resource": [
        "arn:aws:ssm:*::document/AWS-StartPortForwardingSession"
    ],
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "ssm-guiconnect.amazonaws.com"
        }
    }
},
{
    "Sid": "AccessTaggedInstances",
    "Effect": "Allow",
    "Action": [
        "ssm:StartSession"
    ],
    "Resource": [
        "arn:aws:ec2:*:111122223333:instance/*",
        "arn:aws:ssm:*:111122223333:managed-instance/*"
    ],
    "Condition": {
        "StringLike": {
            "ssm:resourceTag/tag key": [
                "tag value"
            ]
        }
    }
},
{
    "Sid": "SSMMessages",
    "Effect": "Allow",
    "Action": [
        "ssmmessages:OpenDataChannel"
    ],
    "Resource": [
        "arn:aws:ssm:*:111122223333:session/*"
    ],
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "ssm-guiconnect.amazonaws.com"
        }
    }
},

```

```

    {
      "Sid": "GuiConnect",
      "Effect": "Allow",
      "Action": [
        "ssm-guiconnect:CancelConnection",
        "ssm-guiconnect:GetConnection",
        "ssm-guiconnect:StartConnection",
        "ssm-guiconnect:ListConnections"
      ],
      "Resource": "*"
    }
  ]
}

```

Politica per Centro identità AWS IAM utenti per connettersi alle istanze EC2

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSO",
      "Effect": "Allow",
      "Action": [
        "sso:ListDirectoryAssociations*",
        "identitystore:DescribeUser"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EC2",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:GetPasswordData"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSM",
      "Effect": "Allow",

```

```

        "Action": [
            "ssm:DescribeInstanceProperties",
            "ssm:GetCommandInvocation",
            "ssm:GetInventorySchema"
        ],
        "Resource": "*"
    },
    {
        "Sid": "TerminateSession",
        "Effect": "Allow",
        "Action": [
            "ssm:TerminateSession"
        ],
        "Resource": "*",
        "Condition": {
            "StringLike": {
                "ssm:resourceTag/aws:ssmmessages:session-id": [
                    "${aws:userName}"
                ]
            }
        }
    },
    {
        "Sid": "SSMStartSession",
        "Effect": "Allow",
        "Action": [
            "ssm:StartSession"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:instance/*",
            "arn:aws:ssm:*:*:managed-instance/*",
            "arn:aws:ssm:*:*:document/AWS-StartPortForwardingSession"
        ],
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:CalledVia": "ssm-guiconnect.amazonaws.com"
            }
        }
    },
    {
        "Sid": "SSMSendCommand",
        "Effect": "Allow",
        "Action": [
            "ssm:SendCommand"
        ],

```

```

    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWSSSO-CreateSSOUser"
    ]
},
{
    "Sid": "SSMMessages",
    "Effect": "Allow",
    "Action": [
        "ssmmessages:OpenDataChannel"
    ],
    "Resource": [
        "arn:aws:ssm:*:111122223333:session/*"
    ],
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "ssm-guiconnect.amazonaws.com"
        }
    }
},
{
    "Sid": "GuiConnect",
    "Effect": "Allow",
    "Action": [
        "ssm-guiconnect:CancelConnection",
        "ssm-guiconnect:GetConnection",
        "ssm-guiconnect:StartConnection",
        "ssm-guiconnect:ListConnections"
    ],
    "Resource": "*"
}
]
}

```

Autenticazione delle connessioni Desktop remoto

Quando stabilisci una connessione remota, puoi autenticarti utilizzando le credenziali Windows o la coppia di chiavi Amazon EC2 (file .pem) associata all'istanza. Per informazioni sull'uso delle coppie di chiavi, consulta [Coppie di chiavi Amazon EC2 e istanze Windows](#) nella Guida per l'utente di Amazon EC2.

In alternativa, se sei autenticato all' Console di gestione AWS uso Centro identità AWS IAM, puoi connetterti alle tue istanze senza fornire credenziali aggiuntive. Per un esempio di policy per consentire l'autenticazione della connessione remota utilizzando Centro identità IAM, consulta [Configurazione delle autorizzazioni IAM per Desktop remoto](#).

Le connessioni Desktop remoto che utilizzano l'autenticazione IAM Identity Center sono disponibili Regioni AWS ovunque sia supportato IAM Identity Center.

Prima di iniziare

Osserva le seguenti condizioni per l'uso dell'autenticazione di Centro identità IAM prima di avviare la connessione utilizzando Desktop remoto.

- Desktop remoto supporta l'autenticazione di Centro identità IAM per i nodi nella stessa Regione AWS in cui hai abilitato Centro identità IAM.
- Desktop remoto supporta nomi utente di IAM Identity Center composti da un massimo di 16 caratteri.
- Desktop remoto supporta nomi utente di IAM Identity Center composti da caratteri alfanumerici e dai seguenti caratteri speciali: . - _

Important

Le connessioni non avranno esito positivo per i nomi utente di IAM Identity Center che contengono i seguenti caratteri: + = ,
IAM Identity Center supporta questi caratteri nei nomi utente, a differenza delle connessioni Fleet Manager RDP.

Inoltre, se il nome utente di IAM Identity Center contiene uno o più @ simboli, Fleet Manager ignora il primo @ simbolo e tutti i caratteri che lo seguono, indipendentemente dal fatto che @ introduca la parte di dominio di un indirizzo email. Ad esempio, per il nome utente IAM Identity Center `diego_ramirez@example.com`, la parte `@example.com` viene ignorata e il nome utente di Fleet Manager diventa `diego_ramirez`. Per `diego_r@mirez@example.com`, Fleet Manager ignora `@mirez@example.com` e il nome utente di Fleet Manager diventa `diego_r`.

- Quando una connessione viene autenticata utilizzando IAM Identity Center, Remote Desktop crea un utente Windows locale nel gruppo Local Administrators dell'istanza. Questo utente persiste dopo la fine della connessione remota.

- Desktop remoto non consente l'autenticazione IAM Identity Center per i nodi che sono controller del dominio Microsoft Active Directory.
- Sebbene Remote Desktop consenta di utilizzare l'autenticazione IAM Identity Center per i nodi uniti a un Active Directory dominio, non è consigliabile farlo. Questo metodo di autenticazione concede autorizzazioni amministrative agli utenti che potrebbero sovrascrivere le autorizzazioni più restrittive concesse dal dominio.

Durata e simultaneità della connessione remota

Le seguenti condizioni si applicano alle connessioni Desktop remoto attive:

- Durata della connessione

Per impostazione predefinita, una connessione Desktop remoto viene interrotta dopo 60 minuti. Per evitare che una connessione venga interrotta, puoi scegliere **Rinnova sessione** prima di disconnetterti per reimpostare il timer di durata.

- Timeout di connessione

Una connessione Desktop remoto si interrompe dopo essere rimasta inattiva per più di 10 minuti.

- Connessioni persistenti

Dopo la connessione a Windows Server tramite Desktop remoto, la connessione persiste fino al raggiungimento della sua massima durata (60 minuti) o del limite di timeout di inattività (10 minuti). La durata della connessione non è determinata dalla durata delle tue credenziali AWS Identity and Access Management (IAM). La connessione persiste dopo la scadenza delle credenziali IAM, se i suoi limiti di durata non vengono soddisfatti. Quando si utilizza Desktop remoto, è necessario terminare la connessione dopo la scadenza delle credenziali IAM uscendo dalla pagina del browser.

- Connessioni simultanee

Per impostazione predefinita, è possibile avere un massimo di 5 connessioni Remote Desktop attive contemporaneamente per la stessa Account AWS e Regione AWS. Per richiedere un aumento di quote di servizio fino a 50 connessioni simultanee, consulta [Richiesta di aumento delle quote](#) nella Guida per l'utente di Service Quotas.

 Note

La licenza standard di Windows Server consente due connessioni RDP simultanee. Per supportare più connessioni, è necessario acquistare licenze di Accesso Client (CAL) aggiuntive da Microsoft o licenze di Servizi Desktop remoto Microsoft da AWS. Per ulteriori informazioni sulle licenze aggiuntive, consulta i seguenti argomenti:

- [Licenze di Accesso Client e licenze di gestione](#) sul sito Web di Microsoft
- [Utilizza gli abbonamenti basati sull'utente di License Manager per i prodotti software supportati](#) nella Guida per l'utente di License Manager

Gestione di Systems Manager GUI Connect Centro identità AWS IAM attributes

Systems Manager GUI Connect è l'API che supporta le connessioni Fleet Manager nelle istanze EC2 tramite RDP. I seguenti dati utente di IAM Identity Center vengono conservati dopo la chiusura di una connessione:

- `username`

Systems Manager GUI Connect crittografa questo attributo di identità inattivo utilizzando per impostazione predefinita un Chiave gestita da AWS. Le chiavi gestite dal cliente non sono supportate per la crittografia di questo attributo in Systems Manager GUI Connect. Se elimini un utente nella tua istanza IAM Identity Center, Systems Manager GUI Connect continua a mantenere l'attributo `username` associato a quell'utente per sette anni, dopodiché viene eliminato. Questi dati vengono conservati per supportare gli eventi di controllo, ad esempio elencare la cronologia delle connessioni di Systems Manager GUI Connect. I dati non possono essere eliminati manualmente.

Connessione a un nodo gestito tramite Desktop remoto

copy/paste Supporto del browser per il testo

Utilizzando i browser Google Chrome e Microsoft Edge, è possibile copiare e incollare testo da un nodo gestito al computer locale e dal computer locale a un nodo gestito a cui hai effettuato la connessione.

Utilizzando il browser Mozilla Firefox, è possibile copiare e incollare il testo da un nodo gestito solo sul proprio computer locale. La copia dal computer locale al nodo gestito non è supportata.

Per connettersi a un nodo gestito utilizzando Fleet Manager Remote Desktop (Desktop remoto)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli il nodo a cui desideri connetterti. Puoi selezionare la casella di controllo o il nome del nodo.
4. Nel menu Operazioni del nodo, scegli Connessione con Desktop remoto.
5. Scegli il tuo Tipo di autenticazione preferito. Se scegli Credenziali utente, inserisci il nome utente e la password per un account utente Windows sul nodo a cui stai eseguendo la connessione. Se scegli Coppia di chiavi, puoi fornire l'autenticazione utilizzando uno dei seguenti metodi:
 - a. Scegli Sfoglia la macchina locale se desideri selezionare la chiave PEM associata all'istanza dal file system locale.

oppure
 - b. Scegli Incolla contenuto della coppia di chiavi se desideri copiare il contenuto del file PEM e incollarlo nel campo fornito.
6. Seleziona Connetti.
7. Per scegliere la risoluzione dello schermo preferita, nel menu Operazioni, scegli Risoluzioni, quindi seleziona una delle seguenti opzioni:
 - Adatta automaticamente
 - 1920 x 1080
 - 1400 x 900
 - 1366 x 768
 - 800 x 600

L'opzione Adatta automaticamente imposta la risoluzione in base alle dimensioni dello schermo rilevate.

Visualizzazione delle informazioni sulle connessioni correnti e completate

Utilizza la sezione Fleet Manager della console Systems Manager per visualizzare le informazioni sulle connessioni RDP effettuate nel proprio account. Utilizzando un set di filtri, è possibile limitare

l'elenco delle connessioni visualizzate a un intervallo di tempo, un'istanza specifica, l'utente che ha effettuato le connessioni e le connessioni con uno stato specifico. La console fornisce anche schede che mostrano informazioni su tutte le connessioni attualmente attive e tutte le connessioni passate.

Per visualizzare le informazioni sulle connessioni correnti e completate

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli Gestione account, Connessione con Remote Desktop (Desktop remoto).
4. Scegli una delle seguenti schede:
 - Connessioni attive
 - Cronologia delle connessioni
5. Per restringere ulteriormente l'elenco dei risultati di connessione visualizzati, specificate uno o più filtri nella casella di ricerca



È anche possibile inserire un termine di ricerca a testo libero.

).

Gestione dei volumi Amazon EBS all'interno di un'istanza gestita

[Amazon Elastic Block Store \(Amazon EBS\)](#) fornisce volumi di archiviazione a blocchi da utilizzare con le istanze Amazon Elastic Compute Cloud (EC2). Il comportamento dei volumi EBS è simile a quello dei dispositivi a blocchi non formattati e non elaborati. Puoi montare questi volumi come dispositivi sulle istanze.

Puoi utilizzarlo Fleet Manager per gestire i volumi Amazon EBS sulle tue istanze gestite. Ad esempio, puoi inizializzare un volume EBS, formattare una partizione e montare il volume per renderlo disponibile all'uso.

Note

Fleet Manager attualmente supporta la gestione dei volumi di Amazon EBS solo per le istanze Windows Server.

Visualizzazione dei dettagli di un volume EBS

Per visualizzare i dettagli di un volume EBS con Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli il pulsante accanto all'istanza gestita di cui desideri visualizzare i dettagli dei volumi EBS.
4. Seleziona Visualizza dettagli.
5. Scegli Strumenti, Volumi EBS.
6. Per visualizzare i dettagli di un volume EBS, scegli il rispettivo ID nella colonna ID volume.

Inizializzazione e formattazione di un volume EBS

Per inizializzare e formattare un volume EBS con Fleet Manager

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Scegli il pulsante accanto all'istanza gestita per la quale desideri inizializzare, formattare e montare un volume EBS. Puoi inizializzare un volume EBS solo se il suo disco è vuoto.
4. Seleziona Visualizza dettagli.
5. Nel menu Strumenti, scegli Volumi EBS.
6. Scegli il pulsante accanto al volume EBS che desideri inizializzare e formattare.
7. Scegli Inizializzazione e formattazione.
8. In Stile di partizione, scegli lo stile di partizione che desideri utilizzare per il volume EBS.
9. (Facoltativo) Scegli una Lettera di unità per la partizione.
10. (Facoltativo) Immetti un Nome della partizione per identificare la partizione.
11. Scegli il File system da utilizzare per organizzare i file e i dati memorizzati nella partizione.
12. Scegli Conferma per rendere il volume EBS disponibile per l'uso. Non è possibile modificare la configurazione della partizione Console di gestione AWS dopo la conferma, tuttavia, è possibile utilizzare SSH o RDP per accedere all'istanza per modificare la configurazione della partizione.

Accesso al portale Red Hat Knowledge base

Puoi utilizzarlo Fleet Manager per accedere al portale della Knowledge base se sei un cliente Red Hat. Sei considerato un cliente Red Hat se esegui istanze Red Hat Enterprise Linux (RHEL) o utilizzi servizi RHEL su AWS. Il portale della Knowledge base include binari e forum di condivisione di conoscenze e discussioni per il supporto della community disponibili solo per i clienti con licenza Red Hat.

Oltre alle autorizzazioni AWS Identity and Access Management (IAM) richieste per Systems Manager Fleet Manager, l'utente o il ruolo utilizzato per accedere alla console deve consentire all'`rhelkb:GetRhelURL` azione di accedere al portale della Knowledge base.

Per accedere al portale Red Hat Knowledgebase

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Seleziona l'istanza RHEL che desideri utilizzare per connetterti al Red Hat Knowledgebase Portal.
4. Scegli Gestione account, Accedi a Red Hat Knowledgebase per aprire la pagina Red Hat Knowledge base.

Se utilizzi RHEL on AWS per eseguire RHEL carichi di lavoro completamente supportati, puoi anche accedere alla Red Hat Knowledge base tramite il sito Web di Red Hat utilizzando AWS le tue credenziali.

Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti

Per diversi AWS Systems Manager strumenti come Run Command Distributor, eSession Manager, puoi scegliere di selezionare manualmente i nodi gestiti su cui desideri eseguire un'operazione. In casi come questi, dopo avere specificato che si desidera scegliere manualmente i nodi, viene visualizzato un elenco dei nodi gestiti. su cui puoi decidere di eseguire l'operazione.

Questo argomento fornisce informazioni per aiutarti nell'esecuzione della diagnosi del motivo per cui un nodo gestito che hai confermato come in esecuzione non è incluso negli elenchi dei nodi gestiti in Systems Manager.

Affinché un nodo possa essere gestito da Systems Manager e disponibile negli elenchi di nodi gestiti, deve soddisfare tre requisiti:

- SSM Agent deve essere installato e in esecuzione su un nodo con un sistema operativo supportato.

Note

Alcuni AWS managed Amazon Machine Images (AMIs) sono configurati per avviare istanze [SSM Agent](#) preinstallate. (È possibile configurare anche una AMI per preinstallare SSM Agent.) Per ulteriori informazioni, consulta [Trova AMI con il Agente SSM preinstallato](#).

- Per le istanze Amazon Elastic Compute Cloud (Amazon EC2), è necessario allegare un profilo di istanza AWS Identity and Access Management (IAM) all'istanza. Il profilo dell'istanza consente all'istanza di comunicare con il servizio Systems Manager. Se non si assegna un profilo dell'istanza all'istanza, è possibile registrarlo utilizzando un'[attivazione ibrida](#), che non è uno scenario comune.
- SSM Agent deve essere in grado di connettersi a un endpoint di Systems Manager per registrarsi con il servizio. Successivamente, il nodo gestito deve essere disponibile per il servizio, il che viene confermato da parte del servizio attraverso l'invio di un segnale ogni cinque minuti per controllare l'integrità dell'istanza.
- Se lo stato di un nodo gestito è rimasto `Connection Lost` per almeno 30 giorni, il nodo potrebbe non essere più elencato nella console Fleet Manager. Per inserirlo nuovamente nell'elenco, è necessario risolvere il problema che ha causato la perdita della connessione.

Dopo aver verificato che un nodo gestito sia in esecuzione, puoi utilizzare il comando seguente per verificare se SSM Agent si è registrato correttamente con il servizio Systems Manager. Questo comando non restituisce risultati fino a quando la registrazione non è correttamente avvenuta.

Linux & macOS

```
aws ssm describe-instance-associations-status \  
  --instance-id instance-id
```

Windows

```
aws ssm describe-instance-associations-status ^  
  --instance-id instance-id
```

PowerShell

```
Get-SSMInstanceAssociationsStatus `
```

```
-InstanceId instance-id
```

Se la registrazione ha avuto esito positivo e il nodo gestito è ora disponibile per le operazioni di Systems Manager, il comando restituisce risultati simili ai seguenti.

```
{
  "InstanceAssociationStatusInfos": [
    {
      "AssociationId": "fa262de1-6150-4a90-8f53-d7eb5EXAMPLE",
      "Name": "AWS-GatherSoftwareInventory",
      "DocumentVersion": "1",
      "AssociationVersion": "1",
      "InstanceId": "i-02573cafcdEXAMPLE",
      "Status": "Pending",
      "DetailedStatus": "Associated"
    },
    {
      "AssociationId": "f9ec7a0f-6104-4273-8975-82e34EXAMPLE",
      "Name": "AWS-RunPatchBaseline",
      "DocumentVersion": "1",
      "AssociationVersion": "1",
      "InstanceId": "i-02573cafcdEXAMPLE",
      "Status": "Queued",
      "AssociationName": "SystemAssociationForScanningPatches"
    }
  ]
}
```

Se la registrazione non è ancora completata o non ha avuto esito positivo, il comando restituisce risultati simili al seguente:

```
{
  "InstanceAssociationStatusInfos": []
}
```

Se il comando non restituisce risultati dopo circa 5 minuti, utilizzare le informazioni seguenti per risolvere i problemi relativi ai nodi gestiti.

Soluzione 1: verifica che Agente SSM è installato e in esecuzione sul nodo gestito

Verifica che sul nodo gestito sia installata e in esecuzione la versione più recente di SSM Agent.

Per determinare se SSM Agent è installato e in esecuzione su un nodo gestito, consulta [Verifica Agente SSM stato e avvio dell'agente](#).

Per installare o reinstallare SSM Agent su un nodo gestito, consulta i seguenti argomenti:

- [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#)
- [Come installare SSM Agent su nodi Linux ibridi](#)
- [Installazione e disinstallazione manuali Agente SSM su istanze EC2 per Windows Server](#)
- [Come installare SSM Agent su nodi Windows ibridi](#)

Soluzione 2: verificare che sia stato specificato un profilo dell'istanza IAM per l'istanza (solo per istanze EC2)

Per le istanze Amazon Elastic Compute Cloud (Amazon EC2), verifica che l'istanza sia configurata con un profilo dell'istanza AWS Identity and Access Management (IAM) che consente all'istanza di comunicare con l'API di Systems Manager. Inoltre, verifica che l'utente disponga di una policy di attendibilità IAM che gli consenta di comunicare con l'API di Systems Manager.

Note

On-premises server, dispositivi edge e macchine virtuali (VM) utilizzano un ruolo di servizio IAM anziché un profilo di istanza. Per ulteriori informazioni, consulta [Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud](#).

Per determinare se un profilo dell'istanza con le autorizzazioni necessarie è collegato a un'istanza EC2

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 in cui verificare la presenza di un profilo dell'istanza.
4. Sulla scheda Descrizione nel riquadro inferiore, individua Ruolo IAM e scegli il nome del ruolo.
5. Nella pagina di riepilogo del ruolo per il profilo dell'istanza, nella scheda Autorizzazioni, assicurati che AmazonSSMManagedInstanceCore sia elencato in Politiche di autorizzazione.

Se invece viene utilizzata una policy personalizzata, assicurati che fornisca le stesse autorizzazioni di AmazonSSMManagedInstanceCore

[Apri AmazonSSMManagedInstanceCore nella console](#)

Per informazioni su ulteriori policy che possono essere allegate a un profilo dell'istanza per Systems Manager, consulta la pagina [Creazione di un profilo dell'istanza IAM richiesto per Systems Manager](#).

Soluzione 3: verifica della connettività degli endpoint del servizio

Verifica che l'istanza disponga della connettività agli endpoint del servizio Systems Manager. Questa connettività viene fornita creando e configurando endpoint VPC per Systems Manager o consentendo il traffico in uscita HTTPS (porta 443) agli endpoint di servizio.

Per le istanze Amazon EC2, l'endpoint del servizio Systems Manager per Regione AWS viene utilizzato per registrare l'istanza se la configurazione del cloud privato virtuale (VPC) consente il traffico in uscita. Tuttavia, se la configurazione VPC in cui è stata avviata l'istanza non permette il traffico in uscita e non è possibile modificarla per consentire la connettività agli endpoint di servizio pubblici, è necessario configurare invece gli endpoint di interfaccia per il VPC.

Per ulteriori informazioni, consulta [Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager](#).

Soluzione 4: verifica del supporto del sistema operativo di destinazione

Verifica che l'operazione scelta possa essere eseguita sul tipo di nodo gestito che si prevede di visualizzare in elenco. Alcune operazioni di Systems Manager possono essere indirizzate solo alle istanze di Windows o solo alle istanze di Linux. Ad esempio, i documenti Systems Manager (SSM) `AWS-InstallPowerShellModule` e `AWS-ConfigureCloudWatch` possono essere eseguiti solo su istanze di Windows. Nella pagina [Esegui un comando](#), se scegli uno di questi documenti e selezioni [Scegli le istanze manualmente](#), vengono elencate e rese disponibili per la selezione solo le istanze di Windows.

Soluzione 5: verifica di lavorare nella stessa Regione AWS come istanza Amazon EC2

Le istanze Amazon EC2 sono create e disponibili in aree specifiche Regioni AWS, ad esempio nella regione Stati Uniti orientali (Ohio) (us-east-2) o nella regione Europa (Irlanda) (eu-west-1). Assicurati di lavorare nella stessa Regione AWS istanza Amazon EC2 con cui desideri lavorare. Per ulteriori informazioni, consulta [Scelta di una Regione](#) in Nozioni di base su Console di gestione AWS.

Soluzione 6: verifica la configurazione del proxy a cui ti sei applicato Agente SSM sul tuo nodo gestito

Verifica che la configurazione proxy applicata a SSM Agent sul tuo nodo gestito sia corretta. Se la configurazione del proxy non è corretta, il nodo non può connettersi agli endpoint di servizio richiesti oppure Systems Manager potrebbe identificare in modo errato il sistema operativo del nodo gestito. Per ulteriori informazioni, consulta [Configurazione Agente SSM usare un proxy su nodi Linux](#) e [Configurazione di SSM Agent per utilizzare un proxy per le istanze Windows Server](#).

Soluzione 7: installazione di un certificato TLS sulle istanze gestite

Un certificato Transport Layer Security (TLS) deve essere installato su ogni istanza gestita con AWS Systems Manager cui si utilizza. Servizi AWS usa questi certificati per crittografare le chiamate ad altri. Servizi AWS

Un certificato TLS è già installato per impostazione predefinita su ogni istanza Amazon EC2 creata da qualsiasi Amazon Machine Image (AMI). La maggior parte dei sistemi operativi moderni include il certificato TLS richiesto dalle autorità di certificazione Amazon Trust Services nel proprio archivio fiduciario.

Per verificare se il certificato richiesto è installato sull'istanza, esegui il seguente comando in base al sistema operativo dell'istanza. Assicurati di sostituire la *region* parte dell'URL con quella Regione AWS in cui si trova l'istanza gestita.

Linux & macOS

```
curl -L https://ssm.region.amazonaws.com
```

Windows

```
Invoke-WebRequest -Uri https://ssm.region.amazonaws.com
```

Il comando dovrebbe restituire un errore `UnknownOperationException`. Se invece ricevi un messaggio SSL/TLS di errore, il certificato richiesto potrebbe non essere installato.

Se trovi che i certificati CA di Amazon Trust Services richiesti non sono installati sui tuoi sistemi operativi di base, su istanze create da AMIs quelle istanze non fornite da Amazon o sui tuoi server e macchine virtuali locali, devi installare e consentire un certificato di [Amazon Trust Services](#) o utilizzare AWS Certificate Manager (ACM) per creare e gestire certificati per un servizio integrato supportato.

In ciascuna delle istanze gestite deve essere installato uno dei seguenti certificati Transport Layer Security (TLS).

- Amazon CA root 1
- Autorità di certificazione root dei servizi Starfield - G2
- Autorità di certificazione Starfield di livello 2

Per ulteriori informazioni su ACM, consulta la Guida per l'utente di [AWS Certificate Manager](#).

Se i certificati nel tuo ambiente di elaborazione sono gestiti da un Group Policy Object (GPO), potresti dover configurare le policy di gruppo affinché includano uno di tali certificati.

Per ulteriori informazioni sui certificati Amazon Root e Starfield, consulta il post del blog [How to Prepare for AWS's Move to Its Own Certificate Authority](#).

Soluzione 8: verifica delle impostazioni predefinite di Host Management Configuration (DHMC)

La configurazione predefinita di gestione degli host (DHMC) consente a Systems Manager di gestire automaticamente le istanze Amazon EC2 senza richiedere un profilo di istanza su ciascuna istanza. Verifica che DHMC sia abilitato nel tuo account e nella tua regione e che il ruolo IAM associato disponga delle autorizzazioni e della politica di fiducia richieste.

Per risolvere i problemi DHMC-related :

1. Verifica che DHMC sia abilitato nel tuo account e nella tua regione. Per ulteriori informazioni, consulta [Gestione automatica delle istanze EC2 con la configurazione di gestione host predefinita](#).
2. Se DHMC è abilitato, verifica che il ruolo IAM associato includa la policy AmazonSSMManagedInstanceCore gestita.
3. Verifica che il ruolo IAM abbia la politica di fiducia corretta che consenta a Systems Manager di assumere il ruolo.

Soluzione 9: verifica le impostazioni di attivazione ibride

Per i nodi attivati in modo ibrido (server locali o VM in altri ambienti cloud), verifica che l'attivazione ibrida sia valida e che il nodo possa connettersi agli endpoint del servizio Systems Manager. Possono verificarsi problemi se l'attivazione è scaduta, il limite di registrazione è stato raggiunto o se ci sono registrazioni in conflitto.

Per risolvere i problemi di attivazione ibrida:

1. Verifica che l'attivazione ibrida non sia scaduta. Se è scaduta, crea una nuova attivazione. Per ulteriori informazioni, consulta [Crea un'attivazione ibrida per registrare i nodi con Systems Manager](#).
2. Verifica che il limite di registrazione all'attivazione non sia stato raggiunto. Se necessario, crea una nuova attivazione con un limite di registrazione più elevato o annulla la registrazione dei nodi inutilizzati.
3. Se hai clonato una macchina virtuale precedentemente registrata con Systems Manager, annulla la registrazione del nodo originale prima di registrare il clone per evitare conflitti di registrazione.
4. Verifica che il nodo ibrido possa raggiungere gli endpoint del servizio Systems Manager richiesti dalla sua posizione di rete. Per ulteriori informazioni, consulta [Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager](#).

Risoluzione dei problemi di disponibilità dei nodi gestiti tramite **ssm-cli**

ssm-cli è uno strumento a riga di comando autonomo incluso nell'installazione di SSM Agent. Quando si installa SSM Agent 3.1.501.0 o versione successiva su un computer, è possibile eseguire comandi **ssm-cli** su quel computer. L'output di questi comandi consente di determinare se la macchina soddisfa i requisiti minimi per la gestione di un'istanza Amazon EC2 o di una macchina non EC2 e quindi viene aggiunta agli elenchi di nodi AWS Systems Manager gestiti in Systems Manager. (SSM Agent la versione 3.1.501.0 è stata rilasciata a novembre 2021.)

Requisiti minimi

Affinché un'istanza Amazon EC2 o una macchina non EC2 possa essere gestita AWS Systems Manager e disponibile in elenchi di nodi gestiti, deve soddisfare tre requisiti principali:

- SSM Agent deve essere installato e in esecuzione su una macchina con un [sistema operativo supportato](#).

Alcuni AWS managed Amazon Machine Images (AMIs) per EC2 sono configurati per avviare istanze preinstallate. [SSM Agent](#) (È possibile configurare anche una AMI per preinstallare SSM Agent.) Per ulteriori informazioni, consulta [Trova AMI con il Agente SSM preinstallato](#).

- Un profilo di istanza AWS Identity and Access Management (IAM) (per istanze EC2) o un ruolo di servizio IAM (per macchine non EC2) che fornisce le autorizzazioni necessarie per comunicare con il servizio Systems Manager deve essere collegato alla macchina.
- SSM Agent deve essere in grado di connettersi a un endpoint di Systems Manager per registrarsi con il servizio. Successivamente, il nodo gestito deve essere disponibile per il servizio, il che viene

confermato dal servizio che invia un segnale ogni cinque minuti per controllare l'integrità del nodo gestito.

Comandi preconfigurati in ssm-cli

Sono inclusi comandi preconfigurati che raccolgono le informazioni richieste per la diagnostica del motivo per cui una macchina confermata come in esecuzione non è inclusa negli elenchi dei nodi gestiti in Systems Manager. Questi comandi vengono eseguiti quando si specifica l'opzione `get-diagnostics`.

Sulla macchina, esegui il seguente comando per utilizzare `ssm-cli` che ti aiuterà a risolvere i problemi relativi alla disponibilità dei nodi gestiti.

Linux & macOS

```
ssm-cli get-diagnostics --output table
```

Windows

Su macchine Windows Server, devi passare alla directory `C:\Program Files\Amazon\SSM` prima di eseguire il comando.

```
ssm-cli.exe get-diagnostics --output table
```

PowerShell

Su macchine Windows Server, devi passare alla directory `C:\Program Files\Amazon\SSM` prima di eseguire il comando.

```
.\ssm-cli.exe get-diagnostics --output table
```

Il comando restituisce un output come una tabella simile alla seguente.

Note

I controlli di connettività verso `ssmmessages`, `s3 kmslogs`, ed `monitoring endpoint` riguardano funzionalità opzionali aggiuntive, ad esempio la possibilità di accedere ad Amazon

Session Manager Simple Storage Service (Amazon S3) o Amazon CloudWatch Logs e utilizzare la crittografia (). AWS Key Management Service AWS KMS

Linux & macOS

```
[root@instance]# ssm-cli get-diagnostics --output table
```

```
#####
# Check                               # Status # Note
#                                     #
#####
# EC2 IMDS                            # Success # IMDS is accessible and has
instance id i-0123456789abcdefa in Region #
#                                     # us-east-2
#                                     #
#####
# Hybrid instance registration        # Skipped # Instance does not have hybrid
registration                          #
#####
# Connectivity to ssm endpoint         # Success # ssm.us-east-2.amazonaws.com is
reachable                             #
#####
# Connectivity to ec2messages endpoint # Success # ec2messages.us-
east-2.amazonaws.com is reachable    #
#####
# Connectivity to ssmmessages endpoint # Success # ssmmessages.us-
east-2.amazonaws.com is reachable    #
#####
# Connectivity to s3 endpoint          # Success # s3.us-east-2.amazonaws.com is
reachable                             #
#####
# Connectivity to kms endpoint         # Success # kms.us-east-2.amazonaws.com is
reachable                             #
#####
# Connectivity to logs endpoint        # Success # logs.us-east-2.amazonaws.com is
reachable                             #
#####
# Connectivity to monitoring endpoint  # Success # monitoring.us-
east-2.amazonaws.com is reachable    #
#####
# AWS Credentials                     # Success # Credentials are for
#
```

```

#                               #                               #
arn:aws:sts::123456789012:assumed-role/Fullaccess/i-0123456789abcdefa #
#                               #                               # and will expire at 2021-08-17
18:47:49 +0000 UTC                               #
#####
# Agent service                               # Success # Agent service is running and is
running as expected user                               #
#####
# Proxy configuration                               # Skipped # No proxy configuration detected
#
#####
# SSM Agent version                               # Success # SSM Agent version is 3.0.1209.0,
latest available agent version is                               #
#                               #                               # 3.1.192.0
#                               #
#####

```

Windows Server and PowerShell

```

PS C:\Program Files\Amazon\SSM> .\ssm-cli.exe get-diagnostics --output table
#####
# Check                               # Status # Note
#                               #
#####
# EC2 IMDS                               # Success # IMDS is accessible and has
instance id i-0123456789EXAMPLE in                               #
#                               #                               # Region us-east-2
#                               #
#####
# Hybrid instance registration           # Skipped # Instance does not have hybrid
registration                               #
#####
# Connectivity to ssm endpoint           # Success # ssm.us-east-2.amazonaws.com is
reachable                               #
#####
# Connectivity to ec2messages endpoint   # Success # ec2messages.us-
east-2.amazonaws.com is reachable                               #
#####
# Connectivity to ssmmessages endpoint   # Success # ssmmessages.us-
east-2.amazonaws.com is reachable                               #
#####
# Connectivity to s3 endpoint            # Success # s3.us-east-2.amazonaws.com is
reachable                               #
#####

```

```
#####
# Connectivity to kms endpoint          # Success # kms.us-east-2.amazonaws.com is
reachable                             #
#####
# Connectivity to logs endpoint         # Success # logs.us-east-2.amazonaws.com is
reachable                             #
#####
# Connectivity to monitoring endpoint   # Success # monitoring.us-
east-2.amazonaws.com is reachable     #
#####
# AWS Credentials                      # Success # Credentials are for
#                                     #
#                                     #
arn:aws:sts::123456789012:assumed-role/SSM-Role/i-123abc45EXAMPLE #
#                                     # and will expire at 2021-09-02
13:24:42 +0000 UTC                   #
#####
# Agent service                        # Success # Agent service is running and is
running as expected user              #
#####
# Proxy configuration                  # Skipped # No proxy configuration detected
#
#####
# Windows sysprep image state          # Success # Windows image state value is at
desired value IMAGE_STATE_COMPLETE   #
#####
# SSM Agent version                   # Success # SSM Agent version is 3.2.815.0,
latest agent version in us-east-2    #
#                                     # is 3.2.985.0
#
#####
```

La tabella seguente fornisce ulteriori dettagli per ciascuna delle verifiche eseguite da `ssm-cli`.

controlli diagnostici `ssm-cli`

Verifica	Informazioni
Servizio di metadati delle istanze Amazon EC2.	Indica se il nodo gestito può raggiungere il servizio di metadati. Un test non riuscito indica un problema di connettività a <code>http://169.254.169.254</code> che può essere causato

Verifica	Informazioni
	da configurazioni di firewall e proxy locali di routing, proxy o sistema operativo (OS).
Registrazione dell'istanza ibrida	Indica se SSM Agent è registrato utilizzando un'attivazione ibrida.
Connettività ad endpoint ssm	Indica se il nodo può raggiungere gli endpoint di servizio per Systems Manager sulla porta TCP 443. Un test non riuscito indica problemi di connettività che <code>https://ssm.region.amazonaws.com</code> dipendono dalla Regione AWS posizione del nodo. I problemi di connettività possono essere causati dalla configurazione VPC, inclusi gruppi di sicurezza, liste di controllo dell'accesso alla rete, tabelle di routing o firewall e proxy del sistema operativo.
Connettività ad endpoint ec2messages	Indica se il nodo può raggiungere gli endpoint di servizio per Systems Manager sulla porta TCP 443. Un test non riuscito indica problemi di connettività che <code>https://ec2messages.region.amazonaws.com</code> dipendono dalla Regione AWS posizione del nodo. I problemi di connettività possono essere causati dalla configurazione VPC, inclusi gruppi di sicurezza, liste di controllo dell'accesso alla rete, tabelle di routing o firewall e proxy del sistema operativo.

Verifica	Informazioni
Connettività ad endpoint ssmessages	Indica se il nodo può raggiungere gli endpoint di servizio per Systems Manager sulla porta TCP 443. Un test non riuscito indica problemi di connettività che <code>https://ssmmessages.region.amazonaws.com</code> dipendono dalla Regione AWS posizione del nodo. I problemi di connettività possono essere causati dalla configurazione VPC, inclusi gruppi di sicurezza, liste di controllo dell'accesso alla rete, tabelle di routing o firewall e proxy del sistema operativo.
Connettività ad endpoint s3	Indica se il nodo può raggiungere l'endpoint di servizio per Amazon Simple Storage Service sulla porta TCP 443. Un test non riuscito indica problemi di connettività che <code>https://s3.region.amazonaws.com</code> dipendono dalla Regione AWS posizione del nodo. La connettività a questo endpoint non è necessaria per la visualizzazione di un nodo nell'elenco dei nodi gestiti.
Connettività ad endpoint kms	Indica se il nodo può raggiungere l'endpoint di servizio AWS Key Management Service sulla porta TCP 443. Un test non riuscito indica problemi di connettività a <code>https://kms.region.amazonaws.com</code> seconda della posizione in Regione AWS cui si trova il nodo. La connettività a questo endpoint non è necessaria per la visualizzazione di un nodo nell'elenco dei nodi gestiti.

Verifica	Informazioni
Connettività ad endpoint logs	Indica se il nodo può raggiungere l'endpoint di servizio per Amazon CloudWatch Logs sulla porta TCP 443. Un test non riuscito indica problemi di connettività che <code>https://logs.<i>region</i>.amazonaws.com</code> dipendono dalla Regione AWS posizione del nodo. La connettività a questo endpoint non è necessaria per la visualizzazione di un nodo nell'elenco dei nodi gestiti.
Connettività ad endpoint monitoring	Indica se il nodo può raggiungere l'endpoint di servizio per Amazon CloudWatch sulla porta TCP 443. Un test non riuscito indica problemi di connettività che <code>https://monitoring.<i>region</i>.amazonaws.com</code> dipendono dalla Regione AWS posizione del nodo. La connettività a questo endpoint non è necessaria per la visualizzazione di un nodo nell'elenco dei nodi gestiti.
AWS Credenziali	Indica se SSM Agent dispone delle credenziali richieste in base al profilo dell'istanza IAM (per le istanze EC2) o al ruolo di servizio IAM (per macchine non EC2) collegate alla macchina. Un test non riuscito indica che nessun profilo dell'istanza IAM o ruolo di servizio IAM è collegato alla macchina o che non contiene le autorizzazioni richieste per Systems Manager.
Servizio agente	Indica se il servizio SSM Agent è in esecuzione e se il servizio è in esecuzione come root per Linux o macOS, o SYSTEM per Windows Server. Un test non riuscito indica che il servizio SSM Agent non è in esecuzione o non è in esecuzione come root o SYSTEM.

Verifica	Informazioni
Configurazione del proxy	Indica se SSM Agent è configurato per l'utilizzo di un proxy.
Stato dell'immagine Sysprep (solo Windows)	Indica lo stato di Sysprep sul nodo, SSM Agent non verrà avviato sul nodo se lo stato Sysprep ha un valore diverso da <code>IMAGE_STATE_COMPLETE</code> .
Versione SSM Agent	Indica se l'ultima versione disponibile di SSM Agent è installata.

AWS Systems Manager Attivazioni ibride

 La pagina delle attivazioni ibride sarà obsoleta il 31 dicembre 2026.

Man mano che semplifichiamo l'esperienza della console di Systems Manager, le attivazioni ibride passeranno alla console unificata di Systems Manager. Tutte le attivazioni esistenti rimangono disponibili tramite API e visualizzabili nella console unificata. [Ulteriori informazioni](#)

Per configurare macchine non EC2 da utilizzare AWS Systems Manager in un [ambiente](#) ibrido e multicloud, crei un'attivazione ibrida. Non-EC2 i tipi di computer supportati come nodi gestiti includono:

- Server presso la propria sede (server on-premises)
- AWS IoT Greengrass dispositivi principali
- AWS IoT e dispositivi non AWS periferici
- Macchine virtuali (VM), incluse le macchine virtuali in altri ambienti cloud

Quando esegui il comando [create-activation](#) per avviare un processo di attivazione ibrido, riceverai un codice di attivazione e un ID nella risposta al comando. Il codice di attivazione e l'ID vengono quindi inclusi nel comando per installare SSM Agent sul computer, come descritto nel passaggio 3 di [Installa Agente SSM su nodi Linux ibridi](#) e nel passaggio 4 di [Installa Agente SSM su ibrido Windows Server nodi](#).

Questo processo di attivazione si applica a tutti i tipi di macchine non EC2 ad eccezione dei dispositivi AWS IoT Greengrass principali. Per informazioni sulla configurazione dei dispositivi core AWS IoT Greengrass per Systems Manager, consulta [Gestione dei dispositivi edge con Systems Manager](#).

 Note

Il supporto non è attualmente fornito per macchine macOS non EC2.

 Note

Importante: a partire dal 30 giugno 2026, il livello di istanze avanzate è stato rimosso. Non esiste più un limite di 1.000 istanze per i nodi gestiti ibridi e non è più necessario abilitare un livello a pagamento da utilizzare su macchine non EC2. Session Manager Invece, a partire dal 30 settembre 2026, utilizza i prezzi Session Manager pay-as-you-go se Run Command utilizzati su nodi gestiti ibridi.

Per ulteriori informazioni sui prezzi, consulta [Prezzi di AWS Systems Manager](#).

AWS Systems Manager Inventory

AWS Systems Manager L'inventario offre visibilità nel tuo ambiente AWS informatico. È possibile utilizzare Inventory per raccogliere i metadati dai tuoi nodi gestiti. È possibile archiviare questi metadati in un bucket centrale Amazon Simple Storage Service (Amazon S3), quindi utilizzare gli strumenti predefiniti per eseguire query sui dati e individuare rapidamente quali nodi eseguono il software e le configurazioni richiesti dalla tua policy software e i nodi che devono essere aggiornati. È possibile Inventory su tutti i nodi gestiti utilizzando una procedura con un solo clic. Puoi anche configurare e visualizzare i dati di inventario da più Regioni AWS unità Account AWS utilizzando Amazon Athena. Per iniziare a utilizzare l'inventario, apri la [console di Systems Manager](#). Nel riquadro di navigazione, seleziona Inventario.

Quando i tipi di metadati preconfigurati raccolti da l'inventario di Systems Manager non soddisfano le proprie esigenze, è possibile creare un inventario personalizzato. Un inventario personalizzato è semplicemente un file JSON con le informazioni che fornisci e aggiungi al nodo gestito in una directory specifica. I dati raccolti da l'inventario di Systems Manager sono quelli contenuti in questo inventario personalizzato. Ad esempio, se esegui un data center di grandi dimensioni, è possibile

specificare la posizione del rack di ciascun server come inventario personalizzato. È possibile quindi visualizzare i dati nello spazio sul rack quando visualizzi altri dati di inventario.

⚠ Important

L'inventario di Systems Manager raccoglie solo i metadati dei nodi gestiti. non accede alle informazioni o ai dati proprietari.

La tabella seguente elenca i tipi di dati da raccogliere con Systems Manager Inventory. La tabella descrive anche diverse offerte per i nodi di destinazione e gli intervalli di raccolta che è possibile specificare.

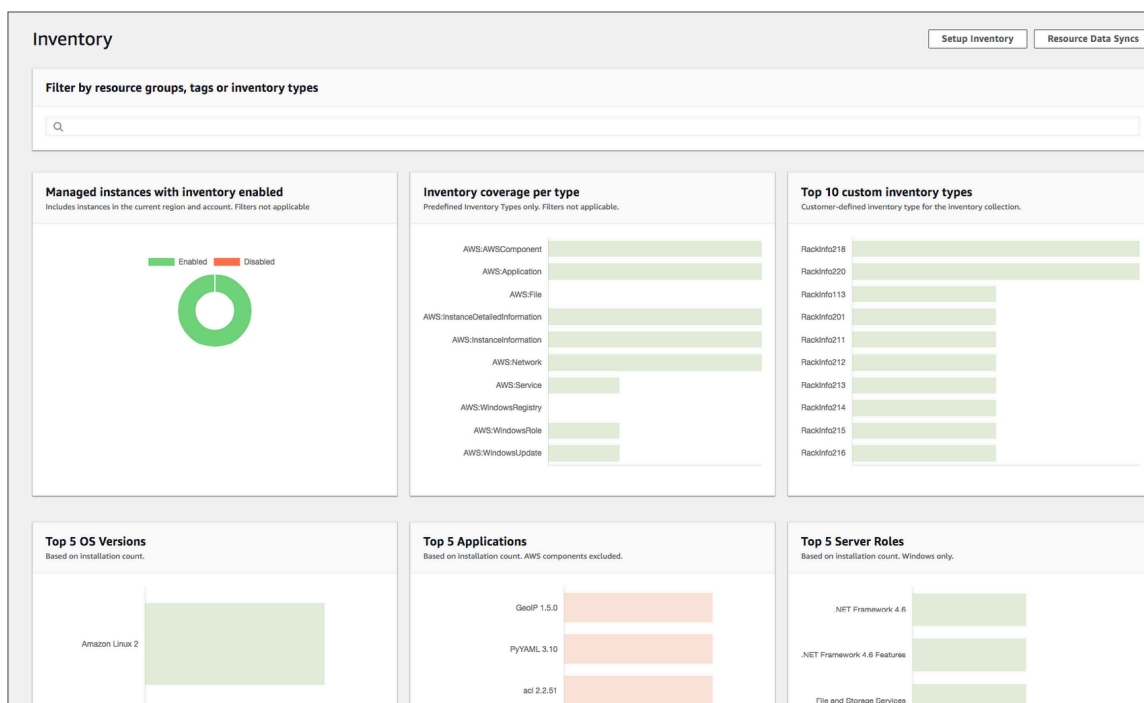
Configurazione	Informazioni
Tipi di metadati	<p>È possibile configurare Inventory per raccogliere i seguenti tipi di dati:</p> <ul style="list-style-type: none">• Applicazioni: nomi delle applicazioni, editori, versioni, ecc.• AWS componenti: driver EC2, agenti, versioni, ecc.• File: nome, dimensioni, versione, data di installazione, ora di modifica e dell'ultimo accesso, ecc.• Configurazione di rete: indirizzo IP, indirizzo MAC, DNS, gateway, maschera sottorete, ecc.• Aggiornamenti di Windows: ID aggiornamento rapido, autore dell'installazione, data di installazione, ecc.• Dettagli dell'istanza: modello CPU, core CPU, CPU, socket CPU, CPUspeedMHz CPUHyperThreadEnabled OSService Packetc

Configurazione	Informazioni
	<ul style="list-style-type: none">• Servizi: nome, nome visualizzato, stato, servizi dipendenti, tipo di servizio, tipo di avvio, ecc.• Tag: i tag assegnati ai tuoi nodi.• Registro di sistema di Windows: percorso della chiave del registro di sistema, nome del valore, tipo di valore e valore.• Ruoli Windows: nome, nome visualizzato, percorso, tipo di funzionalità, stato di installazione, ecc.• Inventario personalizzato: metadati assegnati a un nodo gestito come descritto in Utilizzo di inventari personalizzati. <div> Note Per visualizzare un elenco di tutti i metadati raccolti da Inventory, consulta Metadati raccolti da Inventory.</div>
Nodi di destinazione	Puoi scegliere di inventariare tutti i nodi gestiti nei tuoi nodi Account AWS, seleziona ti individualmente o nei gruppi target di nodi utilizzando i tag. Per ulteriori informazioni sulla raccolta dei dati di inventario da tutti i nodi gestiti, consulta Fai l'inventario di tutti i nodi gestiti nel tuo Account AWS .
Quando raccogliere le informazioni	È possibile specificare un intervallo di raccolta in termini di minuti, ore e giorni. L'intervallo di raccolta più breve è ogni 30 minuti.

Note

A seconda della quantità di dati raccolti, il sistema può impiegare alcuni minuti per restituire i dati sull'output specificato. Dopo aver raccolto le informazioni, i dati vengono inviati tramite un canale HTTPS sicuro a un AWS archivio di testo normale accessibile solo dal tuo Account AWS.

È possibile visualizzare i dati della console Systems Manager nella pagina Inventory (Inventario), che comprende diverse schede predefinite che permettono di eseguire le query sui dati.



Note

Le schede di Inventory (Inventario) filtrano automaticamente le istanze gestite Amazon EC2 con stato terminato e arrestato. Per i nodi locali e gestiti dai dispositivi AWS IoT Greengrass principali, le schede di inventario filtrano automaticamente i nodi con lo stato Terminato.

Se crei una sincronizzazione dati risorsa per sincronizzare e archiviare tutti i tuoi dati in un singolo bucket Amazon S3, è possibile esplorare i dati dalla pagina Inventory Detailed View (Vista dettagliata inventario). Per ulteriori informazioni, consulta [Esecuzione di query sui dati di inventario da più regioni e account](#).

EventBridge supporto

Questo strumento Systems Manager è supportato come tipo di evento nelle EventBridge regole di Amazon. Per informazioni, consulta [Monitoraggio degli eventi di Systems Manager con Amazon EventBridge](#) e [Riferimento: modelli e tipi di EventBridge eventi Amazon per Systems Manager](#).

Indice

- [Ulteriori informazioni su l'inventario di Systems Manager](#)
- [Impostazione dell'inventario di Systems Manager](#)
- [Configurazione della raccolta dell'inventario](#)
- [Esecuzione di query sui dati di inventario da più regioni e account](#)
- [Esecuzione di query su una raccolta di inventario mediante filtri](#)
- [Aggregazione dei dati di inventario](#)
- [Utilizzo di inventari personalizzati](#)
- [Visualizzazione della cronologia e del monitoraggio delle modifiche di Inventory](#)
- [Interruzione della raccolta dati ed eliminazione dei dati di inventario](#)
- [Assegnazione di metadati di inventario personalizzati a un nodo gestito](#)
- [Utilizzo di AWS CLI per configurare la raccolta dei dati di inventario](#)
- [Procedura dettagliata: utilizzo di sincronizzazione dati risorsa per aggregare dati di inventario](#)
- [Risoluzione dei problemi di Inventory Systems Manager](#)

Ulteriori informazioni su l'inventario di Systems Manager

Quando configuri AWS Systems Manager Inventory, specifichi il tipo di metadati da raccogliere, i nodi gestiti da cui effettuare la raccolta e una pianificazione per la raccolta dei metadati. Queste configurazioni vengono salvate insieme all'utente come associazione. Account AWS AWS Systems Manager State Manager Un'associazione è semplicemente una configurazione.

Note

Inventory raccoglie solo metadati. Non raccoglie dati personali o proprietari.

Argomenti

- [Metadati raccolti da Inventory](#)

- [Utilizzo dell'inventario dei file e del registro di sistema di Windows](#)

Metadati raccolti da Inventory

Il seguente esempio mostra la lista completa dei metadati raccolti da ciascun plugin dell'inventario AWS Systems Manager .

```
{
  "typeName": "AWS:InstanceInformation",
  "version": "1.0",
  "attributes":[
    { "name": "AgentType",                "dataType" : "STRING"},
    { "name": "AgentVersion",             "dataType" : "STRING"},
    { "name": "ComputerName",             "dataType" : "STRING"},
    { "name": "InstanceId",               "dataType" : "STRING"},
    { "name": "IpAddress",                "dataType" : "STRING"},
    { "name": "PlatformName",             "dataType" : "STRING"},
    { "name": "PlatformType",             "dataType" : "STRING"},
    { "name": "PlatformVersion",          "dataType" : "STRING"},
    { "name": "ResourceType",             "dataType" : "STRING"},
    { "name": "AgentStatus",              "dataType" : "STRING"},
    { "name": "InstanceStatus",           "dataType" : "STRING"}
  ]
},
{
  "typeName" : "AWS:Application",
  "version": "1.1",
  "attributes":[
    { "name": "Name",                    "dataType": "STRING"},
    { "name": "ApplicationType",         "dataType": "STRING"},
    { "name": "Publisher",               "dataType": "STRING"},
    { "name": "Version",                 "dataType": "STRING"},
    { "name": "Release",                 "dataType": "STRING"},
    { "name": "Epoch",                  "dataType": "STRING"},
    { "name": "InstalledTime",           "dataType": "STRING"},
    { "name": "Architecture",            "dataType": "STRING"},
    { "name": "URL",                     "dataType": "STRING"},
    { "name": "Summary",                 "dataType": "STRING"},
    { "name": "PackageId",               "dataType": "STRING"}
  ]
},
{
  "typeName" : "AWS:File",
```



```

    "version": "1.0",
    "attributes": [
      { "name": "Name", "dataType": "STRING"},
      { "name": "Size", "dataType": "STRING"},
      { "name": "Description", "dataType": "STRING"},
      { "name": "FileVersion", "dataType": "STRING"},
      { "name": "InstalledDate", "dataType": "STRING"},
      { "name": "ModificationTime", "dataType": "STRING"},
      { "name": "LastAccessTime", "dataType": "STRING"},
      { "name": "ProductName", "dataType": "STRING"},
      { "name": "InstalledDir", "dataType": "STRING"},
      { "name": "ProductLanguage", "dataType": "STRING"},
      { "name": "CompanyName", "dataType": "STRING"},
      { "name": "ProductVersion", "dataType": "STRING"}
    ]
  },
  {
    "typeName": "AWS:AWSComponent",
    "version": "1.0",
    "attributes": [
      { "name": "Name", "dataType": "STRING"},
      { "name": "ApplicationType", "dataType": "STRING"},
      { "name": "Publisher", "dataType": "STRING"},
      { "name": "Version", "dataType": "STRING"},
      { "name": "InstalledTime", "dataType": "STRING"},
      { "name": "Architecture", "dataType": "STRING"},
      { "name": "URL", "dataType": "STRING"}
    ]
  },
  {
    "typeName": "AWS:WindowsUpdate",
    "version": "1.0",
    "attributes": [
      { "name": "HotFixId", "dataType": "STRING"},
      { "name": "Description", "dataType": "STRING"},
      { "name": "InstalledTime", "dataType": "STRING"},
      { "name": "InstalledBy", "dataType": "STRING"}
    ]
  },
  {
    "typeName": "AWS:Network",
    "version": "1.0",
    "attributes": [
      { "name": "Name", "dataType": "STRING"},

```

```

    { "name": "SubnetMask",          "dataType": "STRING"},
    { "name": "Gateway",            "dataType": "STRING"},
    { "name": "DHCPsServer",        "dataType": "STRING"},
    { "name": "DNSServer",          "dataType": "STRING"},
    { "name": "MacAddress",         "dataType": "STRING"},
    { "name": "IPV4",               "dataType": "STRING"},
    { "name": "IPV6",               "dataType": "STRING"}
  ]
},
{
  "typeName": "AWS:PatchSummary",
  "version": "1.0",
  "attributes": [
    { "name": "PatchGroup",          "dataType": "STRING"},
    { "name": "BaselineId",          "dataType": "STRING"},
    { "name": "SnapshotId",          "dataType": "STRING"},
    { "name": "OwnerInformation",     "dataType": "STRING"},
    { "name": "InstalledCount",       "dataType": "NUMBER"},
    { "name": "InstalledPendingRebootCount", "dataType": "NUMBER"},
    { "name": "InstalledOtherCount",  "dataType": "NUMBER"},
    { "name": "InstalledRejectedCount", "dataType": "NUMBER"},
    { "name": "NotApplicableCount",   "dataType": "NUMBER"},
    { "name": "UnreportedNotApplicableCount", "dataType": "NUMBER"},
    { "name": "MissingCount",         "dataType": "NUMBER"},
    { "name": "FailedCount",          "dataType": "NUMBER"},
    { "name": "OperationType",        "dataType": "STRING"},
    { "name": "OperationStartTime",   "dataType": "STRING"},
    { "name": "OperationEndTime",     "dataType": "STRING"},
    { "name": "InstallOverrideList",  "dataType": "STRING"},
    { "name": "RebootOption",         "dataType": "STRING"},
    { "name": "LastNoRebootInstallOperationTime", "dataType": "STRING"},
    { "name": "ExecutionId",          "dataType": "STRING"},
    "isOptional": "true",
    { "name": "NonCompliantSeverity",  "dataType": "STRING",
    "isOptional": "true",
    { "name": "SecurityNonCompliantCount", "dataType": "NUMBER",
    "isOptional": "true",
    { "name": "CriticalNonCompliantCount", "dataType": "NUMBER",
    "isOptional": "true",
    { "name": "OtherNonCompliantCount", "dataType": "NUMBER",
    "isOptional": "true"}
  ]
},
{

```

```

    "typeName": "AWS:PatchCompliance",
    "version": "1.0",
    "attributes": [
      { "name": "Title", "dataType": "STRING"},
      { "name": "KBId", "dataType": "STRING"},
      { "name": "Classification", "dataType": "STRING"},
      { "name": "Severity", "dataType": "STRING"},
      { "name": "State", "dataType": "STRING"},
      { "name": "InstalledTime", "dataType": "STRING"}
    ]
  },
  {
    "typeName": "AWS:ComplianceItem",
    "version": "1.0",
    "attributes": [
      { "name": "ComplianceType", "dataType": "STRING",
"isContext": "true"},
      { "name": "ExecutionId", "dataType": "STRING",
"isContext": "true"},
      { "name": "ExecutionType", "dataType": "STRING",
"isContext": "true"},
      { "name": "ExecutionTime", "dataType": "STRING",
"isContext": "true"},
      { "name": "Id", "dataType": "STRING"},
      { "name": "Title", "dataType": "STRING"},
      { "name": "Status", "dataType": "STRING"},
      { "name": "Severity", "dataType": "STRING"},
      { "name": "DocumentName", "dataType": "STRING"},
      { "name": "DocumentVersion", "dataType": "STRING"},
      { "name": "Classification", "dataType": "STRING"},
      { "name": "PatchBaselineId", "dataType": "STRING"},
      { "name": "PatchSeverity", "dataType": "STRING"},
      { "name": "PatchState", "dataType": "STRING"},
      { "name": "PatchGroup", "dataType": "STRING"},
      { "name": "InstalledTime", "dataType": "STRING"},
      { "name": "InstallOverrideList", "dataType": "STRING",
"isOptional": "true"},
      { "name": "DetailedText", "dataType": "STRING",
"isOptional": "true"},
      { "name": "DetailedLink", "dataType": "STRING",
"isOptional": "true"},
      { "name": "CVEIds", "dataType": "STRING",
"isOptional": "true"}
    ]
  }

```

```

},
{
  "typeName": "AWS:ComplianceSummary",
  "version": "1.0",
  "attributes": [
    { "name": "ComplianceType", "dataType": "STRING"},
    { "name": "PatchGroup", "dataType": "STRING"},
    { "name": "PatchBaselineId", "dataType": "STRING"},
    { "name": "Status", "dataType": "STRING"},
    { "name": "OverallSeverity", "dataType": "STRING"},
    { "name": "ExecutionId", "dataType": "STRING"},
    { "name": "ExecutionType", "dataType": "STRING"},
    { "name": "ExecutionTime", "dataType": "STRING"},
    { "name": "CompliantCriticalCount", "dataType": "NUMBER"},
    { "name": "CompliantHighCount", "dataType": "NUMBER"},
    { "name": "CompliantMediumCount", "dataType": "NUMBER"},
    { "name": "CompliantLowCount", "dataType": "NUMBER"},
    { "name": "CompliantInformationalCount", "dataType": "NUMBER"},
    { "name": "CompliantUnspecifiedCount", "dataType": "NUMBER"},
    { "name": "NonCompliantCriticalCount", "dataType": "NUMBER"},
    { "name": "NonCompliantHighCount", "dataType": "NUMBER"},
    { "name": "NonCompliantMediumCount", "dataType": "NUMBER"},
    { "name": "NonCompliantLowCount", "dataType": "NUMBER"},
    { "name": "NonCompliantInformationalCount", "dataType": "NUMBER"},
    { "name": "NonCompliantUnspecifiedCount", "dataType": "NUMBER"}
  ]
},
{
  "typeName": "AWS:InstanceDetailedInformation",
  "version": "1.0",
  "attributes": [
    { "name": "CPUModel", "dataType": "STRING"},
    { "name": "CPUCores", "dataType": "NUMBER"},
    { "name": "CPUs", "dataType": "NUMBER"},
    { "name": "CPUSpeedMHz", "dataType": "NUMBER"},
    { "name": "CPUSockets", "dataType": "NUMBER"},
    { "name": "CPUPhyperThreadEnabled", "dataType": "STRING"},
    { "name": "OSServicePack", "dataType": "STRING"}
  ]
},
{
  "typeName": "AWS:Service",
  "version": "1.0",
  "attributes": [

```

```

        { "name": "Name",                "dataType": "STRING"},
        { "name": "DisplayName",        "dataType": "STRING"},
        { "name": "ServiceType",        "dataType": "STRING"},
        { "name": "Status",              "dataType": "STRING"},
        { "name": "DependentServices",   "dataType": "STRING"},
        { "name": "ServicesDependedOn",  "dataType": "STRING"},
        { "name": "StartType",           "dataType": "STRING"}
    ]
},
{
    "typeName": "AWS:WindowsRegistry",
    "version": "1.0",
    "attributes": [
        { "name": "KeyPath",                "dataType": "STRING"},
        { "name": "ValueName",              "dataType": "STRING"},
        { "name": "ValueType",              "dataType": "STRING"},
        { "name": "Value",                   "dataType": "STRING"}
    ]
},
{
    "typeName": "AWS:WindowsRole",
    "version": "1.0",
    "attributes": [
        { "name": "Name",                "dataType": "STRING"},
        { "name": "DisplayName",          "dataType": "STRING"},
        { "name": "Path",                  "dataType": "STRING"},
        { "name": "FeatureType",           "dataType": "STRING"},
        { "name": "DependsOn",             "dataType": "STRING"},
        { "name": "Description",           "dataType": "STRING"},
        { "name": "Installed",             "dataType": "STRING"},
        { "name": "InstalledState",        "dataType": "STRING"},
        { "name": "SubFeatures",           "dataType": "STRING"},
        { "name": "ServerComponentDescriptor", "dataType": "STRING"},
        { "name": "Parent",                "dataType": "STRING"}
    ]
},
{
    "typeName": "AWS:Tag",
    "version": "1.0",
    "attributes": [
        { "name": "Key",                "dataType": "STRING"},
        { "name": "Value",              "dataType": "STRING"}
    ]
},

```

```
{
  "typeName": "AWS:ResourceGroup",
  "version": "1.0",
  "attributes": [
    { "name": "Name", "dataType": "STRING" },
    { "name": "Arn", "dataType": "STRING" }
  ]
},
{
  "typeName": "AWS:BillingInfo",
  "version": "1.0",
  "attributes": [
    { "name": "BillingProductId", "dataType": "STRING" }
  ]
}
```

Note

- Perché "typeName": "AWS:InstanceInformation", InstanceStatus può essere uno dei seguenti: Attivo, Interrotto ConnectionLost, Terminato.
- Con la versione 2.5, il pacchetto RPM (Resource Package Manager) ha sostituito l'attributo Serial con Epoch. L'attributo Epoch è un numero intero monotonicamente crescente come l'attributo Serial. Quando crei l'inventario utilizzando il tipo AWS:Application, un valore maggiore per Epoch indica una versione più recente. Se i valori di Epoch sono identici o vuoti, utilizza il valore dell'attributo Version o Release per determinare la versione più recente.
- Alcuni metadati non sono disponibili da istanze Linux. In particolare, per «typeName»: "AWS:Network«, i seguenti tipi di metadati non sono ancora supportati per le istanze Linux. SONO supportate per Windows.
 - {«name»: "«, SubnetMask «dataType»: «STRING»},
 - { "name": "DHCPServer", "dataType": "STRING"},
 - { "name": "DNSServer", "dataType": "STRING"},
 - { "name": "Gateway", "dataType": "STRING"},

Utilizzo dell'inventario dei file e del registro di sistema di Windows

AWS Systems Manager Inventory consente di cercare e inventariare i file su Windows Server Linux e sistemi macOS operativi. Puoi anche eseguire un inventario del registro di sistema di Windows in cui eseguire ricerche.

File: puoi raccogliere informazioni sui metadati dei file, ad esempio nomi file, data e ora di creazione dei file, data e ora dell'ultimo accesso/aggiornamento dei file, dimensioni dei file, per citarne alcuni. Per avviare la raccolta dell'inventario dei file, devi specificare un percorso su cui eseguire l'inventario, uno o più modelli che definiscono i tipi di file di cui eseguire un inventario e se il percorso deve essere attraversato in modo ricorsivo. Systems Manager esegue l'inventario di tutti i metadati dei file per i file nel percorso specificato che corrispondono al modello. L'inventario dei file utilizza il seguente parametro di input.

```
{
  "Path": string,
  "Pattern": array[string],
  "Recursive": true,
  "DirScanLimit" : number // Optional
}
```

- Path: il percorso della directory in cui desideri eseguire l'inventario dei file. Per Windows, puoi utilizzare variabili di ambiente, come %PROGRAMFILES% , a condizione che la variabile sia associata a un solo percorso di directory. Ad esempio, se usi la variabile %PATH% associata a più percorsi di directory, Inventory genera un errore.
- Pattern: una gamma di modelli per identificare i file.
- Recursive: un valore booleano che indica se Inventory deve attraversare le directory in modo ricorsivo.
- DirScanLimit: un valore opzionale che specifica quante directory scansionare. Utilizza questo parametro per ridurre al minimo l'impatto sui tuoi nodi gestiti. Inventory analizza un massimo di 5.000 directory.

Note

Inventory raccoglie i metadati per un massimo di 500 file in tutti i percorsi specificati.

Di seguito sono elencati alcuni esempi di come specificare i parametri per l'esecuzione di un inventario di file.

- Su Linux e macOS, raccogli i metadati dei file ".sh" nella directory /home/ec2-user, escludendo tutte le sottodirectory.

```
[{"Path":"/home/ec2-user","Pattern":["*.sh", "*.sh"],"Recursive":false}]
```

- In Windows, raccogli i metadati di tutti i file ".exe" nella cartella Programmi, includendo le sottodirectory in modo ricorsivo.

```
[{"Path":"C:\\Program Files","Pattern":["*.exe"],"Recursive":true}]
```

- In Windows, raccogli i metadati di modelli di log specifici.

```
[{"Path":"C:\\ProgramData\\Amazon","Pattern":["*amazon*.log"],"Recursive":true}]
```

- Limita il numero di directory durante la raccolta ricorsiva.

```
[{"Path":"C:\\Users","Pattern":["*.ps1"],"Recursive":true, "DirScanLimit": 1000}]
```

Windows Registry: puoi raccogliere chiavi e valori del registro di sistema di Windows. È possibile scegliere un percorso chiave e raccogliere tutte le chiavi e i valori in modo ricorsivo. È possibile inoltre raccogliere una determinata chiave di registro e il relativo valore per un percorso specifico. Inventory raccoglie il percorso, il nome, il tipo e il valore delle chiavi.

```
{
  "Path": string,
  "Recursive": true,
  "ValueNames": array[string] // optional
}
```

- Percorso: il percorso della chiave del registro di sistema.
- Recursive: un valore booleano che indica se la funzione Inventario deve attraversare i percorsi del registro di sistema in modo ricorsivo.
- ValueNames: Una serie di nomi di valori per l'esecuzione dell'inventario delle chiavi di registro. Se utilizzi questo parametro, Systems Manager eseguirà l'inventario solo dei nomi di valori specificati per il percorso indicato.

Note

Inventory raccoglie i metadati per un massimo di 250 valori della chiave di registro di sistema per tutti i percorsi specificati.

Di seguito sono elencati alcuni esempi di come specificare i parametri per l'esecuzione di un inventario del registro di sistema di Windows.

- Raccogli in modo ricorsivo tutte le chiavi e i valori per un percorso specifico.

```
[{"Path": "HKEY_LOCAL_MACHINE\\SOFTWARE\\Amazon", "Recursive": true}]
```

- Raccogli tutte le chiavi e i valori per un percorso specifico (ricerca ricorsiva disabilitata).

```
[{"Path": "HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\PSIS\\PSIS_DECODER", "Recursive": false}]
```

- Raccogli una chiave specifica utilizzando l'opzione `ValueNames`.

```
{"Path": "HKEY_LOCAL_MACHINE\\SOFTWARE\\Amazon\\MachineImage", "ValueNames": ["AMIName"]}
```

Impostazione dell'inventario di Systems Manager

Prima di utilizzare AWS Systems Manager Inventory per raccogliere metadati su applicazioni, servizi, AWS componenti e altro in esecuzione sui nodi gestiti, ti consigliamo di configurare la sincronizzazione dei dati delle risorse per centralizzare lo storage dei dati di inventario in un unico bucket Amazon Simple Storage Service (Amazon S3). Ti consigliamo inoltre di configurare il EventBridge monitoraggio di Amazon degli eventi dell'inventario. Questi processi semplificano la visualizzazione e la gestione dei dati di inventario e della raccolta.

Argomenti

- [Creazione di un Resource Data Sync per Inventario](#)
- [Utilizzo EventBridge per monitorare gli eventi dell'inventario](#)

Creazione di un Resource Data Sync per Inventario

In questo argomento viene descritto come impostare e configurare la sincronizzazione dei dati delle risorse per AWS Systems Manager Inventory. Per informazioni sulla sincronizzazione dati risorsa

Systems Manager Explorer, consulta [Configurazione di Systems Manager Explorer per visualizzare dati da più account e regioni](#).

Informazioni su Resource Data Sync

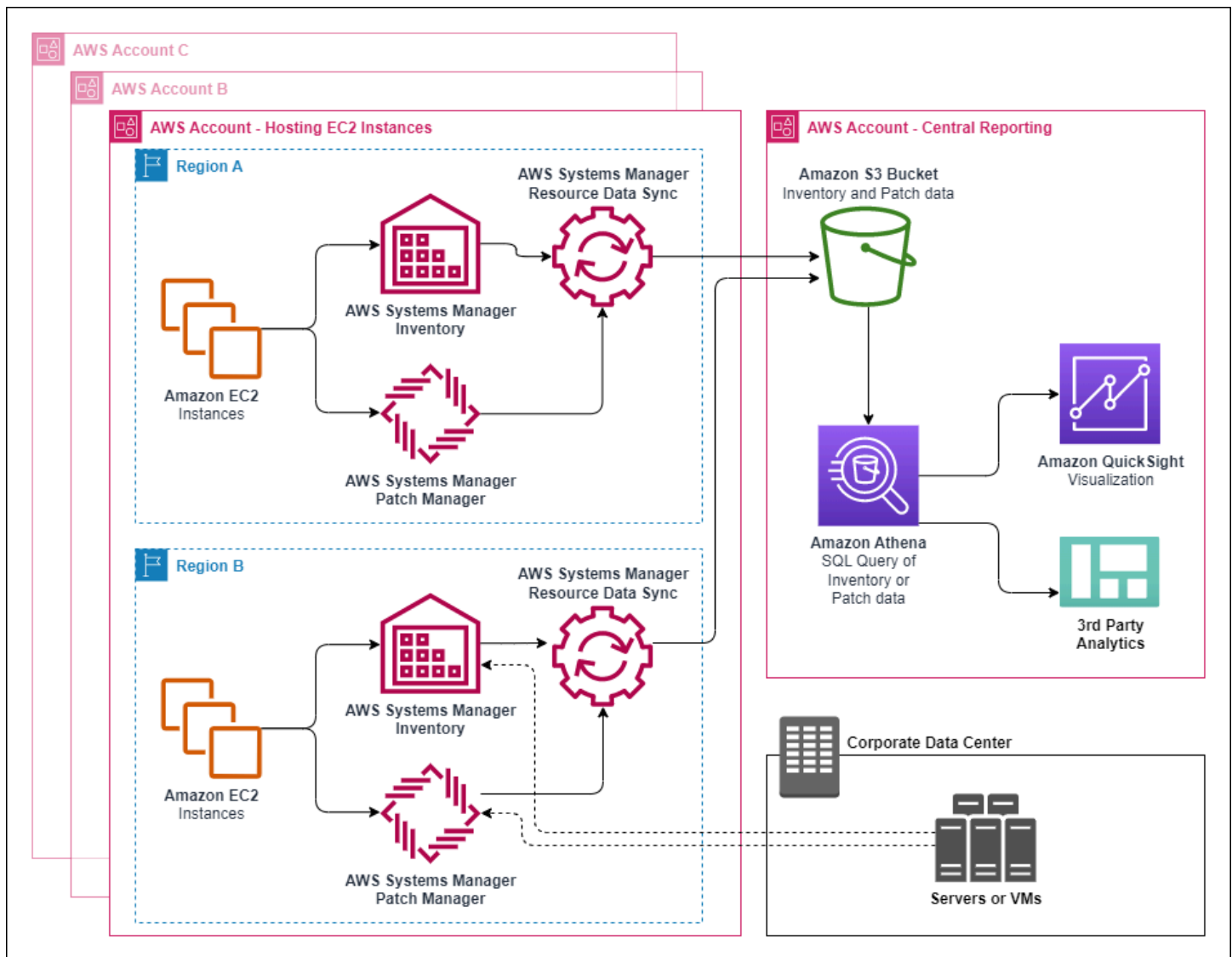
Puoi utilizzare Resource Data Sync di Systems Manager per inviare i dati di inventario raccolti da tutti i nodi gestiti in un singolo bucket Amazon Simple Storage Service (Amazon S3). La sincronizzazione dei dati della risorsa aggiorna automaticamente i dati centralizzati una volta raccolti i nuovi dati inventario. Con tutti i dati di inventario archiviati in un bucket Amazon S3 di destinazione, puoi utilizzare servizi come Amazon Athena e Amazon Quick per interrogare e analizzare i dati aggregati.

Ad esempio, supponi di aver configurato Inventory per raccogliere dati sul sistema operativo e sulle applicazioni in esecuzione in un parco di 150 nodi gestiti. Alcuni di questi nodi si trovano in un data center on-premises, mentre altri sono in esecuzione in Amazon Elastic Compute Cloud (Amazon EC2) su più Regioni AWS. Se non hai configurato Resource Data Sync, devi raccogliere manualmente i dati di inventario raccolti per ogni nodo gestito oppure devi creare script per raccogliere queste informazioni. Dovrai quindi trasferire i dati in un'applicazione per potervi eseguire query e analisi.

Con Resource Data Sync, puoi eseguire un'unica operazione per sincronizzare tutti i dati di Inventory da tutte i tuoi nodi gestiti. Una volta creata la sincronizzazione, Systems Manager crea una base di tutti i dati di inventario e la salva nel bucket Amazon S3 di destinazione. Quando vengono raccolti nuovi dati di inventario, Systems Manager aggiorna automaticamente i dati nel bucket Amazon S3. Potrai quindi trasferire i dati in modo rapido ed economico su Amazon Athena e Amazon Quick.

Il diagramma 1 mostra il modo in cui la sincronizzazione dei dati della risorsa aggrega i dati di inventario di Amazon EC2 e altri tipi di macchina presenti in un ambiente [ibrido e multicloud](#) in un bucket Amazon S3 di destinazione. Questo diagramma mostra anche come funziona la sincronizzazione dei dati delle risorse con più e Account AWS Regioni AWS

Diagramma 1: Sincronizzazione dei dati delle risorse con più e Account AWS Regioni AWS



Se elimini un nodo gestito, Resource Data Sync mantiene il file Inventory per il nodo eliminato. Tuttavia, per i nodi in esecuzione, sincronizzazione dati risorsa sovrascrive automaticamente i file di inventario precedenti quando vengono creati e scritti nel bucket Amazon S3 nuovi file. Se desideri tenere traccia delle variazioni dell'inventario nel tempo, puoi utilizzare il AWS Config servizio per tenere traccia del tipo di `SSM:ManagedInstanceInventory` risorsa. Per ulteriori informazioni, consulta [Guida introduttiva a AWS Config](#).

Utilizza le procedure in questa sezione per creare una sincronizzazione dei dati delle risorse per Inventory utilizzando Amazon S3 e AWS Systems Manager le console. Puoi anche utilizzarla AWS CloudFormation per creare o eliminare una sincronizzazione dei dati delle risorse. Per CloudFormation utilizzarla, aggiungi la [AWS::SSM::ResourceDataSync](#) risorsa al tuo CloudFormation modello. Per informazioni, consulta una delle seguenti fonti:

- [AWS CloudFormation risorsa per la sincronizzazione dei dati delle risorse in AWS Systems Manager](#) (blog)
- [Utilizzo di modelli AWS CloudFormation](#) nella Guida per l'utente di AWS CloudFormation

Note

Puoi usare AWS Key Management Service (AWS KMS) per crittografare i dati di inventario nel bucket Amazon S3. Per un esempio di come creare una sincronizzazione crittografata utilizzando AWS Command Line Interface (AWS CLI) e come lavorare con i dati centralizzati in Amazon Athena e Amazon Quick, consulta. [Procedura dettagliata: utilizzo di sincronizzazione dati risorsa per aggregare dati di inventario](#)

Prima di iniziare

Prima di creare una sincronizzazione dati risorsa, utilizzare la procedura seguente per creare un bucket Amazon S3 centralizzato per archiviare i dati di inventario aggregati. La procedura descrive come assegnare la policy di bucket che consente a Systems Manager di scrivere i dati di inventario nel bucket da più account. Se si dispone già di un bucket Amazon S3 che si desidera utilizzare per aggregare i dati di inventario per la sincronizzazione dati risorsa, è necessario configurare il bucket per utilizzare la policy nella procedura seguente.

Note

L'inventario di Systems Manager non può aggiungere dati a un bucket Amazon S3 specificato se tale bucket è configurato per l'utilizzo del comando Object Lock. Verifica che il bucket Amazon S3 creato o scelto per la sincronizzazione dati risorsa non sia configurato per l'utilizzo del comando Object Lock di Amazon S3. Per ulteriori informazioni, consulta [Come funziona Amazon S3 Object Lock](#) nella Guida per l'utente di Amazon Simple Storage Service.

Creazione e configurazione di un bucket Amazon S3 per la sincronizzazione dati risorsa

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Creare un bucket in cui archiviare i dati di inventario aggregati. Per ulteriori informazioni, consulta [Creazione di un bucket](#) nella Guida per l'utente di Amazon Simple Storage Service. Prendi nota del nome del bucket e del Regione AWS luogo in cui lo hai creato.

3. Scegli la scheda Autorizzazioni e quindi Policy (Policy di bucket).
4. Copia e incolla la policy di bucket seguente nell'editor di policy. *amzn-s3-demo-bucket* Sostituiscilo con il nome del bucket S3 che hai creato. Sostituisci *account_ID_number* con un Account AWS numero ID valido.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSMBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    },
    {
      "Sid": "SSMBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*/*accountid=111122223333/*",
        "arn:aws:s3:::amzn-s3-demo-bucket/*/*accountid=444455556666/*",
        "arn:aws:s3:::amzn-s3-demo-bucket/*/*accountid=123456789012/*",
        "arn:aws:s3:::amzn-s3-demo-bucket/*/*accountid=777788889999/*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
```

```
    "aws:SourceArn": "arn:aws:ssm:*:111122223333:resource-  
data-sync/*"  
  }  
}  
]  
}
```

5. Salvare le modifiche.

Crea una Resource Data Sync per Inventory

Utilizza la procedura seguente per creare un Resource Data Sync per Inventory di Systems Manager utilizzando la console Systems Manager. Per informazioni su come creare una sincronizzazione dei dati delle risorse utilizzando il AWS CLI, vedere [Utilizzo di AWS CLI per configurare la raccolta dei dati di inventario](#).

Come creare una sincronizzazione dei dati delle risorse

1. Aprire la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Nel menu Gestione dell'account, scegli Sincronizzazione dati risorsa.
4. Scegli Crea sincronizzazione dei dati di risorsa.
5. Nel campo Nome di sincronizzazione, inserisci un nome per la configurazione di sincronizzazione.
6. Nel campo Nome bucket, inserire il nome del bucket Amazon S3 creato utilizzando la procedura Creazione e configurazione di un bucket Amazon S3 per la sincronizzazione dati risorsa.
7. (Facoltativo) Nel campo Prefisso bucket, inserisci il nome di un prefisso del bucket Amazon S3 (sottodirectory).
8. Nel campo Regione bucket, scegli Questa Regione, se il bucket Amazon S3 creato si trova nella Regione AWS attuale. Se il bucket si trova in un'altra Regione AWS, scegli Altra Regione e digita il nome della Regione.

Note

Se la sincronizzazione e il bucket Amazon S3 di destinazione si trovano in regioni diverse, potrebbero essere applicati i prezzi per il trasferimento dei dati. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

9. (Facoltativo) Nel campo ARN chiave KMS, digita o incolla un ARN della chiave KMS per crittografare i dati di inventario in Amazon S3.
10. Scegli Create (Crea).

Per sincronizzare i dati di inventario di più dati Regioni AWS, è necessario creare una sincronizzazione dei dati delle risorse in ogni regione. Ripeti questa procedura in ogni Regione AWS punto in cui desideri raccogliere i dati di inventario e inviarli al bucket centrale Amazon S3. Quando si crea la sincronizzazione per ciascuna regione, specificare il bucket Amazon S3 centralizzato nel campo Nome bucket. Quindi utilizzare l'opzione Regione bucket per scegliere la Regione in cui è stato creato il bucket Amazon S3 centralizzato, come illustrato nella schermata seguente. Alla successiva esecuzione dell'associazione per raccogliere i dati di inventario, Systems Manager archivia i dati nel bucket Amazon S3 centralizzato.

Resource data sync

Sync name
TestSync
Sync name can be between 1 and 64 characters

Bucket name
Type a name of a bucket in S3.
MyCentralInventoryBucketForRDS
Bucket name can be between 3 and 63 characters. See [Amazon S3 naming convention](#).

Bucket prefix - *optional*
Type a prefix for the bucket that receives the output.

Bucket region
The region of a bucket in Amazon S3
☐ This region (us-east-2)
☒ Another region
US East (Ohio)

Creazione di una sincronizzazione dei dati delle risorse di inventario per gli account definiti in AWS Organizations

Puoi sincronizzare i dati di inventario da quelli Account AWS definiti in AWS Organizations a un bucket Amazon S3 centrale. Dopo aver completato le procedure seguenti, i dati dell'inventario

vengono sincronizzati con i singoli prefissi chiave Amazon S3 nel bucket centrale. Ogni key prefix rappresenta un ID diverso Account AWS .

Prima di iniziare

Prima di iniziare, verifica di aver configurato e configurato Account AWS in AWS Organizations. Per ulteriori informazioni, consulta [nella Guida per l'utente di AWS Organizations](#) .

Inoltre, tieni presente che devi creare la sincronizzazione dei dati delle risorse basata sull'organizzazione per ciascuna Regione AWS e Account AWS definita in. AWS Organizations

Creazione di un bucket Amazon S3 centralizzato

Utilizza la procedura seguente per creare un bucket Amazon S3 centralizzato per archiviare i dati di inventario aggregati. La procedura descrive come assegnare la policy di bucket che consente a Systems Manager di scrivere i dati di inventario nel bucket dal tuo ID account AWS Organizations . Se si dispone già di un bucket Amazon S3 che si desidera utilizzare per aggregare i dati di inventario per la sincronizzazione dati risorsa, è necessario configurare il bucket per utilizzare la policy nella procedura seguente.

Per creare e configurare un bucket Amazon S3 per la sincronizzazione dei dati delle risorse per più account definiti in AWS Organizations

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Creare un bucket in cui archiviare i dati di inventario aggregati. Per ulteriori informazioni, consulta [Creazione di un bucket](#) nella Guida per l'utente di Amazon Simple Storage Service. Prendi nota del nome del bucket e del Regione AWS luogo in cui lo hai creato.
3. Scegli la scheda Autorizzazioni e quindi Policy (Policy di bucket.
4. Copia e incolla la policy di bucket seguente nell'editor di policy. Sostituisci *amzn-s3-demo-bucket* e *organization-id* con il nome del bucket Amazon S3 che hai creato e un ID account valido AWS Organizations .

Facoltativamente, sostituirlo *bucket-prefix* con il nome di un prefisso Amazon S3 (sottodirectory). Se non hai creato un prefisso, rimuovi *bucket-prefix* dall'ARN nella seguente politica.

JSON

```
{
```



```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "SSMBucketPermissionsCheck",
    "Effect": "Allow",
    "Principal": {
      "Service": "ssm.amazonaws.com"
    },
    "Action": "s3:GetBucketAcl",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
  },
  {
    "Sid": "SSMBucketDelivery",
    "Effect": "Allow",
    "Principal": {
      "Service": "ssm.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/bucket-prefix/*/accountid=*"
    ],
    "Condition": {
      "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control",
        "aws:SourceOrgID": "organization-id"
      }
    }
  },
  {
    "Sid": "SSMBucketDeliveryTagging",
    "Effect": "Allow",
    "Principal": {
      "Service": "ssm.amazonaws.com"
    },
    "Action": "s3:PutObjectTagging",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/bucket-prefix/*/accountid=*"
    ]
  }
]
}

```

Crea una sincronizzazione dei dati delle risorse di inventario per gli account definiti in AWS Organizations

La procedura seguente descrive come utilizzare la AWS CLI per creare una sincronizzazione dei dati delle risorse per gli account definiti in AWS Organizations. È necessario utilizzare il AWS CLI per eseguire questa operazione. È inoltre necessario eseguire questa procedura per ogni Regione AWS elemento Account AWS definito in AWS Organizations.

Per creare una sincronizzazione dei dati delle risorse per un account definito in AWS Organizations (AWS CLI)

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Esegui il comando seguente per accertarti di non disporre di sincronizzazioni di dati della risorsa basata su AWS Organizations. Puoi avere più sincronizzazioni standard, incluse più sincronizzazioni standard e una Organizations-based sincronizzazione. Tuttavia, puoi sincronizzare i dati di una sola Organizations-based risorsa.

```
aws ssm list-resource-data-sync
```

Se il comando restituisce la sincronizzazione dei dati di altre Organizations-based risorse, è necessario eliminarle o scegliere di non crearne una nuova.

3. Eseguire il comando seguente per creare una sincronizzazione dei dati delle risorse per un account definito in AWS Organizations. Per amzn-s3-demo-bucket, specificare il nome del bucket Amazon S3 creato in precedenza in questo argomento. Se hai creato un prefisso (sottodirectory) per il tuo bucket, specifica queste informazioni per. *prefix-name*

```
aws ssm create-resource-data-sync --sync-name name --s3-destination "BucketName=amzn-s3-demo-bucket,Prefix=prefix-name,SyncFormat=JsonSerDe,Region=Regione AWS, for example us-east-2,DestinationDataSharing={DestinationDataSharingType=Organization}"
```

4. Ripeti i passaggi 2 e 3 per ogni Regione AWS Account AWS punto in cui desideri sincronizzare i dati con il bucket Amazon S3 centrale.

Gestione delle sincronizzazioni dei dati della risorsa

Ciascuno Account AWS può avere 5 sincronizzazioni di dati di risorse per persona. Regione AWS
Puoi utilizzare la console AWS Systems Manager Fleet Manager per gestire le sincronizzazioni dei dati della risorsa.

Per visualizzare le sincronizzazioni dei dati della risorsa

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Nel menu a discesa Gestione account, scegli Sincronizzazione dati risorsa.
4. Seleziona una sincronizzazione dei dati della risorsa dalla tabella, quindi scegli Visualizza dettagli per visualizzare le informazioni sulla sincronizzazione dei dati della risorsa.

Come eliminare una sincronizzazione dei dati delle risorse

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Nel menu a discesa Gestione account, scegli Sincronizzazione dati risorsa.
4. Seleziona una sincronizzazione dei dati della risorsa dalla tabella, quindi scegli Elimina.

Utilizzo EventBridge per monitorare gli eventi dell'inventario

Puoi configurare una regola in Amazon EventBridge per creare un evento in risposta alle modifiche dello stato delle risorse di AWS Systems Manager Inventory. EventBridge supporta eventi per le seguenti modifiche allo stato dell'inventario. Tutti gli eventi vengono emessi in base al miglior tentativo.

Tipo di inventario personalizzato eliminato per un'istanza specifica: se una regola è configurata per monitorare questo evento, EventBridge crea un evento quando viene eliminato un tipo di inventario personalizzato su uno specifico gestore. EventBridge invia un evento per nodo per tipo di inventario personalizzato. Di seguito è riportato un modello di evento di esempio.

```
{
```

```

    "timestampMillis": 1610042981103,
    "source": "SSM",
    "account": "123456789012",
    "type": "INVENTORY_RESOURCE_STATE_CHANGE",
    "startTime": "Jan 7, 2021 6:09:41 PM",
    "resources": [
      {
        "arn": "arn:aws:ssm:us-east-1:123456789012:managed-instance/i-12345678"
      }
    ],
    "body": {
      "action-status": "succeeded",
      "action": "delete",
      "resource-type": "managed-instance",
      "resource-id": "i-12345678",
      "action-reason": "",
      "type-name": "Custom:MyCustomInventoryType"
    }
  }
}

```

Evento di eliminazione del tipo di inventario personalizzato per tutte le istanze: se una regola è configurata per monitorare questo evento, EventBridge crea un evento quando viene eliminato un tipo di inventario personalizzato per tutti i nodi gestiti. Di seguito è riportato un modello di evento di esempio.

```

{
  "timestampMillis": 1610042904712,
  "source": "SSM",
  "account": "123456789012",
  "type": "INVENTORY_RESOURCE_STATE_CHANGE",
  "startTime": "Jan 7, 2021 6:08:24 PM",
  "resources": [

  ],
  "body": {
    "action-status": "succeeded",
    "action": "delete-summary",
    "resource-type": "managed-instance",
    "resource-id": "",
    "action-reason": "The delete for type name Custom:SomeCustomInventoryType
was completed. The deletion summary is: {\"totalCount\":1,\"remainingCount\":0,
\"summaryItems\": [{\"version\": \"1.1\", \"count\": 1, \"remainingCount\": 0}]",
    "type-name": "Custom:MyCustomInventoryType"
  }
}

```

```
}  
}
```

[PutInventory](#) chiamata con un evento della versione precedente dello schema: se una regola è configurata per monitorare questo evento, EventBridge crea un evento quando viene effettuata una PutInventory chiamata che utilizza una versione dello schema precedente allo schema corrente. Questo evento si applica a tutti i tipi di inventario. Di seguito è riportato un modello di evento di esempio.

```
{  
  "timestampMillis": 1610042629548,  
  "source": "SSM",  
  "account": "123456789012",  
  "type": "INVENTORY_RESOURCE_STATE_CHANGE",  
  "startTime": "Jan 7, 2021 6:03:49 PM",  
  "resources": [  
    {  
      "arn": "arn:aws:ssm:us-east-1:123456789012:managed-instance/i-12345678"  
    }  
  ],  
  "body": {  
    "action-status": "failed",  
    "action": "put",  
    "resource-type": "managed-instance",  
    "resource-id": "i-01f017c1b2efbe2bc",  
    "action-reason": "The inventory item with type name  
Custom:MyCustomInventoryType was sent with a disabled schema verison 1.0. You must  
send a version greater than 1.0",  
    "type-name": "Custom:MyCustomInventoryType"  
  }  
}
```

Per informazioni su come EventBridge configurare il monitoraggio di questi eventi, vedere [Configurazione EventBridge per gli eventi di Systems Manager](#).

Configurazione della raccolta dell'inventario

Questa sezione descrive come configurare la raccolta AWS Systems Manager dell'inventario su uno o più nodi gestiti utilizzando la console Systems Manager. Per un esempio di come configurare la raccolta dell'inventario utilizzando AWS Command Line Interface (AWS CLI), vedere [Utilizzo di AWS CLI per configurare la raccolta dei dati di inventario](#).

Quando si configura la raccolta dell'inventario, si inizia creando un' AWS Systems Manager State Manager associazione. Systems Manager raccoglie i dati di inventario quando viene eseguita l'associazione. Se non si crea prima l'associazione e si tenta di richiamare il `aws:softwareInventory` plug-in utilizzando, ad esempio AWS Systems Manager Run Command, il sistema restituisce il seguente errore: `The aws:softwareInventory plugin can only be invoked through ssm-associate.`

Note

Tenere presente il comportamento seguente se si creano più associazioni di inventario per un nodo gestito.

- A ogni nodo può essere assegnata un'associazione di inventario destinata a tutti i nodi (--targets «Key=InstanceIds, Values=*»).
- A ogni nodo può essere assegnata anche un'associazione specifica che utilizza key/value coppie di tag o un gruppo di risorse. AWS
- Se a un nodo vengono assegnate più associazioni d'inventario, lo stato mostra Saltato per l'associazione che non è stata eseguita. L'associazione eseguita più di recente visualizza lo stato effettivo dell'associazione d'inventario.
- Se a un nodo vengono assegnate più associazioni di inventario e ciascuna utilizza una key/value coppia di tag, tali associazioni di inventario non vengono eseguite sul nodo a causa del conflitto di tag. L'associazione viene ancora eseguita sui nodi che non presentano il key/value conflitto di tag.

Prima di iniziare

Prima di configurare la raccolta dell'inventario, completa le seguenti attività.

- Aggiornamento AWS Systems Manager SSM Agent sui nodi di cui desideri creare l'inventario. Eseguendo la versione più recente di SSM Agent, ti assicuri di poter raccogliere i metadati per tutti i tipi di inventario supportati. Per informazioni su come aggiornare l'SSM Agent mediante State Manager, consulta [Procedura dettagliata: aggiorna SSM Agent automaticamente con AWS CLI](#).
- Verifica di aver completato i requisiti di configurazione per le istanze Amazon Elastic Compute Cloud (Amazon EC2) e le macchine non EC2 in un ambiente [ibrido e multicloud](#). Per informazioni, consulta [Configurazione dei nodi gestiti per AWS Systems Manager](#).

- Per Windows Server i nodi Microsoft, verifica che il nodo gestito sia configurato con Windows PowerShell 3.0 (o successivo). SSM Agent utilizza il `ConvertTo-Json` cmdlet in PowerShell per convertire i dati di inventario di Windows Update nel formato richiesto.
- (Facoltativo) Crea una sincronizzazione dati risorsa per archiviare centralmente i dati dell'inventario in un bucket Amazon S3. La sincronizzazione dati risorsa aggiorna automaticamente i dati centralizzati quando vengono raccolti nuovi dati dell'inventario. Per ulteriori informazioni, consulta [Procedura dettagliata: utilizzo di sincronizzazione dati risorsa per aggregare dati di inventario](#).
- (Facoltativo) Crea un file JSON per raccogliere un inventario personalizzato. Per ulteriori informazioni, consulta [Utilizzo di inventari personalizzati](#).

Fai l'inventario di tutti i nodi gestiti nel tuo Account AWS

Puoi fare l'inventario di tutti i nodi gestiti del tuo sistema Account AWS creando un'associazione globale di inventario. Un'associazione di inventario globale effettua le seguenti operazioni:

- Applica automaticamente la configurazione globale dell'inventario (associazione) a tutti i nodi gestiti esistenti nel tuo Account AWS. I nodi gestiti che dispongono già di un'associazione di inventario vengono ignorate quando l'associazione di inventario globale viene applicata ed è in esecuzione. Quando un nodo viene saltato, il messaggio di stato dettagliato indica `Overridden By Explicit Inventory Association`. Questi nodi vengono ignorate dall'associazione globale, ma continueranno a riportare l'inventario quando eseguono l'associazione di inventario a esse assegnata.
- Aggiunge automaticamente i nuovi nodi creati nella tua Account AWS associazione di inventario globale.

Note

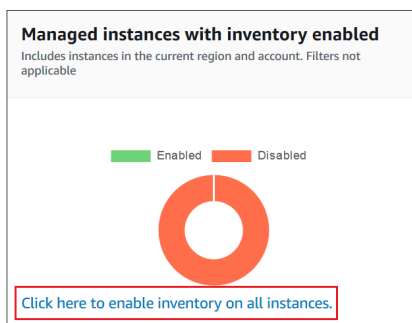
- Se un nodo gestito è configurato per l'associazione di inventario globale e gli viene assegnata un'associazione specifica, l'inventario di Systems Manager declassa l'associazione globale e applica l'associazione specifica.
- Le associazioni di inventario globale sono disponibili in SSM Agent 2.0.790.0 o versione successiva. Per informazioni su come aggiornare l'SSM Agent sui tuoi nodi, consulta [Aggiornamento di SSM Agent utilizzando Run Command](#).

Configurazione della raccolta dell'inventario con un solo clic (console)

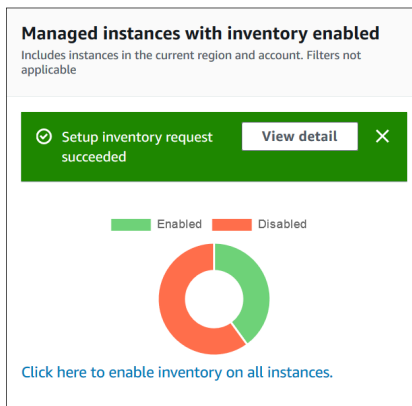
Usa la seguente procedura per configurare Systems Manager Inventory per tutti i nodi gestiti nel tuo Account AWS e in un unico Regione AWS.

Per configurare tutti i nodi gestiti nella Regione corrente per l'inventario Systems Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel riquadro di navigazione, seleziona Inventario.
3. Nella scheda Istanze gestite con inventario abilitato, scegli Fai clic qui per abilitare l'inventario in tutte le istanze.



Se l'esito è positivo, la console mostra il seguente messaggio.



A seconda del numero di nodi gestiti nel tuo account, l'applicazione dell'associazione dell'inventario globale può richiedere alcuni minuti. Attendi qualche minuto, quindi aggiorna la pagina. Verifica che l'immagine cambi per confermare il completamento della configurazione dell'inventario in tutti i nodi gestiti.

Configurazione della raccolta con la console

Questa sezione include informazioni su come configurare l'inventario di Systems Manager per raccogliere metadati dai tuoi nodi gestiti utilizzando la console Systems Manager. Puoi raccogliere rapidamente i metadati da tutti i nodi di uno specifico Account AWS (e da tutti i nodi futuri che potrebbero essere creati in quell'account) oppure puoi raccogliere selettivamente i dati di inventario utilizzando tag o ID di nodo.

Note

Prima di completare questa procedura, verifica se esiste già un'associazione di inventario globale. Se esiste già un'associazione di inventario globale, ogni volta che avvii una nuova istanza, l'associazione viene applicata all'istanza e la nuova istanza viene inserita nell'inventario.

Per configurare la raccolta dell'inventario

1. Apri la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel riquadro di navigazione, seleziona Inventario.
3. Scegli Configura inventario.
4. Nella sezione Destinazioni, identifica i nodi in cui si desidera eseguire questa operazione scegliendo una delle seguenti opzioni.
 - Selezione di tutte le istanze gestite in questo account: questa opzione seleziona tutti i nodi gestiti per le quali non esiste alcuna associazione di inventario. Se si sceglie questa opzione, i nodi che presentano già associazioni di inventario vengono ignorate durante la raccolta dell'inventario e vengono visualizzate con lo stato Ignorato nei risultati dell'inventario. Per ulteriori informazioni, consulta [Fai l'inventario di tutti i nodi gestiti nel tuo Account AWS](#).
 - Specifica di un tag): utilizza questa opzione per specificare un singolo tag per identificare i nodi del proprio account da cui raccogliere l'inventario. Se si utilizza un tag, tutti i nodi create in futuro con lo stesso tag verranno riportate nell'inventario. Se esiste un'associazione di inventario con tutti i nodi, utilizzando un tag per selezionare nodi specifici come destinazione per un altro inventario, l'appartenenza dei nodi viene sostituita nel gruppo di destinazione Tutte le istanze gestite. I nodi gestiti con il tag specificato vengono ignorati nella futura raccolta dell'inventario da Tutte le istanze gestite.

- **Selezione manuale delle istanze:** utilizza questa opzione per scegliere specifici nodi gestiti nel tuo account. Scegliendo esplicitamente nodi specifici mediante questa opzione vengono sostituite le associazioni di inventario nella destinazione Tutte le istanze gestite. Il nodo viene ignorato nella futura raccolta dell'inventario da Tutte le istanze gestite.

 Note

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

5. Nella sezione Pianificazione, scegli la frequenza alla quale desideri che il sistema raccolga metadati di inventario dai tuoi nodi.
6. Nella sezione Parametri, utilizza gli elenchi per attivare/disattivare vari tipi di raccolte di inventario. Per ulteriori informazioni sulla raccolta dell'inventario dei file e del registro di sistema di Windows, consulta [Utilizzo dell'inventario dei file e del registro di sistema di Windows](#).
7. Nella sezione Avanzate, scegli Sincronizza i log di esecuzione dell'inventario in un bucket Amazon S3, se si desidera memorizzare lo stato di esecuzione dell'associazione in un bucket Amazon S3.
8. Scegli Configura inventario. Systems Manager crea un'associazione State Manager ed esegue immediatamente l'inventario sui nodi.
9. Nel pannello di navigazione, scegli State Manager. Verificare che sia stata creata una nuova associazione che utilizza il documento **AWS-GatherSoftwareInventory**. La pianificazione dell'associazione utilizza un'espressione della frequenza. Inoltre, verifica che il campo Stato indichi Completato. Se si sceglie l'opzione Sincronizza i log di esecuzione dell'inventario in un bucket Amazon S3), sarà possibile visualizzare il log dei dati in Amazon S3 dopo qualche minuto. Se desideri visualizzare i dati dell'inventario per un determinato nodo, scegliere Istanze gestite nel pannello di navigazione.
10. Scegli un nodo, quindi scegli Mostra dettagli.
11. Nella pagina dei dettagli del nodo, scegli Inventario. Utilizza gli elenchi Tipo di inventario per filtrare l'inventario.

Esecuzione di query sui dati di inventario da più regioni e account

AWS Systems Manager Inventory si integra con Amazon Athena per aiutarti a interrogare i dati di inventario da più e. Regioni AWS Account AWS L'integrazione con Athena utilizza la sincronizzazione dei dati delle risorse in modo da poter visualizzare i dati di inventario di tutti i nodi gestiti nella pagina di visualizzazione dettagliata della console. AWS Systems Manager

Important

Questa funzionalità consente AWS Glue di eseguire la scansione dei dati nel bucket Amazon Simple Storage Service (Amazon S3) e in Amazon Athena per interrogarli. A seconda della quantità di dati su cui vengono eseguiti il crawling e le query, ti può essere addebitato l'utilizzo di questi servizi. Con AWS Glue, paghi una tariffa oraria, fatturata al secondo, per i crawler (individuazione dei dati) e per i lavori ETL (elaborazione e caricamento dei dati). Con Athena, i costi addebitati dipendono dalla quantità di dati scansionati da ciascuna query. Ti consigliamo di prendere visione delle linee guida in materia di prezzi per tali servizi prima di utilizzare l'integrazione di Amazon Athena con l'inventario di Systems Manager. Per ulteriori dettagli, consulta [Prezzi di Amazon Athena](#) e [AWS Glue Prezzi](#).

Puoi visualizzare i dati di inventario nella pagina Detailed View (Visualizzazione dettagliata) in tutte le Regioni AWS in cui è disponibile Amazon Athena. Per un elenco delle regioni supportate, consulta [Endpoint del servizio Amazon Athena](#) in Riferimenti generali di Amazon Web Services.

Prima di iniziare

L'integrazione di Athena utilizza Resource Data Sync. Devi impostare e configurare Resource Data Sync per l'utilizzo di questa funzionalità. Per ulteriori informazioni, consulta [Procedura dettagliata: utilizzo di sincronizzazione dati risorsa per aggregare dati di inventario](#).

Inoltre, tieni presente che la pagina Visualizzazione dettagliata mostra i dati di inventario per il proprietario del bucket Amazon S3 centralizzato utilizzato da Sincronizzazione dati risorsa. Se non sei il proprietario del bucket Amazon S3 centralizzato, non puoi visualizzare i dati di inventario nella pagina Visualizzazione dettagliata.

Configurazione dell'accesso

Per poter eseguire query e visualizzare i dati da più account e Regioni nella pagina Visualizzazione dettagliata nella console Systems Manager, devi prima configurare l'entità IAM con l'autorizzazione alla visualizzazione dei dati.

Se i dati dell'inventario sono archiviati in un bucket Amazon S3 che utilizza la crittografia AWS Key Management Service (AWS KMS), devi anche configurare la tua entità IAM e il ruolo del Amazon-`GlueServiceRoleForSSM` servizio per AWS KMS la crittografia.

Argomenti

- [Configurazione dell'entità IAM per accedere alla pagina Visualizzazione dettagliata](#)
- [\(Facoltativo\) Configurare le autorizzazioni per la visualizzazione AWS KMS Dati crittografati](#)

Configurazione dell'entità IAM per accedere alla pagina Visualizzazione dettagliata

Di seguito vengono descritte le autorizzazioni minime necessarie per visualizzare i dati di inventario nella pagina Visualizzazione dettagliata.

La policy gestita di **AWSQuicksightAthenaAccess**

Il seguente `PassRole` e altri blocchi di autorizzazioni obbligatorie

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowGlue",
      "Effect": "Allow",
      "Action": [
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetTables",
        "glue:StartCrawler",
        "glue:CreateCrawler"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": [
        "arn:aws:iam::111122223333:role/SSMInventoryGlueRole",
```

```

        "arn:aws:iam::111122223333:role/SSMInventoryServiceRole"
    ],
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "glue.amazonaws.com"
        }
    }
},
{
    "Sid": "iamRoleCreation",
    "Effect": "Allow",
    "Action": [
        "iam:CreateRole",
        "iam:AttachRolePolicy"
    ],
    "Resource": "arn:aws:iam::111122223333:role/*"
},
{
    "Sid": "iamPolicyCreation",
    "Effect": "Allow",
    "Action": "iam:CreatePolicy",
    "Resource": "arn:aws:iam::111122223333:policy/*"
}
]
}

```

(Facoltativo) Se il bucket Amazon S3 utilizzato per archiviare i dati di inventario è crittografato utilizzando AWS KMS, devi anche aggiungere il seguente blocco alla policy.

```

{
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": [
        "arn:aws:kms:Region:account_ID:key/key_ARN"
    ]
}

```

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.

(Facoltativo) Configurare le autorizzazioni per la visualizzazione AWS KMS Dati crittografati

Se il bucket Amazon S3 utilizzato per archiviare i dati di inventario è crittografato utilizzando AWS Key Management Service (AWS KMS), devi configurare la tua entità IAM e il `AmazonGlueServiceRoleForSSM` ruolo con le `kms:Decrypt` autorizzazioni per la chiave AWS KMS

Prima di iniziare

Per fornire le `kms:Decrypt` autorizzazioni per la AWS KMS chiave, aggiungi il seguente blocco di policy alla tua entità IAM:

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt"
  ],
  "Resource": [
    "arn:aws:kms:Region:account_ID:key/key_ARN"
  ]
}
```

Se non l'hai già fatto, completa la procedura e aggiungi `kms:Decrypt` le autorizzazioni per la AWS KMS chiave.

Utilizza la procedura seguente per configurare il `Amazon-GlueServiceRoleForSSM` ruolo con le `kms:Decrypt` autorizzazioni per la AWS KMS chiave.

Per configurare `Amazon-GlueServiceRoleForSSM` ruolo con `KMS:Decrypt` permissions

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, scegli `Ruoli`, quindi utilizza il campo di ricerca per individuare il ruolo. `Amazon-GlueServiceRoleForSSM` Viene visualizzata la pagina Riepilogo.
3. Usa il campo di ricerca per trovare il `Amazon-GlueServiceRoleForSSM` ruolo. Scegli il nome del ruolo. Viene visualizzata la pagina Riepilogo.
4. Scegli il nome del ruolo. Viene visualizzata la pagina Riepilogo.
5. Scegli `Aggiungi policy in linea`. Viene visualizzata la pagina `Crea policy`.
6. Scegli la scheda `JSON`.
7. Elimina il testo JSON esistente nell'editor, quindi copia e incolla la seguente policy nell'editor JSON.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/key_ARN"
      ]
    }
  ]
}
```

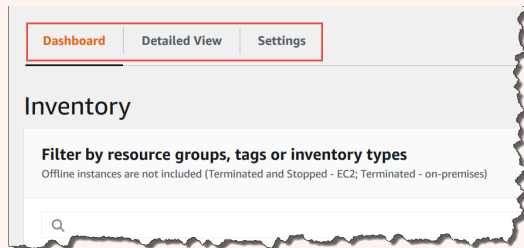
8. Scegli `Esamina policy`.
9. Nella pagina `Rivedi policy`, immetti un nome nel campo `Nome`.
10. Scegli `Crea policy`.

Interrogazione dei dati nella pagina di visualizzazione dettagliata inventario

Utilizzare la procedura seguente per visualizzare i dati di inventario provenienti da più Regioni AWS e nella Account AWS pagina di visualizzazione dettagliata dell'inventario di Systems Manager.

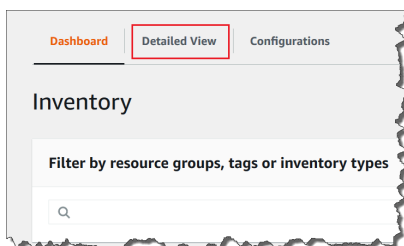
Important

La pagina Visualizzazione dettagliata di Inventario è disponibile solo in Regioni AWS che offrono Amazon Athena. Se le seguenti schede non sono visualizzate nella pagina dell'inventario di Systems Manager, significa che Athena non è disponibile nella Regione e non è possibile utilizzare la funzione Visualizzazione dettagliata per eseguire query sui dati.

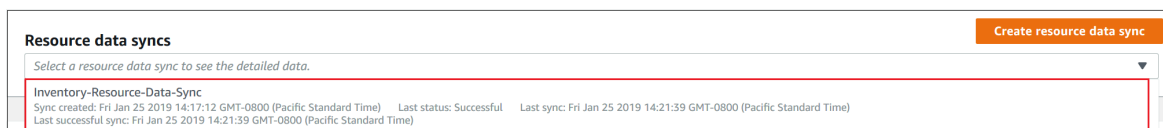


Per visualizzare i dati di inventario di più regioni e account nel AWS Systems Manager console

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel riquadro di navigazione, seleziona Inventario.
3. Scegli la scheda Visualizzazione dettagliata.



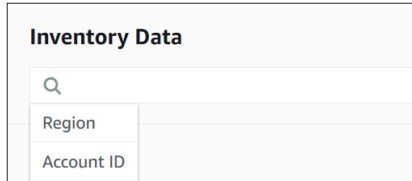
4. Scegli Sincronizzazione dati risorsa per cui eseguire query sui dati.



5. Nell'elenco Tipo di inventario, scegli il tipo di dati di inventario su cui eseguire query, quindi premi Enter.



6. Per filtrare i dati, scegli la barra Filtro, quindi seleziona un'opzione del filtro.



Puoi utilizzare il pulsante Esporta in formato CSV per visualizzare l'attuale set di query in un'applicazione per fogli di calcolo come Microsoft Excel. Puoi anche utilizzare i pulsanti Cronologia delle query ed Esegui query avanzate per visualizzare i dettagli della cronologia e interagire con i tuoi dati in Amazon Athena.

Modificare il AWS Glue pianificazione del crawler

AWS Glue per impostazione predefinita, esegue la scansione dei dati di inventario nel bucket centrale di Amazon S3 due volte al giorno. Se modifichi frequentemente i tipi di dati da raccogliere sui tuoi nodi, puoi eseguire il crawling dei dati con una frequenza maggiore, come descritto nella procedura seguente.

Important

AWS Glue ti addebita in Account AWS base a una tariffa oraria, fatturata al secondo, per i crawler (individuazione dei dati) e i lavori ETL (elaborazione e caricamento dei dati). Prima di modificare la pianificazione del crawler, visualizza la pagina [Prezzi di AWS Glue](#).

Per modificare la pianificazione del crawler dei dati di inventario

1. Apri la console all'indirizzo. AWS Glue <https://console.aws.amazon.com/glue/>
2. Nel riquadro di navigazione, selezionare Crawler.
3. Nell'elenco dei crawler, scegliere l'opzione accanto al crawler dei dati dell'inventario di Systems Manager. Il nome del crawler utilizza il seguente formato:

AWSSystemsManager-*s3-bucket-name-Region-account_ID*

4. Scegli Operazione, quindi Modifica crawler.
5. Nel riquadro di navigazione, seleziona Pianifica.
6. Nel campo Espressione Cron, specifica una nuova pianificazione utilizzando un formato cron. Per ulteriori informazioni sul formato cron, consulta [Time-Based Schedules for Jobs and Crawlers](#) nella Developer Guide. AWS Glue

 Important

Puoi mettere in pausa il crawler per evitare di incorrere in addebiti da AWS Glue. Se si sospende il crawler o si modifica la frequenza in modo che venga eseguito meno spesso il crawling dei dati, la pagina Visualizzazione dettagliata dell'inventario potrebbe visualizzare dati non aggiornati.

Esecuzione di query su una raccolta di inventario mediante filtri

Dopo aver raccolto i dati di inventario, puoi utilizzare le funzionalità di filtro AWS Systems Manager per interrogare i nodi gestiti che soddisfano determinati criteri di filtro.

Per eseguire query sui nodi in base ai filtri di inventario

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel riquadro di navigazione, seleziona Inventario.
3. Nella sezione Filter by resource groups, tags or inventory types (Filtra per gruppi di risorse, tag o tipi di inventario), scegliere la casella di filtro. Viene visualizzato un elenco di filtri predefiniti.
4. Scegliere un attributo a cui applicare il filtro. Ad esempio, scegli **AWS:Application**. Se richiesto, scegliere un attributo secondario da filtrare. Ad esempio, scegli **AWS:Application.Name**.
5. Scegliere un delimitatore dall'elenco. Ad esempio, scegliere Begin with (Inizia per). Viene visualizzata una casella di testo nel filtro.
6. Inserire un valore nella casella di testo. Ad esempio, inserire Amazon (SSM Agent è denominato Amazon SSM Agent).
7. Premi Enter. Il sistema restituisce un elenco di nodi gestiti che include il nome di un'applicazione che inizia con la parola Amazon.

 Note

È possibile combinare più filtri per perfezionare la ricerca.

Aggregazione dei dati di inventario

Dopo aver configurato i nodi gestiti per AWS Systems Manager Inventory, puoi visualizzare i conteggi aggregati dei dati di inventario. Ad esempio, supponi di aver configurato decine o centinaia di nodi gestiti per raccogliere il tipo di inventario `AWS:Application`. Utilizzando le informazioni contenute in questa sezione, puoi visualizzare il numero esatto di nodi configurati per raccogliere questi dati.

Puoi anche visualizzare dettagli di Inventory specifici aggregando un tipo di dati. Ad esempio, il tipo di inventario `AWS:InstanceInformation` raccoglie informazioni sulla piattaforma del sistema operativo con il tipo di dati `Platform`. Aggregando i dati nel tipo di dati `Platform`, puoi visualizzare rapidamente quanti nodi eseguono Windows Server, quanti eseguono Linux e macOS.

Le procedure in questa sezione descrivono come visualizzare i conteggi aggregati dei dati di inventario utilizzando AWS Command Line Interface (AWS CLI). Puoi anche visualizzare i conteggi aggregati preconfigurati nella AWS Systems Manager console nella pagina *Inventario*. Questi pannelli di controllo preconfigurati sono denominati informazioni di inventario e offrono sistemi di correzione con un solo clic per i problemi di configurazione di Inventory.

Nota i seguenti dettagli importanti relativi ai conteggi di aggregazione dei dati di Inventory:

- Se si chiude un nodo gestito per la raccolta dei dati di inventario, Systems Manager conserva i dati di inventario per 30 giorni, quindi li elimina. Per i nodi in esecuzione, il sistema elimina i dati di inventario con più di 30 giorni. Se devi archiviare i dati di inventario per più di 30 giorni, puoi utilizzarli AWS Config per registrare la cronologia o interrogare e caricare periodicamente i dati in un bucket Amazon Simple Storage Service (Amazon S3).
- Se un nodo è stato configurato in precedenza per riportare un determinato tipo di dati di Inventory, ad esempio `AWS:Network`, e in seguito decidi di modificare la configurazione per interrompere la raccolta di quel tipo di dati, i conteggi di aggregazione mostreranno ancora i dati `AWS:Network` finché il nodo non verrà terminato e non saranno passati 30 giorni.

Per informazioni su come configurare e raccogliere rapidamente i dati di inventario da tutti i nodi di uno specifico Account AWS (e da eventuali nodi futuri che potrebbero essere creati in quell'account), consulta [Fai l'inventario di tutti i nodi gestiti nel tuo Account AWS](#)

Argomenti

- [Aggregazione dei dati di inventario per visualizzare il numero di nodi che raccolgono specifici tipi di dati](#)
- [Aggregazione dei dati di inventario con i gruppi per vedere i nodi configurate o non configurate per raccogliere un tipo di inventario](#)

Aggregazione dei dati di inventario per visualizzare il numero di nodi che raccolgono specifici tipi di dati

Puoi utilizzare l'operazione AWS Systems Manager [GetInventory](#) API per visualizzare i conteggi aggregati dei nodi che raccolgono uno o più tipi di inventario e tipi di dati. Ad esempio, il tipo di `AWS:InstanceInformation` inventario consente di visualizzare un aggregato di sistemi operativi utilizzando l'operazione `GetInventory` API con il tipo di `AWS:InstanceInformation.PlatformType` dati. Di seguito è riportato un esempio di comando e output AWS CLI :

```
aws ssm get-inventory --aggregators "Expression=AWS:InstanceInformation.PlatformType"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "Entities":[
    {
      "Data":{
        "AWS:InstanceInformation":{
          "Content":[
            {
              "Count":"7",
              "PlatformType":"windows"
            },
            {
              "Count":"5",
              "PlatformType":"linux"
            }
          ]
        }
      }
    }
  ]
}
```

```
}
```

Nozioni di base

Determina i tipi di Inventory e i tipi di dati di cui desideri visualizzare i conteggi. Puoi visualizzare un elenco dei tipi di inventario e dei tipi di dati che supportano l'aggregazione eseguendo questo comando in AWS CLI.

```
aws ssm get-inventory-schema --aggregator
```

Il comando restituisce un elenco JSON dei tipi di Inventory e dei tipi di dati che supportano l'aggregazione. Il `TypeName` campo mostra i tipi di inventario supportati. Il campo `Nome` mostra ogni tipo di dati. Ad esempio, nell'elenco seguente, il tipo di Inventory `AWS:Application` include tipi di dati per `Name` e `Version`.

```
{
  "Schemas": [
    {
      "TypeName": "AWS:Application",
      "Version": "1.1",
      "DisplayName": "Application",
      "Attributes": [
        {
          "DataType": "STRING",
          "Name": "Name"
        },
        {
          "DataType": "STRING",
          "Name": "Version"
        }
      ]
    },
    {
      "TypeName": "AWS:InstanceInformation",
      "Version": "1.0",
      "DisplayName": "Platform",
      "Attributes": [
        {
          "DataType": "STRING",
          "Name": "PlatformName"
        },
        {

```

```

        "DataType": "STRING",
        "Name": "PlatformType"
    },
    {
        "DataType": "STRING",
        "Name": "PlatformVersion"
    }
]
},
{
    "TypeName": "AWS:ResourceGroup",
    "Version": "1.0",
    "DisplayName": "ResourceGroup",
    "Attributes": [
        {
            "DataType": "STRING",
            "Name": "Name"
        }
    ]
},
{
    "TypeName": "AWS:Service",
    "Version": "1.0",
    "DisplayName": "Service",
    "Attributes": [
        {
            "DataType": "STRING",
            "Name": "Name"
        },
        {
            "DataType": "STRING",
            "Name": "DisplayName"
        },
        {
            "DataType": "STRING",
            "Name": "ServiceType"
        },
        {
            "DataType": "STRING",
            "Name": "Status"
        },
        {
            "DataType": "STRING",
            "Name": "StartType"
        }
    ]
}

```

```

        }
      ]
    },
    {
      "TypeName": "AWS:WindowsRole",
      "Version": "1.0",
      "DisplayName": "WindowsRole",
      "Attributes": [
        {
          "DataType": "STRING",
          "Name": "Name"
        },
        {
          "DataType": "STRING",
          "Name": "DisplayName"
        },
        {
          "DataType": "STRING",
          "Name": "FeatureType"
        },
        {
          "DataType": "STRING",
          "Name": "Installed"
        }
      ]
    }
  ]
}

```

Puoi aggregare i dati per tutti i tipi di Inventory elencati creando un comando che utilizzi la sintassi seguente:

```
aws ssm get-inventory --aggregators "Expression=InventoryType.DataType"
```

Ecco alcuni esempi.

Esempio 1

Questo esempio aggrega il conteggio dei ruoli Windows utilizzati dai tuoi nodi.

```
aws ssm get-inventory --aggregators "Expression=AWS:WindowsRole.Name"
```

Esempio 2

Questo esempio aggrega il conteggio delle applicazioni installate nei tuoi nodi.

```
aws ssm get-inventory --aggregators "Expression=AWS:Application.Name"
```

Combinazione di più aggregatori

È possibile anche combinare più tipi di Inventory e tipi di dati in un unico comando per aiutarti a comprendere meglio i dati. Ecco alcuni esempi.

Esempio 1

Questo esempio aggrega il conteggio dei sistemi operativi utilizzati dai tuoi nodi. Restituisce inoltre il nome specifico dei sistemi operativi.

```
aws ssm get-inventory --aggregators '[{"Expression":  
  "AWS:InstanceInformation.PlatformType", "Aggregators":[{"Expression":  
    "AWS:InstanceInformation.PlatformName"}]}]'
```

Esempio 2

Questo esempio aggrega il conteggio delle applicazioni in esecuzione sui tuoi nodi e la versione specifica di ciascuna applicazione.

```
aws ssm get-inventory --aggregators '[{"Expression": "AWS:Application.Name",  
  "Aggregators":[{"Expression": "AWS:Application.Version"}]}]'
```

Se preferisci, puoi creare un'espressione di aggregazione con uno o più tipi di Inventory e tipi di dati in un file JSON e richiamare il file tramite AWS CLI. Il file JSON deve utilizzare la seguente sintassi:

```
[  
  {  
    "Expression": "string",  
    "Aggregators": [  
      {  
        "Expression": "string"  
      }  
    ]  
  }  
]
```

Devi salvare il file con l'estensione .json.

Di seguito è riportato un esempio che utilizza più tipi di Inventory e tipi di dati.

```
[
  {
    "Expression": "AWS:Application.Name",
    "Aggregators": [
      {
        "Expression": "AWS:Application.Version",
        "Aggregators": [
          {
            "Expression": "AWS:InstanceInformation.PlatformType"
          }
        ]
      }
    ]
  }
]
```

Utilizza il comando seguente per richiamare il file tramite AWS CLI.

```
aws ssm get-inventory --aggregators file://file_name.json
```

Il comando restituisce informazioni simili alle seguenti.

```
{
  "Entities": [
    {
      "Data": {
        "AWS:Application": {
          "Content": [
            {
              "Count": "3",
              "PlatformType": "linux",
              "Version": "2.6.5",
              "Name": "audit-libs"
            },
            {
              "Count": "2",
              "PlatformType": "windows",
              "Version": "2.6.5",
              "Name": "audit-libs"
            },
            {
              "Count": "4",
              "PlatformType": "windows",
              "Version": "6.2.8",
              "Name": "microsoft office"
            },
            {
              "Count": "2",
```

```

        "PlatformType": "windows",
        "Version": "2.6.5",
        "Name": "chrome"},
    {"Count": "1",
     "PlatformType": "linux",
     "Version": "2.6.5",
     "Name": "chrome"},
    {"Count": "2",
     "PlatformType": "linux",
     "Version": "6.3",
     "Name": "authconfig"}
  ]
},
"ResourceType": "ManagedInstance"}
]
}

```

Aggregazione dei dati di inventario con i gruppi per vedere i nodi configurate o non configurate per raccogliere un tipo di inventario

I gruppi in Inventory di Systems Manager ti consentono di vedere rapidamente il numero di nodi gestiti che sono o meno configurati per raccogliere uno o più tipi di Inventory. Con i gruppi, devi specificare uno o più tipi di Inventory nonché un filtro che utilizzi l'operatore `exists`.

Ad esempio, supponi di disporre di quattro nodi gestiti, configurati per raccogliere i seguenti tipi di Inventory:

- Nodo 1: `AWS:Application`
- Nodo 2: `AWS:File`
- Nodo 3: `AWS:Application`, `AWS:File`
- Nodo 4: `AWS:Network`

È possibile eseguire il seguente comando da AWS CLI per vedere quanti nodi sono configurati per raccogliere `AWS:Application` sia i `AWS:File` inventory tipi che. La risposta restituisce anche il numero di nodi non configurati per raccogliere questi tipi di Inventory.

```

aws ssm get-inventory --aggregators
  'Groups=[{Name=ApplicationAndFile,Filters=[{Key=TypeName,Values=[AWS:Application],Type=Exists}
{Key=TypeName,Values=[AWS:File],Type=Exists}]]]'

```

La risposta del comando mostra che è configurata un solo nodo gestito per raccogliere entrambi i tipi di Inventory, `AWS:Application` e `AWS:File`.

```
{
  "Entities": [
    {
      "Data": {
        "ApplicationAndFile": {
          "Content": [
            {
              "notMatchingCount": "3"
            },
            {
              "matchingCount": "1"
            }
          ]
        }
      }
    }
  ]
}
```

Note

I gruppi non restituiscono il conteggio dei tipi di dati. Inoltre, non puoi eseguire il drill-down dei risultati per vedere gli ID dei nodi configurate o non configurate per raccogliere il tipo di inventario.

Se preferisci, puoi creare un'espressione di aggregazione con uno o più tipi di Inventory in un file JSON e richiamare il file tramite AWS CLI. Il file JSON deve utilizzare la seguente sintassi:

```
{
  "Aggregators": [
    {
      "Groups": [
        {
          "Name": "Name",
          "Filters": [
            {
              "Key": "TypeName",

```

```

        "Values": [
            "Inventory_type"
        ],
        "Type": "Exists"
    },
    {
        "Key": "TypeName",
        "Values": [
            "Inventory_type"
        ],
        "Type": "Exists"
    }
]
}

```

Devi salvare il file con l'estensione .json.

Utilizza il comando seguente per richiamare il file tramite AWS CLI.

```
aws ssm get-inventory --cli-input-json file://file_name.json
```

Esempi aggiuntivi

I seguenti esempi illustrano come aggregare dati di Inventory per vedere quali nodi gestiti sono o meno configurati per raccogliere i tipi di Inventory specificati. Questi esempi utilizzano AWS CLI. Ogni esempio include un comando completo con filtri, eseguibile dalla riga di comando, e un file di esempio input.json, nel caso tu preferisca inserire le informazioni in un file.

Esempio 1

Questo esempio aggrega il conteggio dei nodi configurate o meno per raccogliere il tipo di Inventory `AWS:Application` oppure `AWS:File`.

Utilizza il comando seguente da AWS CLI.

```
aws ssm get-inventory --aggregators
'Groups=[{Name=ApplicationORFile,Filters=[{Key=TypeName,Values=[AWS:Application,
AWS:File],Type=Exists}]]'
```

Se preferisci utilizzare un file, copia e incolla il seguente esempio in un file e salvalo come input.json.

```
{
  "Aggregators":[
    {
      "Groups":[
        {
          "Name":"ApplicationORFile",
          "Filters":[
            {
              "Key":"TypeName",
              "Values":[
                "AWS:Application",
                "AWS:File"
              ],
              "Type":"Exists"
            }
          ]
        }
      ]
    }
  ]
}
```

Utilizza il comando seguente da AWS CLI.

```
aws ssm get-inventory --cli-input-json file://input.json
```

Il comando restituisce informazioni simili alle seguenti.

```
{
  "Entities":[
    {
      "Data":{
        "ApplicationORFile":{
          "Content":[
            {
              "notMatchingCount":"1"
            },
            {
              "matchingCount":"3"
            }
          ]
        }
      }
    }
  ]
}
```

```

    ]
  }
}
]
}

```

Esempio 2

Questo esempio aggrega il conteggio dei nodi configurati o meno per raccogliere i tipi di inventario `AWS:Application`, `AWS:File` e `AWS:Network`.

Utilizza il comando seguente da AWS CLI.

```

aws ssm get-inventory --aggregators
'Groups=[{Name=Application,Filters=[{Key=TypeName,Values=[AWS:Application],Type=Exists}]},
{Name=File,Filters=[{Key=TypeName,Values=[AWS:File],Type=Exists}]},
{Name=Network,Filters=[{Key=TypeName,Values=[AWS:Network],Type=Exists}]]]'

```

Se preferisci utilizzare un file, copia e incolla il seguente esempio in un file e salvalo come `input.json`.

```

{
  "Aggregators": [
    {
      "Groups": [
        {
          "Name": "Application",
          "Filters": [
            {
              "Key": "TypeName",
              "Values": [
                "AWS:Application"
              ],
              "Type": "Exists"
            }
          ]
        },
        {
          "Name": "File",
          "Filters": [
            {
              "Key": "TypeName",

```

```

        "Values":[
            "AWS:File"
        ],
        "Type":"Exists"
    }
],
{
    "Name":"Network",
    "Filters":[
        {
            "Key":"TypeName",
            "Values":[
                "AWS:Network"
            ],
            "Type":"Exists"
        }
    ]
}
]
}
]
}

```

Utilizza il comando seguente da AWS CLI.

```
aws ssm get-inventory --cli-input-json file://input.json
```

Il comando restituisce informazioni simili alle seguenti.

```

{
  "Entities":[
    {
      "Data":{
        "Application":{
          "Content":[
            {
              "notMatchingCount":"2"
            },
            {
              "matchingCount":"2"
            }
          ]
        }
      }
    }
  ]
}

```

```

    },
    "File":{
      "Content":[
        {
          "notMatchingCount":"2"
        },
        {
          "matchingCount":"2"
        }
      ]
    },
    "Network":{
      "Content":[
        {
          "notMatchingCount":"3"
        },
        {
          "matchingCount":"1"
        }
      ]
    }
  }
}

```

Utilizzo di inventari personalizzati

Puoi assegnare tutti i metadati che desideri ai tuoi nodi creando AWS Systems Manager un inventario personalizzato di Inventory. Ad esempio, supponiamo che tu gestisca un numero elevato di server nel tuo data center e che i server siano stati configurati come nodi gestiti da Systems Manager. Attualmente, le informazioni relative alla posizione del rack dei server vengono archiviate in un foglio di calcolo. Con l'inventario personalizzato, puoi specificare la posizione del rack di ciascun nodo come metadati del nodo. Quando raccogli l'inventario con Systems Manager, i metadati vengono raccolti con altri metadati di inventario. Puoi poi trasferire tutti i metadati di inventario in un bucket Amazon S3 centralizzato utilizzando [Resource Data Sync](#) ed eseguendo una query sui dati.

Note

Systems Manager supporta un massimo di 20 tipi di inventario personalizzati per Account AWS.

Per assegnare un inventario personalizzato a un nodo, è possibile utilizzare l'operazione dell'[PutInventory](#) API Systems Manager, come descritto in [Assegnazione di metadati di inventario personalizzati a un nodo gestito](#). In alternativa, puoi creare e caricare nel nodo un file JSON dell'inventario personalizzato. Questa sezione descrive come creare il file JSON.

Il file JSON di esempio seguente con inventario personalizzato specifica le informazioni rack relative a un server on-premises. Questo esempio specifica un tipo di dati di inventario personalizzato ("TypeName": "Custom:RackInformation"), con più voci in Content che descrivono i dati.

```
{
  "SchemaVersion": "1.0",
  "TypeName": "Custom:RackInformation",
  "Content": {
    "Location": "US-EAST-02.CMH.RACK1",
    "InstalledTime": "2016-01-01T01:01:01Z",
    "vendor": "DELL",
    "Zone" : "BJS12",
    "TimeZone": "UTC-8"
  }
}
```

Puoi anche specificare voci distinte nella sezione Content, come mostrato nell'esempio seguente.

```
{
  "SchemaVersion": "1.0",
  "TypeName": "Custom:PuppetModuleInfo",
  "Content": [{
    "Name": "puppetlabs/aws",
    "Version": "1.0"
  },
  {
    "Name": "puppetlabs/dsc",
    "Version": "2.0"
  }
]
```

Lo schema JSON per l'inventario personalizzato richiede le sezioni SchemaVersion, TypeName e Content, in cui puoi definire le informazioni.

```
{
```

```

"SchemaVersion": "user_defined",
"TypeName": "Custom:user_defined",
"Content": {
  "user_defined_attribute1": "user_defined_value1",
  "user_defined_attribute2": "user_defined_value2",
  "user_defined_attribute3": "user_defined_value3",
  "user_defined_attribute4": "user_defined_value4"
}
}

```

Il valore di `TypeName` è limitato a 100 caratteri. Inoltre, il valore di `TypeName` deve iniziare con la parola `Custom` in maiuscolo. Ad esempio, `Custom:PuppetModuleInfo`. Pertanto, i seguenti esempi costituirebbero un'eccezione: `CUSTOM:PuppetModuleInfo`, `custom:PuppetModuleInfo`.

La `Content` sezione include attributi e *data*. Questi elementi non prevedono alcuna distinzione tra maiuscole e minuscole. Tuttavia, se definisci un attributo (ad esempio: `"Vendor": "DELL"`), sarà necessario fare riferimento a tale attributo in modo coerente nei tuoi file dell'inventario personalizzato. Se specifichi `"Vendor": "DELL"` (utilizzando la maiuscola "V" in `vendor`) in un file e quindi specifichi `"vendor": "DELL"` (utilizzando la minuscola "v" in `vendor`) in un altro file, il sistema restituisce un errore.

Note

È necessario salvare il file con estensione `.json` e l'inventario definito deve essere costituito solo da valori stringa.

Dopo aver creato il file, devi salvarlo nel nodo. La tabella riportata di seguito mostra il percorso in cui devono essere archiviati i file JSON dell'inventario personalizzato nel nodo.

Sistema operativo	Path
Linux	<code>/var/lib/amazon/ssm/<i>node-id</i>/inventory/custom</code>
macOS	<code>/opt/aws/ssm/data/<i>node-id</i>/inventory/custom</code>

Sistema operativo	Path
Windows Server	%SystemDrive%\ProgramData\ Amazon\ SSM \\ InstanceData node-id \ inventario\ personali zzato

Per un esempio di come utilizzare l'inventario personalizzato, consulta [Get Disk Utilization of Your Fleet Using EC2 Systems Manager Custom Inventory Types](#).

Eliminazione di un inventario personalizzato

Puoi utilizzare l'operazione [DeleteInventory](#) API per eliminare un tipo di inventario personalizzato e i dati associati a quel tipo. Puoi richiamare il comando delete-inventory tramite AWS Command Line Interface (AWS CLI) per eliminare tutti i dati di un tipo di inventario. Puoi richiamare il comando delete-inventory tramite SchemaDeleteOption per eliminare un tipo di inventario personalizzato.

Note

Il tipo di inventario viene chiamato anche schema di inventario.

Il parametro SchemaDeleteOption include le seguenti opzioni:

- DeleteSchema: Questa opzione elimina il tipo personalizzato specificato e tutti i dati ad esso associati. Puoi ricreare lo schema in un secondo momento, se lo desideri.
- DisableSchema: Se si sceglie questa opzione, il sistema disattiva la versione corrente, elimina tutti i relativi dati e ignora tutti i nuovi dati se la versione è inferiore o uguale alla versione disattivata. Puoi consentire nuovamente questo tipo di inventario chiamando l'[PutInventory](#) azione per una versione successiva alla versione disattivata.

Per eliminare o disattivare l'inventario personalizzato utilizzando il AWS CLI

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Eseguire questo comando per utilizzare l'opzione dry-run per vedere quali dati verranno eliminati dal sistema. Questo comando non elimina alcun dato.

```
aws ssm delete-inventory --type-name "Custom:custom_type_name" --dry-run
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "DeletionSummary":{
    "RemainingCount":3,
    "SummaryItems":[
      {
        "Count":2,
        "RemainingCount":2,
        "Version":"1.0"
      },
      {
        "Count":1,
        "RemainingCount":1,
        "Version":"2.0"
      }
    ],
    "TotalCount":3
  },
  "TypeName":"Custom:custom_type_name"
}
```

Per informazioni su come comprendere il riepilogo di eliminazione dell'inventario, consultare [Comprendere il riepilogo di eliminazione dell'inventario](#).

3. Eseguire questo comando per eliminare tutti i dati di un tipo di inventario personalizzato.

```
aws ssm delete-inventory --type-name "Custom:custom_type_name"
```

Note

L'output di questo comando non mostra l'avanzamento dell'eliminazione. Per questo motivo, TotalCount e Remaining Count sono sempre gli stessi perché il sistema non ha ancora eliminato nulla. È possibile utilizzare il comando `describe-inventory-deletions` per visualizzare l'avanzamento dell'eliminazione, come descritto più avanti in questo argomento.

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "DeletionId": "system_generated_deletion_ID",
  "DeletionSummary": {
    "RemainingCount": 3,
    "SummaryItems": [
      {
        "Count": 2,
        "RemainingCount": 2,
        "Version": "1.0"
      },
      {
        "Count": 1,
        "RemainingCount": 1,
        "Version": "2.0"
      }
    ],
    "TotalCount": 3
  },
  "TypeName": "custom_type_name"
}
```

Il sistema elimina dal servizio Inventory di Systems Manager tutti i dati del tipo di inventario personalizzato specificato.

4. Eseguire il seguente comando seguente. Il comando esegue le operazioni seguenti per la versione corrente del tipo di inventario: disattiva la versione corrente, elimina tutti i dati e ignora tutti i nuovi dati se la versione è inferiore o uguale a quella disattivata.

```
aws ssm delete-inventory --type-name "Custom:custom_type_name" --schema-delete-option "DisableSchema"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "DeletionId": "system_generated_deletion_ID",
  "DeletionSummary": {
    "RemainingCount": 3,
    "SummaryItems": [
```

```

    {
      "Count":2,
      "RemainingCount":2,
      "Version":"1.0"
    },
    {
      "Count":1,
      "RemainingCount":1,
      "Version":"2.0"
    }
  ],
  "TotalCount":3
},
"TypeName":"Custom:custom_type_name"
}

```

È possibile visualizzare un tipo di inventario disattivato utilizzando il comando seguente.

```
aws ssm get-inventory-schema --type-name Custom:custom_type_name
```

5. Eseguire questo comando per eliminare un tipo di inventario.

```
aws ssm delete-inventory --type-name "Custom:custom_type_name" --schema-delete-option "DeleteSchema"
```

Il sistema elimina lo schema e tutti i dati del tipo di inventario personalizzato specificato.

Il sistema restituisce informazioni simili alle seguenti.

```

{
  "DeletionId":"system_generated_deletion_ID",
  "DeletionSummary":{
    "RemainingCount":3,
    "SummaryItems":[
      {
        "Count":2,
        "RemainingCount":2,
        "Version":"1.0"
      },
      {
        "Count":1,
        "RemainingCount":1,

```

```

        "Version": "2.0"
      }
    ],
    "TotalCount": 3
  },
  "TypeName": "Custom:custom_type_name"
}

```

Visualizzazione dello stato dell'eliminazione

È possibile controllare lo stato di un'operazione di eliminazione utilizzando il `describe-inventory-deletions` AWS CLI comando. Puoi specificare un ID di eliminazione per visualizzare lo stato di una determinata operazione di eliminazione. In alternativa, puoi omettere l'ID di eliminazione per visualizzare un elenco di tutte le eliminazioni eseguite negli ultimi 30 giorni.

1. Eseguire questo comando per visualizzare lo stato di un'operazione di eliminazione. Il sistema restituisce l'ID di eliminazione nel riepilogo `delete-inventory`.

```
aws ssm describe-inventory-deletions --deletion-id system_generated_deletion_ID
```

Il sistema restituisce lo stato più recente. L'operazione di eliminazione potrebbe non essere ancora completata. Il sistema restituisce informazioni simili alle seguenti.

```

{"InventoryDeletions":
  [
    {"DeletionId": "system_generated_deletion_ID",
      "DeletionStartTime": 1521744844,
      "DeletionSummary":
        {"RemainingCount": 1,
          "SummaryItems":
            [
              {"Count": 1,
                "RemainingCount": 1,
                "Version": "1.0"}
            ],
          "TotalCount": 1},
      "LastStatus": "InProgress",
      "LastStatusMessage": "The Delete is in progress",
      "LastStatusUpdateTime": 1521744844,
      "TypeName": "Custom:custom_type_name"}
  ]
}

```

```
]
}
```

Se l'operazione di eliminazione viene completata correttamente, `LastStatusMessage` indica "Deletion is successful".

```
{
  "InventoryDeletions": [
    {
      "DeletionId": "system_generated_deletion_ID",
      "DeletionStartTime": 1521744844,
      "DeletionSummary": {
        "RemainingCount": 0,
        "SummaryItems": [
          {
            "Count": 1,
            "RemainingCount": 0,
            "Version": "1.0"
          }
        ],
        "TotalCount": 1
      },
      "LastStatus": "Complete",
      "LastStatusMessage": "Deletion is successful",
      "LastStatusUpdateTime": 1521745253,
      "TypeName": "Custom:custom_type_name"
    }
  ]
}
```

2. Eseguire questo comando per visualizzare un elenco di tutte le eliminazioni effettuate negli ultimi 30 giorni.

```
aws ssm describe-inventory-deletions --max-results a number
```

```
{
  "InventoryDeletions": [
    {
      "DeletionId": "system_generated_deletion_ID",
      "DeletionStartTime": 1521682552,
      "DeletionSummary": {
        "RemainingCount": 0,
        "SummaryItems": [
          {
            "Count": 1,
            "RemainingCount": 0,

```



```

        "Version": "1.0"}
    ],
    "TotalCount": 1},
    "LastStatus": "Complete",
    "LastStatusMessage": "Deletion is successful",
    "LastStatusUpdateTime": 1521682852,
    "TypeName": "Custom:custom_type_name"},
{"DeletionId": "system_generated_deletion_ID",
  "DeletionStartTime": 1521744844,
  "DeletionSummary":
    {"RemainingCount": 0,
     "SummaryItems":
      [
        {"Count": 1,
         "RemainingCount": 0,
         "Version": "1.0"}
      ],
     "TotalCount": 1},
    "LastStatus": "Complete",
    "LastStatusMessage": "Deletion is successful",
    "LastStatusUpdateTime": 1521745253,
    "TypeName": "Custom:custom_type_name"},
{"DeletionId": "system_generated_deletion_ID",
  "DeletionStartTime": 1521680145,
  "DeletionSummary":
    {"RemainingCount": 0,
     "SummaryItems":
      [
        {"Count": 1,
         "RemainingCount": 0,
         "Version": "1.0"}
      ],
     "TotalCount": 1},
    "LastStatus": "Complete",
    "LastStatusMessage": "Deletion is successful",
    "LastStatusUpdateTime": 1521680471,
    "TypeName": "Custom:custom_type_name"}
  ],
  "NextToken": "next-token"

```

Comprendere il riepilogo di eliminazione dell'inventario

Per poter comprendere i contenuti del riepilogo di eliminazione dell'inventario, prendi in considerazione l'esempio seguente. Un Custom:RackSpace inventario assegnato dall'utente a tre nodi. Gli articoli di inventario 1 e 2 utilizzano la versione 1.0 di tipo personalizzato (« SchemaVersion «:"1.0"). L'articolo 3 dell'inventario utilizza la versione 2.0 di tipo personalizzato (« SchemaVersion «:"2.0").

RackSpace inventario personalizzato 1

```
{
  "CaptureTime":"2018-02-19T10:48:55Z",
  "TypeName":"CustomType:RackSpace",
  "InstanceId":"i-1234567890",
  "SchemaVersion":"1.0"   "Content":[
    {
      content of custom type omitted
    }
  ]
}
```

RackSpace inventario personalizzato 2

```
{
  "CaptureTime":"2018-02-19T10:48:55Z",
  "TypeName":"CustomType:RackSpace",
  "InstanceId":"i-1234567891",
  "SchemaVersion":"1.0"   "Content":[
    {
      content of custom type omitted
    }
  ]
}
```

RackSpace inventario personalizzato 3

```
{
  "CaptureTime":"2018-02-19T10:48:55Z",
  "TypeName":"CustomType:RackSpace",
  "InstanceId":"i-1234567892",
  "SchemaVersion":"2.0"   "Content":[
```

```
{
  content of custom type omitted
}
]
```

L'utente esegue il comando seguente per visualizzare in anteprima i dati che saranno eliminati.

```
aws ssm delete-inventory --type-name "Custom:RackSpace" --dry-run
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "DeletionId":"1111-2222-333-444-66666",
  "DeletionSummary":{
    "RemainingCount":3,
    "TotalCount":3,
    TotalCount and RemainingCount are the number of items that would be
    deleted if this was not a dry run. These numbers are the same because the system
    didn't delete anything.
    "SummaryItems":[
      {
        "Count":2,
        The system found two items that use SchemaVersion
1.0. Neither item was deleted.
        "RemainingCount":2,
        "Version":"1.0"
      },
      {
        "Count":1,
        The system found one item that uses SchemaVersion
1.0. This item was not deleted.
        "RemainingCount":1,
        "Version":"2.0"
      }
    ],
  },
  "TypeName":"Custom:RackSpace"
}
```

L'utente esegue il seguente comando per eliminare l' Custom:RackSpace inventario.

Note

L'output di questo comando non mostra l'avanzamento dell'eliminazione. Per questo motivo, `TotalCount` e `RemainingCount` restano invariati, dato che il sistema non ha ancora effettuato eliminazioni. Puoi utilizzare il comando `describe-inventory-deletions` per visualizzare l'avanzamento dell'eliminazione.

```
aws ssm delete-inventory --type-name "Custom:RackSpace"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "DeletionId":"1111-2222-333-444-7777777",
  "DeletionSummary":{
    "RemainingCount":3,          There are three items to delete
    "SummaryItems":[
      {
        "Count":2,              The system found two items that use SchemaVersion
1.0.
        "RemainingCount":2,
        "Version":"1.0"
      },
      {
        "Count":1,              The system found one item that uses SchemaVersion
2.0.
        "RemainingCount":1,
        "Version":"2.0"
      }
    ],
    "TotalCount":3
  },
  "TypeName":"RackSpace"
}
```

Visualizzazione delle azioni di eliminazione dell'inventario in EventBridge

Puoi configurare Amazon EventBridge per creare un evento ogni volta che un utente elimina l'inventario personalizzato. EventBridge offre tre tipi di eventi per le operazioni personalizzate di eliminazione dell'inventario:

- Operazione di eliminazione per un'istanza: indica se l'inventario personalizzato per un determinato nodo gestito è stato eliminato o meno.
- Riepilogo dell'operazione di eliminazione: un riepilogo dell'operazione di eliminazione.
- Avviso per la disattivazione del tipo di inventario personalizzato: un evento di avviso se un utente ha chiamato l'operazione [PutInventory](#) API per una versione del tipo di inventario personalizzato che era stata precedentemente disattivata.

Di seguito sono riportati gli esempi di ciascun evento:

Operazione di eliminazione per un'istanza

```
{
  "version": "0",
  "id": "998c9cde-56c0-b38b-707f-0411b3ff9d11",
  "detail-type": "Inventory Resource State Change",
  "source": "aws.ssm",
  "account": "478678815555",
  "time": "2018-05-24T22:24:34Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ssm:us-east-1:478678815555:managed-instance/i-0a5feb270fc3f0b97"
  ],
  "detail": {
    "action-status": "succeeded",
    "action": "delete",
    "resource-type": "managed-instance",
    "resource-id": "i-0a5feb270fc3f0b97",
    "action-reason": "",
    "type-name": "Custom:MyInfo"
  }
}
```

Riepilogo dell'operazione di eliminazione

```
{
  "version": "0",
  "id": "83898300-f576-5181-7a67-fb3e45e4fad4",
  "detail-type": "Inventory Resource State Change",
  "source": "aws.ssm",
  "account": "478678815555",
  "time": "2018-05-24T22:28:25Z",
```

```

    "region": "us-east-1",
    "resources": [

],
    "detail": {
        "action-status": "succeeded",
        "action": "delete-summary",
        "resource-type": "managed-instance",
        "resource-id": "",
        "action-reason": "The delete for type name Custom:MyInfo was completed. The
deletion summary is: {\"totalCount\":2,\"remainingCount\":0,\"summaryItems\":
[{\"version\": \"1.0\", \"count\":2,\"remainingCount\":0}]}\",
        "type-name": "Custom:MyInfo"
    }
}

```

Avviso per il tipo di inventario personalizzato disattivato

```

{
    "version": "0",
    "id": "49c1855c-9c57-b5d7-8518-b64aeef5e4a",
    "detail-type": "Inventory Resource State Change",
    "source": "aws.ssm",
    "account": "478678815555",
    "time": "2018-05-24T22:46:58Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:478678815555:managed-instance/i-0ee2d86a2cfc371f6"
    ],
    "detail": {
        "action-status": "failed",
        "action": "put",
        "resource-type": "managed-instance",
        "resource-id": "i-0ee2d86a2cfc371f6",
        "action-reason": "The inventory item with type name Custom:MyInfo was sent with a
disabled schema version 1.0. You must send a version greater than 1.0",
        "type-name": "Custom:MyInfo"
    }
}

```

Utilizza la procedura seguente per creare una EventBridge regola per le operazioni personalizzate di eliminazione dell'inventario. Questa procedura illustra come creare una regola che invia notifiche per le operazioni di eliminazione di inventari personalizzati a un argomento Amazon SNS. Prima di

iniziare, verifica di avere un argomento Amazon SNS o creane uno nuovo. Per ulteriori informazioni, consulta [Nozioni di base](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service.

EventBridge Per configurare le operazioni di eliminazione dell'inventario

1. Apri la EventBridge console Amazon all'indirizzo <https://console.aws.amazon.com/events/>.
2. Nel pannello di navigazione, scegli Regole.
3. Scegli Crea regola.
4. Inserisci un nome e una descrizione per la regola.

Una regola non può avere lo stesso nome di un'altra regola nella stessa Regione e sullo stesso router di eventi.

5. Per Router di eventi, seleziona il router di eventi che desideri associare a questa regola. Se desideri che questa regola risponda agli eventi corrispondenti generati dai tuoi Account AWS, seleziona Predefinito. Quando un Servizio AWS utente del tuo account emette un evento, questo passa sempre al bus eventi predefinito del tuo account.
6. Per Tipo di regola, scegli Regola con un modello di eventi.
7. Scegli Next (Successivo).
8. Per Event source, scegli AWS eventi o eventi EventBridge partner.
9. Nella sezione Modello di eventi, scegli Modulo di modello di eventi.
10. Per Origine evento, scegli Servizi AWS .
11. Per AWS , scegli Systems Manager.
12. Per Tipo di evento, scegli Inventario.
13. Per Tipi di dettagli specifici, scegli Modifica dello stato della risorsa inventario.
14. Scegli Next (Successivo).
15. Per Tipi di destinazione, scegli Servizio AWS .
16. Per Seleziona una destinazione, scegli Argomento SNS, quindi scegli l'argomento dall'elenco Argomento.
17. Nella sezione Impostazioni aggiuntive, per Configura l'input di destinazione, verifica che sia selezionato Evento abbinato.
18. Scegli Next (Successivo).
19. (Facoltativo) Inserire uno o più tag per la regola. Per ulteriori informazioni, consulta [Tagging Your Amazon EventBridge Resources](#) nella Amazon EventBridge User Guide.

20. Scegli Next (Successivo).
21. Rivedi i dettagli della regola e scegli Crea regola.

Visualizzazione della cronologia e del monitoraggio delle modifiche di Inventory

Puoi visualizzare la cronologia AWS Systems Manager dell'inventario e il monitoraggio delle modifiche per tutti i tuoi nodi gestiti utilizzando [AWS Config](#). AWS Config fornisce una visualizzazione dettagliata della configurazione delle AWS risorse nel tuo Account AWS. Questo include le relazioni tra le risorse e la maniera in cui sono state configurate in passato, in modo che tu possa vedere come le configurazioni e le relazioni cambiano nel corso del tempo. Per visualizzare la cronologia e il monitoraggio delle modifiche dell'inventario, devi attivare le risorse seguenti in AWS Config:

- SSM:ManagedInstanceInventory
- SSM:PatchCompliance
- SSM:AssociationCompliance
- SSM:FileData

Note

Tieni presente le informazioni importanti sulla cronologia dell'inventario e sul monitoraggio delle modifiche riportate di seguito.

- Se si utilizza AWS Config per tenere traccia delle modifiche nel sistema, è necessario configurare Systems Manager Inventory per raccogliere AWS:File i metadati in modo da poter visualizzare le modifiche ai file in AWS Config (SSM:FileData). Se non lo fai, allora AWS Config non tiene traccia delle modifiche ai file sul tuo sistema.
- Attivando SSM:PatchCompliance e SSM:AssociationCompliance, è possibile visualizzare la cronologia di conformità e il monitoraggio delle modifiche delle Patch Manager patch di Systems Manager e delle State Manager associazioni Systems Manager. Per ulteriori informazioni sulla gestione della conformità per queste risorse, consulta [Scopri i dettagli sulla conformità](#).

La procedura seguente descrive come attivare la cronologia dell'inventario e la registrazione delle modifiche AWS Config utilizzando (). AWS Command Line Interface AWS CLI Per ulteriori informazioni su come scegliere e configurare queste risorse in AWS Config, consulta [Selezione dei](#)

[AWS Config record di risorse nella Guida](#) per gli AWS Config sviluppatori. Per informazioni sui prezzi di AWS Config , consulta la pagina dei [prezzi di](#) .

Prima di iniziare

AWS Config richiede le autorizzazioni AWS Identity and Access Management (IAM) per ottenere dettagli di configurazione sulle risorse di Systems Manager. Nella procedura seguente, è necessario specificare un Amazon Resource Name (ARN) per un ruolo IAM che AWS Config autorizza le risorse di Systems Manager. Puoi collegare la policy gestita AWS_ConfigRole al ruolo IAM assegnato a AWS Config. Per ulteriori informazioni su questo ruolo, consulta [AWS managed policy: AWS_ConfigRole](#) nella AWS Config Developer Guide. Per informazioni su come creare un ruolo IAM e assegnare la policy gestita AWS_ConfigRole a tale ruolo, consulta [Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS](#) nella Guida per l'utente IAM.

Per attivare la cronologia dell'inventario e la registrazione delle modifiche in AWS Config

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Copia e incolla il seguente esempio JSON in un semplice file di testo e salvalo come registrazioneGroup.json.

```
{
  "allSupported":false,
  "includeGlobalResourceTypes":false,
  "resourceTypes":[
    "AWS::SSM::AssociationCompliance",
    "AWS::SSM::PatchCompliance",
    "AWS::SSM::ManagedInstanceInventory",
    "AWS::SSM::FileData"
  ]
}
```

3. Esegui il comando seguente per caricare il Group.json file di registrazione in AWS Config.

```
aws configservice put-configuration-recorder --configuration-recorder
name=myRecorder,roleARN=arn:aws:iam::123456789012:role/myConfigRole --recording-
group file://recordingGroup.json
```

4. Eseguire questo comando per avviare la registrazione della cronologia e del monitoraggio delle modifiche di Inventory.

```
aws configservice start-configuration-recorder --configuration-recorder-  
name myRecorder
```

Dopo aver configurato la cronologia e il monitoraggio delle modifiche, è possibile eseguire il drill-down della cronologia per un determinato nodo gestito scegliendo il pulsante AWS Config nella console Systems Manager. Puoi accedere al pulsante AWS Config dalla pagina Istanze gestite o dalla pagina Inventario. A seconda delle dimensioni del monitor, potresti dover scorrere la pagina verso destra per visualizzare il pulsante.

Interruzione della raccolta dati ed eliminazione dei dati di inventario

Se non desideri più utilizzare AWS Systems Manager Inventory per visualizzare i metadati relativi alle tue AWS risorse, puoi interrompere la raccolta dei dati ed eliminare i dati che sono già stati raccolti. Questa sezione include le seguenti informazioni.

Argomenti

- [Interruzione della raccolta dei dati](#)
- [Eliminazione di un Resource Data Sync di Inventory](#)

Interruzione della raccolta dei dati

Quando si configura inizialmente Systems Manager per la raccolta dei dati di inventario, il sistema crea un'associazione State Manager che definisce la pianificazione e le risorse da cui raccogliere i metadati. È possibile interrompere la raccolta dei dati eliminando qualsiasi associazione State Manager che utilizza il documento AWS-GatherSoftwareInventory.

Eliminazione di un'associazione Inventory

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli State Manager.
3. Scegliere un'associazione che utilizzi il documento AWS-GatherSoftwareInventory e quindi scegliere Delete (Elimina).

4. Ripetere il passaggio tre per tutte le associazioni rimanenti che utilizzano il documento AWS-GatherSoftwareInventory.

Eliminazione di un Resource Data Sync di Inventory

Se non desideri più utilizzare AWS Systems Manager Inventory per visualizzare i metadati relativi alle tue AWS risorse, ti consigliamo anche di eliminare le sincronizzazioni dei dati delle risorse utilizzate per la raccolta dei dati di inventario.

Eliminare un Resource Data Sync di Inventory

1. Apri la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel riquadro di navigazione, seleziona Inventario.
3. Scegliere Resource Data Syncs (Sincronizzazioni dati risorsa).
4. Scegliere una sincronizzazione dall'elenco.

Important

Assicurati di scegliere la sincronizzazione utilizzata per Inventory. Systems Manager supporta la sincronizzazione dei dati delle risorse per molteplici strumenti. Se si sceglie la sincronizzazione errata, è possibile interrompere l'aggregazione dei dati per Systems Manager Explorer o la conformità di Systems Manager.

5. Seleziona Delete (Elimina)
6. Ripetere questi passaggi per tutte le sincronizzazioni dati risorsa rimanenti da eliminare.
7. Elimina il bucket Amazon Simple Storage Service (Amazon S3) in cui sono stati archiviati i dati. Per informazioni sull'eliminazione di un bucket Amazon S3, consulta [Eliminazione di un bucket](#).

Assegnazione di metadati di inventario personalizzati a un nodo gestito

La procedura seguente illustra il processo di utilizzo dell'operazione AWS Systems Manager [PutInventory](#) API per assegnare i metadati di inventario personalizzati a un nodo gestito. Questo esempio assegna le informazioni sulla posizione della pila a un nodo. Per ulteriori informazioni sull'inventario personalizzato, consulta [Utilizzo di inventari personalizzati](#).

Per assegnare metadati di Inventory personalizzati a un nodo

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Eseguire questo comando per assegnare informazioni sulla posizione della pila a un nodo.

Linux

```
aws ssm put-inventory --instance-id "ID" --items '[{"CaptureTime":  
  "2016-08-22T10:01:01Z", "TypeName": "Custom:RackInfo", "Content":[{"RackLocation":  
  "Bay B/Row C/Rack D/Shelf E"}], "SchemaVersion": "1.0"}]'
```

Windows

```
aws ssm put-inventory --instance-id "ID" --items  
  "TypeName=Custom:RackInfo,SchemaVersion=1.0,CaptureTime=2021-05-22T10:01:01Z,Content=[{RackLocation=  
  B/Row C/Rack D/Shelf F'}]"
```

3. Eseguire questo comando per visualizzare le voci dell'inventario personalizzato per questo nodo.

```
aws ssm list-inventory-entries --instance-id ID --type-name "Custom:RackInfo"
```

Il sistema risponde con informazioni simili alle seguenti.

```
{  
  "InstanceId": "ID",  
  "TypeName": "Custom:RackInfo",  
  "Entries": [  
    {  
      "RackLocation": "Bay B/Row C/Rack D/Shelf E"  
    }  
  ],  
  "SchemaVersion": "1.0",  
  "CaptureTime": "2016-08-22T10:01:01Z"  
}
```

4. Eseguire il comando seguente per visualizzare lo schema di inventario personalizzato.

```
aws ssm get-inventory-schema --type-name Custom:RackInfo
```

Il sistema risponde con informazioni simili alle seguenti.

```
{
  "Schemas": [
    {
      "TypeName": "Custom:RackInfo",
      "Version": "1.0",
      "Attributes": [
        {
          "DataType": "STRING",
          "Name": "RackLocation"
        }
      ]
    }
  ]
}
```

Utilizzo di AWS CLI per configurare la raccolta dei dati di inventario

Le procedure seguenti forniranno le istruzioni per configurare AWS Systems Manager Inventory per raccogliere i metadati dai tuoi nodi gestiti. Quando configuri la raccolta dell'inventario, puoi iniziare creando un'associazione State Manager Systems Manager. Systems Manager raccoglie i dati di inventario quando viene eseguita l'associazione. Se non crei prima l'associazione e tenti di richiamare il plugin `aws:softwareInventory` utilizzando, ad esempio, Run Command Systems Manager, il sistema restituisce il seguente errore:

The `aws:softwareInventory` plugin can only be invoked via `ssm-associate`.

Note

Un nodo può avere una sola associazione di Inventory configurata alla volta. Se configuri un nodo con due o più associazioni di Inventory, l'associazione non viene eseguita e non viene raccolto alcun dato dell'inventario.

Configurazione rapida di tutti i nodi gestiti per Inventory (CLI)

Puoi configurare rapidamente tutti i nodi gestiti nella tua regione Account AWS e nella regione corrente per raccogliere i dati di inventario. Questo processo è noto come creazione di un'associazione di inventario globale. Per creare un'associazione di inventario globale utilizzando AWS CLI, utilizzate l'opzione wildcard per il `instanceIds` valore, come illustrato nella procedura seguente.

Per configurare l'inventario per tutti i nodi gestiti nella tua regione Account AWS e nella regione corrente (CLI)

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Eseguire il seguente comando seguente.

Linux & macOS

```
aws ssm create-association \  
--name AWS-GatherSoftwareInventory \  
--targets Key=InstanceIds,Values=* \  
--schedule-expression "rate(1 day)" \  
--parameters  
    applications=Enabled,awsComponents=Enabled,customInventory=Enabled,instanceDetailedInfo
```

Windows

```
aws ssm create-association ^  
--name AWS-GatherSoftwareInventory ^  
--targets Key=InstanceIds,Values=* ^  
--schedule-expression "rate(1 day)" ^  
--parameters  
    applications=Enabled,awsComponents=Enabled,customInventory=Enabled,instanceDetailedInfo
```

Note

Questo comando non consente a Inventory di raccogliere metadati per il Registro di sistema o i file di Windows. Per l'inventario di questi tipi di dati, utilizza la procedura successiva.

Configurazione manuale di Inventory nei tuoi nodi gestiti (CLI)

Utilizza la seguente procedura per configurare manualmente AWS Systems Manager Inventory sui nodi gestiti utilizzando ID o tag dei nodi.

Per configurare manualmente i nodi gestiti per Inventory (CLI)

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Eseguire questo comando per creare un'associazione State Manager che esegue Inventory di Systems Manager sul nodo. Sostituisci ogni *example resource placeholder* con le tue informazioni. Questo comando configura il servizio perché venga eseguito ogni sei ore e per raccogliere da un nodo dati su configurazione della rete, Windows Update e metadati dell'applicazione.

Linux & macOS

```
aws ssm create-association \  
--name "AWS-GatherSoftwareInventory" \  
--targets "Key=instanceids,Values=an_instance_ID" \  
--schedule-expression "rate(240 minutes)" \  
--output-location "{ \"S3Location\": { \"OutputS3Region\": \"region_ID,  
for example us-east-2\", \"OutputS3BucketName\": \"amzn-s3-demo-bucket\",  
\"OutputS3KeyPrefix\": \"Test\" } }" \  
--parameters "networkConfig=Enabled,windowsUpdates=Enabled,applications=Enabled"
```

Windows

```
aws ssm create-association ^  
--name "AWS-GatherSoftwareInventory" ^  
--targets "Key=instanceids,Values=an_instance_ID" ^  
--schedule-expression "rate(240 minutes)" ^  
--output-location "{ \"S3Location\": { \"OutputS3Region\": \"region_ID,  
for example us-east-2\", \"OutputS3BucketName\": \"amzn-s3-demo-bucket\",  
\"OutputS3KeyPrefix\": \"Test\" } }" ^  
--parameters "networkConfig=Enabled,windowsUpdates=Enabled,applications=Enabled"
```

Il sistema risponde con informazioni simili alle seguenti.

```

{
  "AssociationDescription": {
    "ScheduleExpression": "rate(240 minutes)",
    "OutputLocation": {
      "S3Location": {
        "OutputS3KeyPrefix": "Test",
        "OutputS3BucketName": "Test bucket",
        "OutputS3Region": "us-east-2"
      }
    },
    "Name": "The name you specified",
    "Parameters": {
      "applications": [
        "Enabled"
      ],
      "networkConfig": [
        "Enabled"
      ],
      "windowsUpdates": [
        "Enabled"
      ]
    },
    "Overview": {
      "Status": "Pending",
      "DetailedStatus": "Creating"
    },
    "AssociationId": "1a2b3c4d5e6f7g-1a2b3c-1a2b3c-1a2b3c-1a2b3c4d5e6f7g",
    "DocumentVersion": "$DEFAULT",
    "LastUpdateAssociationDate": 1480544990.06,
    "Date": 1480544990.06,
    "Targets": [
      {
        "Values": [
          "i-02573cafcfEXAMPLE"
        ],
        "Key": "InstanceIds"
      }
    ]
  }
}

```


È possibile definire come target grandi gruppi di nodi utilizzando il parametro `Targets` con i tag EC2. Guarda l'esempio seguente.

Linux & macOS

```
aws ssm create-association \
--name "AWS-GatherSoftwareInventory" \
--targets "Key=tag:Environment,Values=Production" \
--schedule-expression "rate(240 minutes)" \
--output-location "{ \"S3Location\": { \"OutputS3Region\": \"us-east-2\",
  \"OutputS3BucketName\": \"amzn-s3-demo-bucket\", \"OutputS3KeyPrefix\": \"Test
\" } }" \
--parameters "networkConfig=Enabled,windowsUpdates=Enabled,applications=Enabled"
```

Windows

```
aws ssm create-association ^
--name "AWS-GatherSoftwareInventory" ^
--targets "Key=tag:Environment,Values=Production" ^
--schedule-expression "rate(240 minutes)" ^
--output-location "{ \"S3Location\": { \"OutputS3Region\": \"us-east-2\",
  \"OutputS3BucketName\": \"amzn-s3-demo-bucket\", \"OutputS3KeyPrefix\": \"Test
\" } }" ^
--parameters "networkConfig=Enabled,windowsUpdates=Enabled,applications=Enabled"
```

È anche possibile eseguire un inventario di file e chiavi del registro di sistema di Windows su un nodo Windows Server utilizzando i tipi di inventario `files` e `windowsRegistry` con espressioni. Per ulteriori informazioni su questi tipi di inventario, consulta [Utilizzo dell'inventario dei file e del registro di sistema di Windows](#).

Linux & macOS

```
aws ssm create-association \
--name "AWS-GatherSoftwareInventory" \
--targets "Key=instanceids,Values=i-0704358e3a3da9eb1" \
--schedule-expression "rate(240 minutes)" \
--parameters '{"files":["[{\\"Path\\": \\"C:\\\\Program Files\\", \\"Pattern\\":
[\\\"*.exe\\\"], \\"Recursive\\": true}]]", "windowsRegistry": [{"\\"Path\\":
\\"HKEY_LOCAL_MACHINE\\\\Software\\\\Amazon\\", \\"Recursive\\":true}]]}]' \
```

```
--profile dev-pdx
```

Windows

```
aws ssm create-association ^
--name "AWS-GatherSoftwareInventory" ^
--targets "Key=instanceids,Values=i-0704358e3a3da9eb1" ^
--schedule-expression "rate(240 minutes)" ^
--parameters '{"files":["[{\"Path\": \"C:\\Program Files\\\", \"Pattern\": [\"*.exe\"], \"Recursive\": true}]]\", \"windowsRegistry\": [{\"Path\": \"HKEY_LOCAL_MACHINE\\Software\\Amazon\\\", \"Recursive\":true}]]}' ^
--profile dev-pdx
```

3. Eseguire questo comando per visualizzare lo stato dell'associazione.

```
aws ssm describe-instance-associations-status --instance-id an_instance_ID
```

Il sistema risponde con informazioni simili alle seguenti.

```
{
  "InstanceAssociationStatusInfos": [
    {
      "Status": "Pending",
      "DetailedStatus": "Associated",
      "Name": "reInvent2016PolicyDocumentTest",
      "InstanceId": "i-1a2b3c4d5e6f7g",
      "AssociationId": "1a2b3c4d5e6f7g-1a2b3c-1a2b3c-1a2b3c-1a2b3c4d5e6f7g",
      "DocumentVersion": "1"
    }
  ]
}
```

Procedura dettagliata: utilizzo di sincronizzazione dati risorsa per aggregare dati di inventario

La procedura dettagliata seguente descrive come creare una configurazione di sincronizzazione dei dati delle risorse per AWS Systems Manager Inventory utilizzando AWS Command Line Interface (AWS CLI). Una sincronizzazione dati risorsa trasferisce automaticamente i dati di inventario della porta da tutti i nodi gestiti a un bucket Amazon Simple Storage Service (Amazon S3) centralizzato. La

sincronizzazione aggiorna automaticamente i dati nel bucket Amazon S3 centralizzato ogni volta che vengono rilevati dati di inventario.

Questa procedura dettagliata descrive anche come utilizzare Amazon Athena e Amazon Quick per interrogare e analizzare i dati aggregati. Per informazioni sulla creazione di una sincronizzazione dei dati delle risorse utilizzando Systems Manager in Console di gestione AWS, vedere [Procedura dettagliata: utilizzo di sincronizzazione dati risorsa per aggregare dati di inventario](#). Per informazioni sull'interrogazione dell'inventario da più Regioni AWS account utilizzando Systems Manager in Console di gestione AWS, vedere [Esecuzione di query sui dati di inventario da più regioni e account](#).

Note

Questa procedura guidata include informazioni su come crittografare la sincronizzazione utilizzando AWS Key Management Service (AWS KMS). Inventory non raccoglie dati sensibili, proprietari o specifici dell'utente, pertanto la crittografia è facoltativa. Per ulteriori informazioni in merito AWS KMS, vedere la [Guida per AWS Key Management Service gli sviluppatori](#).

Prima di iniziare

Prima di iniziare la spiegazione passo per passo in questa sezione, consulta o completa i processi descritti di seguito.

- Raccogli dati di inventario dai tuoi nodi gestiti. Ai fini delle sezioni Amazon Athena e Amazon Quick di questa procedura dettagliata, ti consigliamo di raccogliere i dati dell'Applicazione. Per ulteriori informazioni su come raccogliere i dati di Inventory, consulta [Configurazione della raccolta dell'inventario](#) o [Utilizzo di AWS CLI per configurare la raccolta dei dati di inventario](#).
- (Facoltativo) Se i dati di inventario sono archiviati in un bucket Amazon Simple Storage Service (Amazon S3) che AWS Key Management Service utilizza la crittografia AWS KMS(), devi anche configurare il tuo account IAM e il ruolo del servizio per Amazon-GlueServiceRoleForSSM la crittografia. AWS KMS Se non si configura l'account IAM e questo ruolo, Systems Manager visualizza Cannot load Glue tables, quando si sceglie l'opzione Visualizzazione dettagliata nella console. Per ulteriori informazioni, consulta [\(Facoltativo\) Configurare le autorizzazioni per la visualizzazione AWS KMS Dati crittografati](#).
- (Facoltativo) Se desideri crittografare la sincronizzazione dei dati delle risorse utilizzando AWS KMS, devi creare una nuova chiave che includa la seguente politica oppure aggiornare una chiave esistente e aggiungervi questa politica.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "ssm-access-policy",
  "Statement": [
    {
      "Sid": "ssm-access-policy-statement",
      "Action": [
        "kms:GenerateDataKey"
      ],
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Resource": "arn:aws:kms:us-east-1:123456789012:key/KMS_key_id",
      "Condition": {
        "StringLike": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ssm:*:123456789012:resource-data-
sync/*"
        }
      }
    }
  ]
}
```

Per creare un Resource Data Sync for Inventory

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Creare un bucket in cui archiviare i dati di inventario aggregati. Per ulteriori informazioni, consulta [Creazione di un bucket](#) nella Guida per l'utente di Amazon Simple Storage Service. Prendi nota del nome del bucket e del Regione AWS luogo in cui lo hai creato.
3. Dopo aver creato il bucket, scegliere la scheda Autorizzazioni, quindi Policy del bucket.
4. Copia e incolla la policy di bucket seguente nell'editor di policy. Sostituisci amzn-s3-demo-bucket e con il *account-id* nome del bucket Amazon S3 che hai creato e un ID valido. Account AWS Quando aggiungi più account, aggiungi una stringa di condizioni e un ARN

aggiuntivi per ogni account. Rimuovi i segnaposto aggiuntivi dall'esempio quando aggiungi un account. Facoltativamente, sostituirlo *bucket-prefix* con il nome di un prefisso Amazon S3 (sottodirectory). Se non hai creato un prefisso, rimuovilo *bucket-prefix/* dall'ARN nella policy.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSMBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/bucket-prefix/*/"
        accountid=111122223333/*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": [
            "111122223333",
            "444455556666",
            "123456789012",
            "777788889999"
          ]
        }
      },
      "ArnLike": {
        "aws:SourceArn": [
          "arn:aws:ssm:*:111122223333:resource-data-sync/*",
          "arn:aws:ssm:*:444455556666:resource-data-sync/*",
          "arn:aws:ssm:*:123456789012:resource-data-sync/*",
          "arn:aws:ssm:*:777788889999:resource-data-sync/*"
        ]
      }
    }
  ]
}
```

}

5. (Facoltativo) Per crittografare la sincronizzazione, devi aggiungere le seguenti condizioni alla policy riportata nel passaggio precedente. Aggiungila nella sezione `StringEquals`.

```
"s3:x-amz-server-side-encryption":"aws:kms",
"s3:x-amz-server-side-encryption-aws-kms-key-id":"arn:aws:kms:region:account_ID:key/KMS_key_ID"
```

Ecco un esempio:

```
"StringEquals": {
  "s3:x-amz-acl": "bucket-owner-full-control",
  "aws:SourceAccount": "account-id",
  "s3:x-amz-server-side-encryption":"aws:kms",
  "s3:x-amz-server-side-encryption-aws-kms-key-id":"arn:aws:kms:region:account_ID:key/KMS_key_ID"
}
```

6. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

7. (Facoltativo) Se desideri crittografare la sincronizzazione, esegui il comando seguente per verificare che la policy del bucket applichi il AWS KMS requisito chiave. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux & macOS

```
aws s3 cp ./A_file_in_the_bucket s3://amzn-s3-demo-bucket/prefix/ \
--sse aws:kms \
--sse-kms-key-id "arn:aws:kms:region:account_ID:key/KMS_key_id" \
--region region, for example, us-east-2
```

Windows

```
aws s3 cp ./A_file_in_the_bucket s3://amzn-s3-demo-bucket/prefix/ ^
--sse aws:kms ^
--sse-kms-key-id "arn:aws:kms:region:account_ID:key/KMS_key_id" ^
```

```
--region region, for example, us-east-2
```

8. Eseguire questo comando per creare una configurazione della sincronizzazione dati risorsa per aggregare dati di inventario con il bucket Amazon S3 creato all'inizio di questa procedura. Questo comando crea una sincronizzazione dal momento in Regione AWS cui hai effettuato l'accesso.

Note

Se la sincronizzazione e il bucket Amazon S3 di destinazione si trovano in regioni diverse, potrebbero essere applicati i prezzi per il trasferimento dei dati. Per ulteriori informazioni, consulta [Prezzi di Amazon S3](#).

Linux & macOS

```
aws ssm create-resource-data-sync \  
--sync-name a_name \  
--s3-destination "BucketName=amzn-s3-demo-bucket,Prefix=prefix_name,  
if_specified,SyncFormat=JsonSerDe,Region=bucket_region"
```

Windows

```
aws ssm create-resource-data-sync ^  
--sync-name a_name ^  
--s3-destination "BucketName=amzn-s3-demo-bucket,Prefix=prefix_name,  
if_specified,SyncFormat=JsonSerDe,Region=bucket_region"
```

È possibile utilizzare il parametro `region` per specificare la regione in cui creare la configurazione di sincronizzazione. Nell'esempio seguente, i dati di inventario dalla regione `us-west-1` saranno sincronizzati nel bucket Amazon S3 nella regione `us-west-2`.

Linux & macOS

```
aws ssm create-resource-data-sync \  
--sync-name InventoryDataWest \  
--s3-destination "BucketName=amzn-s3-demo-  
bucket,Prefix=HybridEnv,SyncFormat=JsonSerDe,Region=us-west-2"
```

```
--region us-west-1
```

Windows

```
aws ssm create-resource-data-sync ^
--sync-name InventoryDataWest ^
--s3-destination "BucketName=amzn-s3-demo-
bucket,Prefix=HybridEnv,SyncFormat=JsonSerDe,Region=us-west-2" ^ --region us-
west-1
```

(Facoltativo) Se desideri crittografare la sincronizzazione utilizzando AWS KMS, esegui il comando seguente per creare la sincronizzazione. Se crittografi la sincronizzazione, la AWS KMS chiave e il bucket Amazon S3 devono trovarsi nella stessa regione.

Linux & macOS

```
aws ssm create-resource-data-sync \
--sync-name sync_name \
--s3-destination "BucketName=amzn-s3-demo-bucket,Prefix=prefix_name,
if_specified,SyncFormat=JsonSerDe,AWSKMSKeyARN=arn:aws:kms:region:account_ID:key/
KMS_key_ID,Region=bucket_region" \
--region region
```

Windows

```
aws ssm create-resource-data-sync ^
--sync-name sync_name ^
--s3-destination "BucketName=amzn-s3-demo-bucket,Prefix=prefix_name,
if_specified,SyncFormat=JsonSerDe,AWSKMSKeyARN=arn:aws:kms:region:account_ID:key/
KMS_key_ID,Region=bucket_region" ^
--region region
```

9. Eseguire questo comando per visualizzare lo stato della configurazione di sincronizzazione.

```
aws ssm list-resource-data-sync
```

Se la configurazione di sincronizzazione è stata creata in un'altra regione, è necessario specificare il parametro `region`, come mostrato nel seguente esempio.


```
aws ssm list-resource-data-sync --region us-west-1
```

10. Una volta creata la configurazione di sincronizzazione, esamina il bucket di destinazione in Amazon S3. I dati di inventario dovrebbero essere visualizzati entro pochi minuti.

Utilizzo dei dati in Amazon Athena

La sezione seguente descrive come visualizzare ed eseguire query sui dati in Amazon Athena. Prima di iniziare, ti consigliamo di familiarizzare con Athena. Per ulteriori informazioni, consulta [Che cos'è Amazon Athena?](#) e [Utilizzo dei dati](#) nella Guida per l'utente di Amazon Athena.

Per visualizzare ed eseguire query sui dati in Amazon Athena

1. Apri la console Athena all'indirizzo <https://console.aws.amazon.com/athena/>.
2. Copia e incolla la seguente istruzione nell'editor di query e scegli Esegui query.

```
CREATE DATABASE ssminventory
```

Il sistema crea un database denominato ssminventory.

3. Copia e incolla la seguente istruzione nell'editor di query e scegli Esegui query. Sostituisci amzn-s3-demo-bucket e con il *bucket_prefix* nome e il prefisso del target Amazon S3.

```
CREATE EXTERNAL TABLE IF NOT EXISTS ssminventory.AWS_Application (
  Name string,
  ResourceId string,
  ApplicationType string,
  Publisher string,
  Version string,
  InstalledTime string,
  Architecture string,
  URL string,
  Summary string,
  PackageId string
)
PARTITIONED BY (AccountId string, Region string, ResourceType string)
ROW FORMAT SERDE 'org.openx.data.jsonserde.JsonSerDe'
WITH SERDEPROPERTIES (
  'serialization.format' = '1'
) LOCATION 's3://amzn-s3-demo-bucket/bucket_prefix/AWS:Application/'
```

4. Copia e incolla la seguente istruzione nell'editor di query e scegli Esegui query.

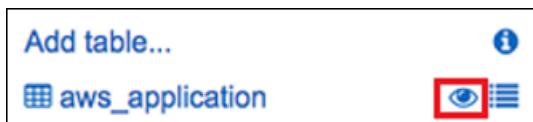
```
MSCK REPAIR TABLE ssminventory.AWS_Application
```

Il sistema esegue la partizione della tabella.

Note

Se crei sincronizzazioni dei dati delle risorse da un sistema operativo aggiuntivo Regioni AWS Account AWS, devi eseguire nuovamente questo comando per aggiornare le partizioni. Potrebbe anche essere necessario aggiornare la policy del bucket Amazon S3.

5. Per visualizzare un'anteprima dei dati, scegliere l'icona vista accanto alla tabella AWS_Application.



6. Copia e incolla la seguente istruzione nell'editor di query e scegli Esegui query.

```
SELECT a.name, a.version, count( a.version) frequency
from aws_application a where
a.name = 'aws-cfn-bootstrap'
group by a.name, a.version
order by frequency desc
```

La query restituisce un conteggio di diverse versioni di `aws-cfn-bootstrap`, che è un' AWS applicazione presente sulle istanze Amazon Elastic Compute Cloud (Amazon EC2) per Linux, e. macOS Windows Server

7. Copia e incolla singolarmente le seguenti istruzioni nell'editor di query, sostituisci `amzn-s3-demo-bucket` e ***bucket-prefix*** con informazioni per Amazon S3, quindi scegli Run Query. Queste istruzioni configurano tabelle Inventory aggiuntive in Athena.

```
CREATE EXTERNAL TABLE IF NOT EXISTS ssminventory.AWS_AWSComponent (
  `ResourceId` string,
  `Name` string,
  `ApplicationType` string,
  `Publisher` string,
  `Version` string,
```

```

    `InstalledTime` string,
    `Architecture` string,
    `URL` string
)
PARTITIONED BY (AccountId string, Region string, ResourceType string)
ROW FORMAT SERDE 'org.openx.data.jsonserde.JsonSerDe'
WITH SERDEPROPERTIES (
    'serialization.format' = '1'
) LOCATION 's3://amzn-s3-demo-bucket/bucket-prefix/AWS:AWSComponent/'

```

```
MSCK REPAIR TABLE ssminventory.AWS_AWSComponent
```

```

CREATE EXTERNAL TABLE IF NOT EXISTS ssminventory.AWS_WindowsUpdate (
    `ResourceId` string,
    `HotFixId` string,
    `Description` string,
    `InstalledTime` string,
    `InstalledBy` string
)
PARTITIONED BY (AccountId string, Region string, ResourceType string)
ROW FORMAT SERDE 'org.openx.data.jsonserde.JsonSerDe'
WITH SERDEPROPERTIES (
    'serialization.format' = '1'
) LOCATION 's3://amzn-s3-demo-bucket/bucket-prefix/AWS:WindowsUpdate/'

```

```
MSCK REPAIR TABLE ssminventory.AWS_WindowsUpdate
```

```

CREATE EXTERNAL TABLE IF NOT EXISTS ssminventory.AWS_InstanceInformation (
    `AgentType` string,
    `AgentVersion` string,
    `ComputerName` string,
    `IamRole` string,
    `InstanceId` string,
    `IpAddress` string,
    `PlatformName` string,
    `PlatformType` string,
    `PlatformVersion` string
)
PARTITIONED BY (AccountId string, Region string, ResourceType string)
ROW FORMAT SERDE 'org.openx.data.jsonserde.JsonSerDe'
WITH SERDEPROPERTIES (

```

```
'serialization.format' = '1'
) LOCATION 's3://amzn-s3-demo-bucket/bucket-prefix/AWS:InstanceInformation/'
```

```
MSCK REPAIR TABLE ssminventory.AWS_InstanceInformation
```

```
CREATE EXTERNAL TABLE IF NOT EXISTS ssminventory.AWS_Network (
  `ResourceId` string,
  `Name` string,
  `SubnetMask` string,
  `Gateway` string,
  `DHCPServer` string,
  `DNSServer` string,
  `MacAddress` string,
  `IPV4` string,
  `IPV6` string
)
PARTITIONED BY (AccountId string, Region string, ResourceType string)
ROW FORMAT SERDE 'org.openx.data.jsonserde.JsonSerDe'
WITH SERDEPROPERTIES (
  'serialization.format' = '1'
) LOCATION 's3://amzn-s3-demo-bucket/bucket-prefix/AWS:Network/'
```

```
MSCK REPAIR TABLE ssminventory.AWS_Network
```

```
CREATE EXTERNAL TABLE IF NOT EXISTS ssminventory.AWS_PatchSummary (
  `ResourceId` string,
  `PatchGroup` string,
  `BaselineId` string,
  `SnapshotId` string,
  `OwnerInformation` string,
  `InstalledCount` int,
  `InstalledOtherCount` int,
  `NotApplicableCount` int,
  `MissingCount` int,
  `FailedCount` int,
  `OperationType` string,
  `OperationStartTime` string,
  `OperationEndTime` string
)
PARTITIONED BY (AccountId string, Region string, ResourceType string)
ROW FORMAT SERDE 'org.openx.data.jsonserde.JsonSerDe'
```



```
WITH SERDEPROPERTIES (  
  'serialization.format' = '1'  
) LOCATION 's3://amzn-s3-demo-bucket/bucket-prefix/AWS:PatchSummary/'
```

```
MSCK REPAIR TABLE ssminventory.AWS_PatchSummary
```

Utilizzo dei dati in Amazon Quick

La sezione seguente fornisce una panoramica con collegamenti per la creazione di una visualizzazione in Amazon Quick.

Per creare una visualizzazione in Amazon Quick

1. Registrati ad [Amazon Quick](#) e accedi alla console Quick.
2. Creare un set di dati dalla tabella `AWS_Application` e da tutte le altre tabelle create. Per ulteriori informazioni, consulta [Creazione di un set di dati utilizzando i dati di Amazon Athena](#) nella Amazon Quick User Guide.
3. Unire le tabelle. Ad esempio, è possibile unire la colonna `instanceid` dalla tabella `AWS_InstanceInformation` poiché corrisponde alla colonna `resourceid` di altre tabelle di inventario. Per ulteriori informazioni sull'unione delle tabelle, consulta [Joining data](#) nella Amazon Quick User Guide.
4. Creare una visualizzazione. Per ulteriori informazioni, consulta [Analisi e report: visualizzazione dei dati in Amazon Quick Sight nella Amazon Quick](#) User Guide.

Risoluzione dei problemi di Inventory Systems Manager

Questo argomento include informazioni su come risolvere gli errori o i problemi più comuni relativi a Inventory. AWS Systems Manager In caso di problemi nella visualizzazione dei nodi in Systems Manager, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#).

Argomenti

- [Non sono supportate tutte le associazioni in applicazione multipla con il documento 'AWS-GatherSoftwareInventory'](#)
- [Lo stato di esecuzione dell'inventario non risulta mai in sospeso](#)
- [L'esecuzione del documento AWS-ListWindowsInventory fallisce](#)

- [La console non visualizza il pannello di controllo di Inventory | Visualizzazione dettagliata | Schede Impostazioni](#)
- [UnsupportedAgent](#)
- [Saltato](#)
- [Non riuscito](#)
- [Conformità dell'inventario non riuscita per un'istanza Amazon EC2](#)
- [L'oggetto bucket S3 contiene vecchi dati](#)

Non sono supportate tutte le associazioni in applicazione multipla con il documento '**AWS-GatherSoftwareInventory**'

Un errore Multiple apply all associations with document 'AWS-GatherSoftwareInventory' are not supported significa che una o più Regioni AWS in cui stai tentando di configurare un'associazione Inventory per tutti i nodi sono già configurate con un'associazione Inventory per tutti i nodi. Se necessario, puoi eliminare l'associazione di inventario esistente per tutti i nodi e crearne una nuova. Per visualizzare le associazioni Inventory esistenti, scegli State Manager nella console di Systems Manager e quindi individua le associazioni che utilizzano il documento SSM di AWS-GatherSoftwareInventory. Se l'associazione Inventory esistente per tutti i nodi è stata creata in più regioni e si desidera crearne una nuova, è necessario eliminare l'associazione esistente da ogni regione in cui è presente.

Lo stato di esecuzione dell'inventario non risulta mai in sospeso

Ci sono due motivi per cui la raccolta dell'inventario non è mai in stato Pending.

- Nessun nodo tra quelli selezionati: Regione AWS

Se si crea un'associazione di inventario globale utilizzando Quick Setup Systems Manager, lo stato dell'associazione di inventario (documento AWS-GatherSoftwareInventory) mostra Pending se non ci sono nodi disponibili nella regione selezionata .

- Autorizzazioni insufficienti:

Un'associazione di inventario mostra Pending se uno o più nodi non dispongono dell'autorizzazione per eseguire Inventory di Systems Manager. Verifica che il profilo dell'istanza AWS Identity and Access Management (IAM) includa la policy AmazonSSMManagedInstanceCore gestita. Per informazioni su come aggiungere questa policy a un profilo dell'istanza, consulta [Configurazione alternativa per le autorizzazioni delle istanze EC2](#).

Al minimo, il profilo dell'istanza deve disporre delle autorizzazioni IAM descritte di seguito.

JSON

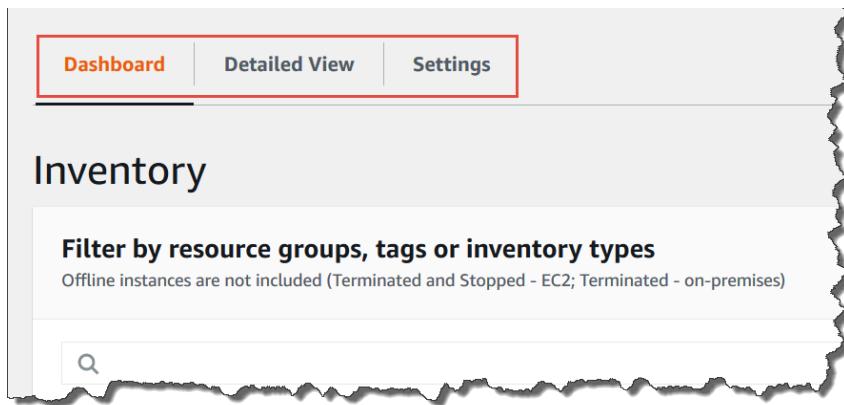
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:DescribeAssociation",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource": "*"
    }
  ]
}
```

L'esecuzione del documento **AWS-ListWindowsInventory** fallisce

Il documento AWS-ListWindowsInventory è obsoleto. Non utilizzare questo documento per raccogliere l'inventario. Utilizza invece uno dei processi descritti in [Configurazione della raccolta dell'inventario](#).

La console non visualizza il pannello di controllo di Inventory | Visualizzazione dettagliata | Schede Impostazioni

La pagina Detailed View (Visualizzazione dettagliata) di Inventory è disponibile solo in Regioni AWS che offrono Amazon Athena. Se le seguenti schede non sono visualizzate nella pagina Inventory, significa che Athena non è disponibile nella regione e non è possibile utilizzare la Detailed View (Visualizzazione dettagliata) per eseguire query sui dati.



UnsupportedAgent

Se viene visualizzato `UnsupportedAgent` lo stato dettagliato di un'associazione di inventario e lo stato dell'associazione indica Non riuscita, la versione di AWS Systems Manager SSM Agent sul nodo gestito non è corretta. Ad esempio, per creare un'associazione di inventario globale (per inventariare tutti i nodi del tuo Account AWS), devi utilizzare la SSM Agent versione 2.0.790.0 o successiva. Puoi visualizzare la versione dell'agente in esecuzione su ciascuno dei tuoi nodi nella pagina Istanze gestite nella colonna Versione agente. Per informazioni su come aggiornare l'SSM Agent sui tuoi nodi, consulta [Aggiornamento di SSM Agent utilizzando Run Command](#).

Saltato

Se lo stato dell'associazione di inventario per un nodo mostra Saltato, questo indica che un'associazione di inventario con priorità più alta è già in esecuzione in quel nodo. Systems Manager segue un ordine di priorità specifico quando è possibile applicare molteplici associazioni di inventario allo stesso nodo gestito.

Ordine di priorità dell'associazione di inventario

Systems Manager applica le associazioni di inventario nel seguente ordine di priorità:

1. Associazioni di inventario Quick Setup: associazioni create utilizzando Quick Setup e la console unificata. Queste associazioni hanno nomi che iniziano con `AWS-QuickSetup-SSM-CollectInventory-` e sono diretti a tutti i nodi gestiti.
2. Associazioni di inventario esplicite: associazioni che hanno come destinazione nodi gestiti specifici utilizzando:
 - ID istanza
 - Coppie chiave-valore del tag

- AWS gruppi di risorse
3. Associazioni di inventario globali: associazioni che hanno come destinazione tutti i nodi gestiti (utilizzando `--targets "Key=InstanceIds,Values=*"`), ma non sono state create tramite Quick Setup.

Scenari comuni

Scenario 1: l'associazione Quick Setup ha la precedenza sull'associazione esplicita

- Hai un'associazione di inventario Quick Setup destinata a tutte le istanze
- Crei un'associazione manuale destinata a nodi gestiti specifici per tag
- Risultato: l'associazione manuale viene visualizzata come `Skipped` con uno stato `OverriddenByExplicitInventoryAssociation` dettagliato
- L'associazione Quick Setup continua a raccogliere l'inventario di tutte le istanze

Scenario 2: l'associazione esplicita ha la precedenza sull'associazione globale

- Hai un'associazione di inventario globale destinata a tutte le istanze (non creata da Quick Setup)
- Crei un'associazione destinata a istanze specifiche
- Risultato: l'associazione globale viene visualizzata come `Skipped` per le istanze con destinazione specifica
- L'associazione esplicita viene eseguita sulle istanze di destinazione

Passaggi di risoluzione

Se desideri utilizzare la tua associazione di inventario invece di Quick Setup:

1. Identifica le associazioni Quick Setup: nella console Systems Manager, vai a State Manager e cerca le associazioni con nomi che iniziano con `AWS-QuickSetup-SSM-CollectInventory-`.
2. Rimuovi la configurazione di Quick Setup:
 - Vai a Quick Setup nella console di Systems Manager.
 - Trova la configurazione della tua collezione di inventario.
 - Elimina la configurazione Quick Setup (questa operazione rimuove l'associazione di inventario associata).

 Note

Non è necessario eliminare manualmente l'associazione creata da Quick Setup.

3. Verifica che l'associazione funzioni: dopo aver rimosso la configurazione Quick Setup, l'associazione di inventario esplicita dovrebbe iniziare a funzionare correttamente.

Se desideri modificare il comportamento esistente:

- Per visualizzare le associazioni Inventory esistenti, scegli State Manager nella console di Systems Manager e quindi individua le associazioni che utilizzano il documento SSM di AWS-GatherSoftwareInventory.
- Ricorda che ogni nodo gestito può avere una sola associazione di inventario alla volta.

 Important

- I dati di inventario vengono comunque raccolti dai nodi ignorati quando viene eseguita l'associazione di inventario assegnata (con priorità più alta).
- Le associazioni di inventario Quick Setup hanno la precedenza su tutti gli altri tipi, anche su quelle con targeting esplicito.
- Il messaggio `OverriddenByExplicitInventoryAssociation` di stato dettagliato viene visualizzato quando un'associazione è sostituita da un'altra con priorità più alta, indipendentemente dal tipo di associazione.

Non riuscito

Se lo stato dell'associazione di inventario per un nodo mostra Non riuscito, il nodo potrebbe essere assegnata a più associazioni di inventario. Un nodo può essere assegnato a una sola associazione di inventario alla volta. Un'associazione di inventario utilizza il AWS-GatherSoftwareInventory AWS Systems Manager documento (documento SSM). È possibile eseguire il comando seguente utilizzando AWS Command Line Interface (AWS CLI) per visualizzare un elenco di associazioni per un nodo.

```
aws ssm describe-instance-associations-status --instance-id instance-ID
```

Conformità dell'inventario non riuscita per un'istanza Amazon EC2

La conformità dell'inventario per un'istanza Amazon Elastic Compute Cloud (Amazon EC2) può fallire se si assegnano più associazioni di inventario all'istanza.

Per risolvere questo problema, elimina una o più associazioni di inventario assegnate all'istanza. Per ulteriori informazioni, consulta [Eliminazione di un'associazione](#).

Note

Tenere presente il comportamento seguente se si creano più associazioni di inventario per un nodo gestito.

- A ogni nodo può essere assegnata un'associazione di inventario destinata a tutti i nodi (--targets «Key=InstanceId, Values=*»).
- A ciascun nodo può essere assegnata anche un'associazione specifica che utilizza coppie chiave-valore di tag o un gruppo di risorse. AWS
- Se a un nodo vengono assegnate più associazioni d'inventario, lo stato mostra Saltato per l'associazione che non è stata eseguita. L'associazione eseguita più di recente visualizza lo stato effettivo dell'associazione d'inventario.
- Se a un nodo vengono assegnate più associazioni d'inventario e ognuna utilizza una coppia chiave-valore di tag, le associazioni d'inventario non vengono eseguite sul nodo a causa del conflitto di tag. L'associazione viene ancora eseguita su nodi che non hanno il conflitto chiave-valore di tag.

L'oggetto bucket S3 contiene vecchi dati

I dati all'interno dell'oggetto bucket Amazon S3 vengono aggiornati quando l'associazione di inventario ha esito positivo e vengono scoperti nuovi dati. L'oggetto bucket Amazon S3 viene aggiornato per ogni nodo quando l'associazione viene eseguita e ha esito negativo, ma in questo caso i dati all'interno dell'oggetto non vengono aggiornati. I dati all'interno dell'oggetto bucket Amazon S3 verranno aggiornati solo quando l'associazione viene eseguita correttamente. Quando l'associazione dell'inventario fallisce, vengono visualizzati i vecchi dati nell'oggetto bucket Amazon S3.

AWS Systems Manager Patch Manager

Patch Manager automatizza il processo di applicazione di patch ai nodi gestiti con aggiornamenti relativi alla sicurezza e di altro tipo.

Questa sezione contiene gli argomenti seguenti.

- [Risoluzione dei problemi Patch Manager](#)
- [Tutorial: aggiorna le dipendenze dell'applicazione, applica patch a un nodo gestito ed esegui un controllo dell'integrità specifico dell'applicazione tramite la console](#)
- [Apertura con le baseline delle patch](#)
- [Correzione dei nodi gestiti non conformi con Patch Manager](#)
- [Applicazione di patch live del kernel tramite Run Command](#)
- [AWS Systems Manager Patch Manager tutorial](#)
- [Accensione Applicazione di patch live del kernel utilizzo di Run Command](#)
- [Applicazioni di patch rilasciate da Microsoft il Windows Server](#)
- [Lavorare con Patch Manager risorse e conformità utilizzando la console](#)
- [Utilizzo Applicazione di patch live del kernel su nodi gestiti Amazon Linux 2](#)
- [Visualizzazione delle patch disponibili](#)
- [Differenze nelle operazioni di patching tra Linux e Windows Server](#)
- [Creazione di una policy di patch](#)
- [In che modo Patch Manager operazioni funzionano](#)
- [Aggiornamento o eliminazione di una baseline delle patch personalizzata](#)

Note

Systems Manager fornisce supporto per le policy di patch in Quick Setup, uno strumento di AWS Systems Manager. L'utilizzo delle policy di patch è il metodo consigliato per configurare le operazioni di applicazione di patch. Con una singola configurazione delle policy di patch, è possibile definire l'applicazione di patch per tutti gli account in tutte le regioni dell'organizzazione, per regioni e account selezionati o per una singola coppia account-regione. Per ulteriori informazioni, consulta [Configurazioni delle policy sulle patch in Configurazione rapida](#).

È possibile utilizzare Patch Manager per applicare patch sia per i sistemi operativi sia per le applicazioni. (In Windows Server, il supporto delle applicazioni è limitato ai soli aggiornamenti delle applicazioni Microsoft). È possibile utilizzare Patch Manager per installare Service Pack nei nodi di Windows ed eseguire aggiornamenti di versione secondari sui nodi di Linux. È possibile applicare patch a parchi di istanze Amazon Elastic Compute Cloud (Amazon EC2), dispositivi edge, server on-premises e macchine virtuali (VM), in base al tipo di sistema operativo. Sono incluse le versioni supportate di diversi sistemi operativi, come elencato su [Patch Manager prerequisiti](#). È possibile analizzare le istanze per visualizzare solo un report delle patch mancanti, oppure analizzare e installare automaticamente tutte le patch mancanti. Per iniziare a utilizzare Patch Manager, apri la [console di Systems Manager](#). Nel pannello di navigazione, scegli Patch Manager.

AWS non testa le patch prima di renderle disponibili in. Patch Manager Inoltre, Patch Manager non supporta l'aggiornamento delle versioni principali dei sistemi operativi, ad esempio da Windows Server 2016 a Windows Server 2019, o da Red Hat Enterprise Linux (RHEL) 7.0 a RHEL 8.0.

Per i tipi di sistema Linux-based operativo che segnalano un livello di gravità per le patch, Patch Manager utilizza il livello di gravità riportato dal produttore del software per l'avviso di aggiornamento o la singola patch. Patch Manager non deriva i livelli di gravità da fonti di terze parti, come il [Common Vulnerability Scoring System](#) (CVSS), o dalle metriche rilasciate dal National Vulnerability Database (NVD). <https://nvd.nist.gov/vuln>

Come può Patch Manager avvantaggiare la mia organizzazione?

Patch Manager automatizza il processo di applicazione di patch ai nodi gestiti con aggiornamenti relativi alla sicurezza e di altro tipo. Fornisce diversi vantaggi:

- Controllo centralizzato dell'applicazione di patch: tramite le policy di patch, è possibile configurare operazioni di applicazione di patch ricorrenti per tutti gli account in tutte le Regioni dell'organizzazione, in account e Regioni specifici o in una singola coppia account-regione.
- Operazioni di applicazione di patch flessibili: è possibile scegliere di analizzare le istanze per visualizzare solo un report delle patch mancanti oppure analizzare e installare automaticamente tutte le patch mancanti.
- Esecuzione di report completi sulla conformità: dopo le operazioni di analisi, è possibile visualizzare informazioni dettagliate su quali nodi gestiti non sono conformi alle patch e quali patch mancano.
- Cross-platform supporto: Patch Manager supporta più sistemi operativi, tra cui varie distribuzioni Linux macOS e Windows Server.

- **Baseline delle patch personalizzate:** è possibile definire ciò che costituisce la conformità delle patch per l'organizzazione tramite baseline delle patch personalizzate che specificano quali patch sono approvate per l'installazione.
- **Integrazione con altri AWS servizi:** Patch Manager si integra con AWS Organizations, AWS Security Hub CSPM AWS CloudTrail, e AWS Config per una gestione e una sicurezza avanzate.
- **Aggiornamenti deterministici:** supporto per gli aggiornamenti deterministici tramite repository con versioni per sistemi operativi come Amazon Linux 2023.

Chi dovrebbe utilizzarlo Patch Manager?

Patch Manager è progettato per i seguenti casi d'uso:

- Amministratori IT che devono mantenere la conformità delle patch in tutto il parco istanze di nodi gestiti;
- Responsabili delle operazioni che necessitano di visibilità sullo stato di conformità delle patch nell'intera infrastruttura;
- Architetti del cloud che desiderano implementare soluzioni di applicazione di patch automatizzate su larga scala;
- DevOps ingegneri che hanno bisogno di integrare le patch nei loro flussi di lavoro operativi
- Organizzazioni con implementazioni in più account/multi regioni che necessitano di una gestione centralizzata delle patch
- Chiunque sia responsabile del mantenimento del livello di sicurezza e dell'integrità operativa di nodi AWS gestiti, dispositivi edge, server locali e macchine virtuali

Quali sono le caratteristiche principali di Patch Manager?

Patch Manager offre diverse funzionalità chiave:

- **Policy sulle patch:** configura le operazioni di patching su più Account AWS aree geografiche utilizzando un'unica policy tramite l'integrazione con AWS Organizations.
- **Baseline delle patch personalizzate:** definisci regole per l'approvazione automatica delle patch entro pochi giorni dalla relativa pubblicazione, nonché un elenco delle patch approvate e rifiutate.
- **Diversi metodi di applicazione di patch:** scegli tra policy di patch, finestre di manutenzione oppure operazioni "Applica patch ora" su richiesta, per soddisfare le tue esigenze specifiche.

- Esecuzione di report di conformità: genera report dettagliati sullo stato di conformità delle patch da inviare a un bucket Amazon S3 in formato CSV.
- Cross-platform supporto: applica patch ai sistemi operativi e alle applicazioni su Windows Server varie distribuzioni Linux e macOS
- Flessibilità di pianificazione: imposta pianificazioni diverse per l'analisi e l'installazione delle patch utilizzando espressioni CRON o della frequenza personalizzate.
- Hook del ciclo di vita: esegui script personalizzati prima e dopo le operazioni di applicazione di patch utilizzando i documenti di Systems Manager.
- Attenzione alla sicurezza: per impostazione predefinita, Patch Manager si concentra sugli aggiornamenti relativi alla sicurezza anziché sull'installazione di tutte le patch disponibili.
- Controllo della frequenza: configura le soglie di concorrenza e di errore nelle operazioni di applicazione di patch per ridurre al minimo l'impatto operativo.

In cosa consiste la conformità Patch Manager?

Il parametro di riferimento per determinare la conformità delle patch per i nodi gestiti delle flotte di Systems Manager non è definito né dai AWS fornitori di sistemi operativi (OS) né da terze parti, come le società di consulenza in materia di sicurezza.

Al contrario, è l'utente che definisce cosa significa conformità delle patch per i nodi gestiti nell'organizzazione o nell'account in una baseline delle patch. Una baseline delle patch è una configurazione che specifica le regole per le quali le patch devono essere installate su un nodo gestito. Un nodo gestito è conforme alle patch quando è aggiornato con tutte le patch che soddisfano i criteri di approvazione specificati nella baseline delle patch.

Tieni presente che essere conforme a baseline delle patch non significa che un nodo gestito sia necessariamente sicuro. Conforme significa che le patch definite dalla baseline delle patch, che siano disponibili o approvate, sono state installate sul nodo. La sicurezza complessiva di un nodo gestito è determinata da molti fattori che non rientrano nell'ambito di Patch Manager. Per ulteriori informazioni, consulta [Sicurezza](#).

Ogni baseline delle patch è una configurazione per uno specifico tipo di sistema operativo (OS) supportato, ad esempio Red Hat Enterprise Linux (RHEL) macOS o Windows Server. Una baseline delle patch può definire le regole di applicazione di patch per tutte le versioni supportate di un sistema operativo o essere limitata solo a quelle specificate dall'utente, ad esempio RHEL 7.8. e RHEL 9.3.

In una baseline delle patch, è possibile specificare che tutte le patch con specifici classificazioni e livelli di gravità siano approvate per l'installazione. Ad esempio, è possibile includere tutte le patch classificate come `Security`, ma escludere altre classificazioni, come `Bugfix` o `Enhancement`. È inoltre possibile includere tutte le patch con una gravità pari a `Critical` ed escluderne altre, ad esempio `Important` e `Moderate`.

Puoi anche definire le patch in modo esplicito in una baseline delle patch aggiungendo i relativi ID agli elenchi di patch specifiche da approvare o rifiutare, ad esempio `KB2736693` per Windows Server o `dbus.x86_64:1:1.12.28-1.amzn2023.0.1` per Amazon Linux 2023 (AL2023). Facoltativamente, puoi specificare un certo numero di giorni di attesa per l'applicazione delle patch dopo che una patch diventa disponibile. Per Linux e macOS, è possibile specificare un elenco esterno di patch per la conformità (un elenco "Installa sovrascrivi") anziché quelle definite dalle regole della baseline delle patch.

Quando viene eseguita un'operazione di applicazione di patch, Patch Manager confronta le patch attualmente applicate a un nodo gestito con quelle da applicare in base alle regole configurate nella baseline delle patch. È possibile impostare Patch Manager in modo che mostri soltanto un report delle patch mancanti (un'operazione `Scan`) oppure Patch Manager può installare automaticamente tutte le patch mancanti in un nodo gestito (un'operazione `Scan and install`).

Note

I dati sulla conformità delle patch rappresentano un'istantanea temporale dell'ultima operazione di patching riuscita. Ogni rapporto di conformità contiene un orario di acquisizione che identifica quando è stato calcolato lo stato di conformità. Quando esamini i dati sulla conformità, considera il tempo di acquisizione per determinare se l'operazione è stata eseguita come previsto.

Patch Manager fornisce baseline delle patch predefinite che è possibile utilizzare per le operazioni di applicazione di patch; tuttavia, queste configurazioni predefinite vengono fornite come esempi e non come best practice consigliate. Ti consigliamo di creare baseline delle patch personalizzate per le tue patch, così potrai esercitare un maggiore controllo su ciò che costituisce la conformità delle patch per il tuo parco istanze.

Per ulteriori informazioni sulle baseline delle patch, consulta i seguenti argomenti:

- [Baseline delle patch predefinite e personalizzate](#)

- [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#)
- [Visualizzazione AWS linee di base predefinite delle patch](#)
- [Utilizzo delle baseline delle patch personalizzate](#)
- [Utilizzo dei report sulla conformità delle patch](#)

Componenti principali

Prima di iniziare a utilizzare lo strumento Patch Manager, è necessario acquisire familiarità con alcuni componenti e funzionalità principali delle operazioni di applicazione di patch dello strumento.

Baseline delle patch

Patch Manager utilizza le linee di base delle patch, che includono regole per l'approvazione automatica delle patch entro pochi giorni dal loro rilascio, oltre a elenchi opzionali di patch approvate e rifiutate. Quando viene eseguita un'operazione di applicazione di patch, Patch Manager confronta le patch attualmente applicate a un nodo gestito con quelle da applicare in base alle regole configurate nella baseline delle patch. È possibile impostare Patch Manager in modo che mostri soltanto un report delle patch mancanti (un'operazione Scan) oppure Patch Manager può installare automaticamente tutte le patch mancanti in un nodo gestito (un'operazione Scan and install).

Metodi operativi di applicazione di patch

Patch Manager offre attualmente quattro metodi per eseguire operazioni Scan e Scan and install:

- (Consigliato) Una policy sulle patch configurata in Quick Setup: in base all'integrazione con AWS Organizations, una singola policy sulle patch può definire le pianificazioni e le linee di base delle patch per un'intera organizzazione, inclusi più account e tutti gli account in cui operano. Account AWS Regioni AWS Una policy di patch è inoltre destinata solo ad alcune unità organizzative (UO) in un'organizzazione. È possibile utilizzare un'unica policy di patch per eseguire l'analisi e l'installazione in base a pianificazioni diverse. Per ulteriori informazioni, consulta [Configurare l'applicazione di patch per le istanze in un'organizzazione utilizzando un Configurazione rapida politica sulle patch](#) e [Configurazioni delle policy sulle patch in Configurazione rapida](#).
- Un'opzione di gestione degli host configurata in Quick Setup: le configurazioni di gestione degli host sono supportate anche dall'integrazione con AWS Organizations, che consente di eseguire un'operazione di patching per un massimo di un'intera organizzazione. Tuttavia, questa opzione si limita alla ricerca delle patch mancanti utilizzando l'attuale baseline delle patch predefinita e fornendo esiti nei report di conformità. Questo metodo operativo non è in grado di installare patch.

Per ulteriori informazioni, consulta [Configura la gestione degli host di Amazon EC2 utilizzando Configurazione rapida](#).

- Una finestra di manutenzione per eseguire un'attività di **Scan** o **Install** di patch è una finestra di manutenzione configurabile nello strumento di Systems Manager chiamato Maintenance Windows. Questa configurazione serve a eseguire diversi tipi di attività secondo una pianificazione definita dall'utente. Un'attività di tipo Run Command viene utilizzata per eseguire processi Scan o Scan and install in un set di nodi gestiti di tua scelta. Ogni attività della finestra di manutenzione può essere indirizzata ai nodi gestiti in una sola coppia Account AWS.Regione AWS Per ulteriori informazioni, consulta [Tutorial: creazione di una finestra di manutenzione per l'applicazione di patch tramite console](#).
- Un'operazione Patch now (Applica subito una patch) on demand in Patch Manager. L'opzione Patch now (Applica subito una patch) consente di ignorare le impostazioni di pianificazione quando è necessario applicare patch ai nodi gestiti il più rapidamente possibile. Con Patch now (Applica subito una patch), è possibile specificare se eseguire l'operazione Scan o Scan and install e scegliere i nodi gestiti sui cui eseguirla. È possibile inoltre scegliere di eseguire i documenti Systems Manager (documenti SSM) come hook del ciclo di vita durante l'applicazione di patch. Ogni operazione Patch now può essere indirizzata ai nodi gestiti in una sola Account AWSRegione AWS coppia. Per ulteriori informazioni, consulta [Patching dei nodi gestiti on demand](#).

Creazione di report di conformità

Dopo un'operazione Scan, è possibile utilizzare la console di Systems Manager per visualizzare le informazioni relative ai nodi gestiti che non sono conformi alle patch e alle patch mancanti per ciascun nodo. È possibile anche generare report di conformità alle patch in formato .csv inviati a un bucket Amazon Simple Storage Service (Amazon S3) di tua scelta. È possibile generare report una tantum o generare report in base a una pianificazione regolare. Per un singolo nodo, i report includono dettagli di tutte le patch per il nodo. Per un report su tutti i nodi gestiti, viene fornito solo un riepilogo del numero di patch mancanti. Dopo aver generato un report, puoi utilizzare uno strumento come Amazon Quick per importare e analizzare i dati. Per ulteriori informazioni, consulta [Utilizzo dei report sulla conformità delle patch](#).

Note

Un elemento di conformità generato tramite l'uso di una policy di patch ha un tipo di esecuzione PatchPolicy. Un elemento di conformità non generato in un'operazione di policy di patch presenta un tipo di esecuzione Command.

Integrazioni

Patch Manager si integra con le seguenti altre: Servizi AWS

- **AWS Identity and Access Management (IAM)** — Usa IAM per controllare quali utenti, gruppi e ruoli hanno accesso alle Patch Manager operazioni. Per ulteriori informazioni, consulta [In che modo AWS Systems Manager funziona con IAM](#) e [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#).
- **AWS CloudTrail**— Utilizzato CloudTrail per registrare una cronologia verificabile degli eventi delle operazioni di patching avviati da utenti, ruoli o gruppi. Per ulteriori informazioni, consulta [Registrazione dei log AWS Systems Manager Chiamate API con AWS CloudTrail](#).
- **AWS Security Hub CSPM**— I dati sulla conformità delle patch da Patch Manager possono essere inviati a. AWS Security Hub CSPM Security Hub CSPM offre una visione completa degli avvisi di sicurezza ad alta priorità e dello stato di conformità. Monitora anche lo stato di applicazione di patch del parco istanze. Per ulteriori informazioni, consulta [Integrazione Patch Manager con AWS Security Hub CSPM](#).
- **AWS Config**— Configura la registrazione AWS Config per visualizzare i dati di gestione delle istanze di Amazon EC2 nel dashboard. Patch Manager Per ulteriori informazioni, consulta [Visualizzazione dei riepiloghi del pannello di controllo delle patch](#).

Configurazioni delle policy sulle patch in Configurazione rapida

AWS consiglia l'uso di politiche sulle patch per configurare l'applicazione delle patch per la tua organizzazione e. Account AWS Le policy di patch sono state introdotte su Patch Manager a dicembre 2022.

Una politica di patch è una configurazione che si imposta utilizzando Quick Setup. Le policy di patch offrono un controllo più ampio e centralizzato sulle operazioni di applicazione di patch rispetto ai metodi precedenti. Le policy di patch possono essere utilizzate con [tutti i sistemi operativi supportati da Patch Manager](#), comprese le versioni supportate di Linux, macOS e Windows Server. Per istruzioni sulla creazione di una policy di patch, consulta [Configurare l'applicazione di patch per le istanze in un'organizzazione utilizzando un Configurazione rapida politica sulle patch](#).

Funzionalità principali delle politiche di patch

Invece di utilizzare altri metodi per applicare patch ai nodi, impiega una policy di patch per sfruttare le funzionalità principali seguenti:

- **Configurazione singola:** l'impostazione delle operazioni di applicazione di patch tramite una finestra di manutenzione o un'associazione State Manager può richiedere più attività in diverse parti della console di Systems Manager. Con una policy di patch, tutte le operazioni possono essere configurate in un'unica procedura guidata.
- **Multi-account/Multi-Region supporto:** utilizzando una finestra di manutenzione, un'associazione State Manager o la funzionalità Patch now di Patch Manager, puoi concentrare i nodi gestiti in una singola Account AWS/Regione AWS coppia. Se utilizzi più account e regioni, le attività di configurazione e manutenzione possono richiedere molto tempo a causa dell'esecuzione delle attività di impostazione in ciascuna coppia account-regione. Tuttavia, se lo utilizzi AWS Organizations, puoi impostare una policy di patch che si applichi a tutti i nodi gestiti Regioni AWS in tutto il tuo Account AWS. In alternativa, se lo desideri, è possibile applicare una policy di patch solo a determinate unità organizzative (UO) negli account e nelle regioni che scegli. Una policy di patch può essere applicata anche a un singolo account locale, se lo desideri.
- **Supporto all'installazione a livello organizzativo:** l'opzione di configurazione di gestione host esistente in Quick Setup fornisce supporto per una scansione giornaliera dei nodi gestiti al fine di verificare la conformità delle patch. Tuttavia, tale scansione viene eseguita in un momento prestabilito e genera solo informazioni sulla conformità delle patch, senza alcuna installazione. Utilizzando una policy di patch, è possibile specificare diverse pianificazioni per la scansione e l'installazione. È possibile anche scegliere la frequenza e l'ora in cui eseguire tali operazioni con espressioni CRON o Rate personalizzate. Ad esempio, è possibile eseguire la scansione giornaliera delle patch mancanti in modo da ottenere informazioni sulla conformità regolarmente aggiornate. La pianificazione dell'installazione, tuttavia, potrebbe essere prevista solo una volta alla settimana per evitare tempi di inattività indesiderati.
- **Selezione semplificata della baseline delle patch:** le policy di patch incorporano le baseline delle patch e non vi sono modifiche alla loro modalità di configurazione. Tuttavia, quando si crea o si aggiorna una policy di patch, è possibile selezionare la baseline AWS gestita o personalizzata che si desidera utilizzare per ogni tipo di sistema operativo (OS) in un unico elenco. Non è necessario specificare la baseline predefinita per ogni tipo di sistema operativo in attività separate.

Note

Durante l'applicazione di patch in base all'esecuzione di una policy di patch, si utilizza il documento SSM AWS-RunPatchBaseline. Per ulteriori informazioni, consulta [Documento di comando SSM per l'applicazione di patch: AWS-RunPatchBaseline](#).

Informazioni correlate

[Implementa centralmente le operazioni di patching in tutta AWS l'organizzazione utilizzando Systems Manager Quick Setup](#) (AWS Cloud Operations and Migrations Blog)

Altre differenze relative alle policy di patch

Di seguito sono riportate altre differenze da notare quando si utilizzano policy di patch anziché metodi precedenti:

- Non sono richiesti gruppi di patch: nelle precedenti operazioni di applicazione di patch, era possibile assegnare tag a più nodi appartenenti a un unico gruppo di patch e quindi specificare la baseline delle patch da utilizzare per tale gruppo. Se non si specificava alcun gruppo, Patch Manager applicava le patch alle istanze con la baseline delle patch predefinita corrente per il tipo di sistema operativo. Con le policy di patch, non è più necessario configurare e gestire gruppi di patch.

Note

La funzionalità dei gruppi di patch non è supportata nella console per le coppie account-Regione, che non utilizzavano già i gruppi di patch prima del rilascio del supporto per le policy di patch il 22 dicembre 2022. La funzionalità dei gruppi di patch è ancora disponibile nelle coppie account-Regione, che hanno iniziato a utilizzare i gruppi di patch prima di questa data.

- È stata rimossa la pagina "Configure patching" (Configurazione dell'applicazione di patch): prima del rilascio delle policy di patch, era possibile specificare l'operazione di applicazione di patch e i valori predefiniti per i nodi a cui applicarle nella pagina Configure patching (Configurazione dell'applicazione di patch). Questa pagina è stata rimossa da Patch Manager e le relative opzioni sono ora specificate nelle policy di patch.
- Nessun supporto «Patch now»: la possibilità di applicare patch ai nodi su richiesta è ancora limitata a una singola Account AWS coppia alla volta.Regione AWS Per informazioni, consulta [Patching dei nodi gestiti on demand](#).
- Policy di patch e informazioni sulla conformità: quando i nodi gestiti vengono analizzati per verificarne la conformità in base a una configurazione delle policy di patch, i dati sulla conformità vengono messi a disposizione dell'utente. È possibile visualizzare e utilizzare i dati nello stesso modo in cui impieghi altri metodi di scansione della conformità. Sebbene sia possibile impostare una politica di patch per un'intera organizzazione o per più unità organizzative, le informazioni sulla

conformità vengono riportate individualmente per ciascuna coppia Account AWS.Regione AWS Per ulteriori informazioni, consulta [Utilizzo dei report sulla conformità delle patch](#).

- Stato di conformità dell'associazione e policy di patch: lo stato di applicazione di patch per un nodo gestito soggetto a una policy Quick Setup di patch corrisponde allo stato dell'esecuzione dell'associazione State Manager per quel nodo. Quando lo stato di esecuzione dell'associazione è **Compliant**, anche lo stato di applicazione di patch per il nodo gestito viene contrassegnato come **Compliant**. Quando lo stato di esecuzione dell'associazione è **Non-Compliant**, anche lo stato di applicazione di patch per il nodo gestito viene contrassegnato come **Non-Compliant**.

Regioni AWS supportato per le politiche sulle patch

Le configurazioni delle policy di patch in Quick Setup sono attualmente supportate nelle seguenti regioni:

- Stati Uniti orientali (Ohio) (us-east-2)
- Stati Uniti orientali (Virginia settentrionale) (us-east-1)
- Stati Uniti occidentali (California settentrionale) (us-west-1)
- Stati Uniti occidentali (Oregon) (us-west-2)
- Asia Pacifico (Mumbai) (ap-south-1)
- Asia Pacifico (Seoul) (ap-northeast-2)
- Asia Pacifico (Singapore) (ap-southeast-1)
- Asia Pacifico (Sydney) (ap-southeast-2)
- Asia Pacifico (Tokyo) (ap-northeast-1)
- Canada (Centrale) (ca-central-1)
- Europa (Francoforte) (eu-central-1)
- Europa (Irlanda) (eu-west-1)
- Europa (Londra) (eu-west-2)
- Europa (Parigi) (eu-west-3)
- Europa (Stoccolma) (eu-north-1)
- Sud America (San Paolo) (sa-east-1)

Patch Manager prerequisiti

Assicuratevi di aver soddisfatto i prerequisiti richiesti prima di utilizzare Patch Manager uno strumento in. AWS Systems Manager

Agente SSM version

La Versione 2.0.834.0 o successiva SSM Agent è in esecuzione sui nodi gestiti che si desidera gestire con Patch Manager.

Note

Una versione aggiornata di SSM Agent viene distribuita ogni volta che vengono aggiunti nuovi strumenti a Systems Manager o eseguiti aggiornamenti degli strumenti esistenti. Il mancato utilizzo della versione più recente dell'agente può impedire al nodo gestito di utilizzare vari strumenti e funzionalità di Systems Manager. Per questo motivo, ti consigliamo di automatizzare il processo di aggiornamento di SSM Agent sulle macchine. Per informazioni, consulta [Automatizzazione degli aggiornamenti a Agente SSM](#). Iscriviti alla pagina [Note di rilascio di SSM Agent](#) su GitHub per ricevere notifiche sugli aggiornamenti di SSM Agent.

Versione di Python

Per macOS e la maggior parte dei sistemi operativi (OS) Linux, Patch Manager supporta attualmente le versioni di Python da 2.6 a 3.12. I Ubuntu Server sistemi operativi AlmaLinuxDebian Server, e richiedono una versione supportata di Python 3 (3.0 - 3.12).

Requisiti aggiuntivi del pacchetto

Per i sistemi DNF-based operativi, potrebbero essere necessarie unzip le utilità zstdxz, e per decomprimere le informazioni del repository e i file di patch. DNF-based i sistemi operativi includono Amazon Linux 2023, Red Hat Enterprise Linux 8 e versioni successive, Oracle Linux 8 e versioni successive,, Rocky Linux AlmaLinux, e CentOS 8 e versioni successive. Se visualizzi un errore simile a `No such file or directory: b'zstd'` o `No such file or directory: b'unxz'`, o errori nell'applicazione delle patch dovuti a una mancanza di unzip, devi installare queste utilità. zstd,xz, e unzip può essere installato eseguendo quanto segue:

```
dnf install zstd xz unzip
```

Connettività all'origine della patch

Se i nodi gestiti non dispongono di una connessione diretta a Internet e utilizzi un Amazon Virtual Private Cloud (Amazon VPC) con un endpoint VPC, devi assicurarti che i nodi abbiano accesso ai repository di patch di origine (repository). Nei nodi Linux, gli aggiornamenti delle patch vengono solitamente scaricati dai repository remoti configurati nel nodo. Pertanto, il nodo deve essere in grado di connettersi al repository, in modo che possa essere eseguita l'applicazione di patch. Per ulteriori informazioni, consulta [Come vengono selezionate le patch di sicurezza](#).

Quando applichi una patch a un nodo in esecuzione in un ambiente solo IPv6, assicurati che il nodo sia connesso alla fonte della patch. È possibile controllare l'Run Commandoutput dell'esecuzione delle patch per verificare la presenza di avvisi relativi a repository inaccessibili. Per i sistemi DNF-based operativi, è possibile configurare i repository non disponibili da ignorare durante l'applicazione delle patch se l'opzione è impostata su `under. skip_if_unavailable True /etc/dnf/dnf.conf`. DNF-basedi sistemi operativi includono Amazon Linux 2023, Red Hat Enterprise Linux 8 e versioni successive, Oracle Linux 8 e versioni successive, Rocky Linux AlmaLinux, e CentOS 8 e versioni successive. Su Amazon Linux 2023, l'`skip_if_unavailable` opzione è impostata su per impostazione `True` predefinita.

CentOS Stream: abilita la **EnableNonSecurity** bandiera

I nodi CentOS Stream utilizzano DNF come programma di gestione dei pacchetti, che si avvale del principio di avviso degli aggiornamenti. Un avviso di aggiornamento è semplicemente una raccolta di pacchetti per la risoluzione di problemi specifici.

Tuttavia, i repository CentOS Stream predefiniti non sono configurati con un avviso degli aggiornamenti. Ciò significa che Patch Manager non è in grado di rilevare i pacchetti in un repository CentOS Stream predefinito. Per abilitare Patch Manager all'elaborazione di pacchetti non sono contenuti in un avviso di aggiornamento, dovrai abilitare il flag **EnableNonSecurity** nelle regole di baseline delle patch.

Windows Server: garantisci la connettività al catalogo di Windows Update o a Windows Server Update Services (WSUS)

I nodi gestiti Windows Server devono essere in grado di connettersi al catalogo di Windows Update o a Windows Server Update Services (WSUS). Verificare che i nodi dispongano della connettività al [Catalogo Microsoft Update](#) tramite un gateway Internet, un gateway NAT o un'istanza NAT. Se si utilizza WSUS, verificare che il nodo disponga della connettività al server WSUS nell'ambiente in uso. Se un firewall limita il traffico in uscita, consenti i Microsoft domini richiesti. Windows Update Per

ulteriori informazioni sulla configurazione del firewall, consulta [Configurare il firewall per consentire al primo WSUS server di connettersi ai Microsoft domini su Internet](#) sul sito Web Learn. Microsoft Per ulteriori informazioni sui problemi di connettività, consulta. [Problema: il nodo gestito non ha accesso a Windows Update Catalog o WSUS](#)

Accesso agli endpoint S3

Indipendentemente dal fatto che i nodi gestiti operino in una rete privata o pubblica, senza accesso ai bucket AWS gestiti di Amazon Simple Storage Service (Amazon S3) richiesti, le operazioni di patching falliscono. Per informazioni sui bucket S3 a cui i nodi gestiti devono essere in grado di accedere, consulta [Agente SSM comunicazioni con AWS bucket S3 gestiti](#) e [Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager](#).

Autorizzazioni per installare le patch localmente

Sui sistemi operativi Linux e Windows Server, Patch Manager utilizza, rispettivamente, l'account amministratore e l'account utente root per installare le patch.

Ad ogni modo, su macOS, per Brew e Brew Cask, Homebrew non supporta i comandi eseguiti con l'account dell'utente root. Di conseguenza, Patch Manager esegue query e i comandi Homebrew come proprietario della directory Homebrew, oppure come utente valido appartenente al gruppo proprietario della directory Homebrew. Pertanto, per installare le patch, il proprietario della homebrew directory necessita anche di autorizzazioni ricorsive per la directory. `/usr/local`

Tip

Il comando seguente fornisce questa autorizzazione per l'utente specificato:

```
sudo chown -R $USER:admin /usr/local
```

Sistemi operativi supportati per Patch Manager

Lo strumento Patch Manager non supporta tutte le stesse versioni dei sistemi operativi supportate da altri strumenti di Systems Manager. (Per l'elenco completo dei sistemi Manager-supported operativi Systems, vedere [Sistemi operativi supportati per Systems Manager](#).) Pertanto, assicurati che i nodi gestiti con cui desideri utilizzare Patch Manager eseguano uno dei sistemi operativi elencati nella tabella seguente.

 Note

Patch Manager si basa sui repository di patch configurati su un nodo gestito, come Windows Update Catalog e Windows Server Update Services per Windows, in modo da recuperare le patch disponibili da installare. Pertanto, per le versioni del sistema operativo EOL (end of life), nel caso non siano disponibili nuovi aggiornamenti, Patch Manager potrebbe non essere in grado di segnalare i nuovi aggiornamenti. Ciò è dovuto al fatto che non vengono rilasciati nuovi aggiornamenti dal manutentore della distribuzione Linux, Microsoft o Apple, o perché il nodo gestito non dispone della licenza appropriata per accedervi.

Ti consigliamo vivamente di evitare di utilizzare versioni del sistema operativo che hanno raggiunto End-of-Life (EOL). I fornitori di sistemi operativi, tra cui AWS in genere, non forniscono patch di sicurezza o altri aggiornamenti per le versioni che hanno raggiunto il termine di scadenza. Continuare a utilizzare un sistema EOL aumenta notevolmente il rischio di non poter applicare gli aggiornamenti, comprese le correzioni di sicurezza, e altri problemi operativi. AWS non verifica la funzionalità di Systems Manager sulle versioni del sistema operativo che hanno raggiunto il termine di scadenza.

Patch Manager riporta lo stato di conformità rispetto alle patch disponibili sul nodo gestito. Pertanto, quando un'istanza esegue un sistema operativo EOL e non sono disponibili aggiornamenti, Patch Manager potrebbe segnalare il nodo come conforme, a seconda delle baseline delle patch configurate per la relativa operazione di applicazione.

Sistema operativo	Informazioni
Linux	<ul style="list-style-type: none">• AlmaLinux 8. x, 9 x.• Amazon Linux 2 versione 2.0 e tutte le versioni successive• Amazon Linux 2023• CentOS Stream 9• Debian Server 11.x e 12.x• Oracle Linux 7.5–8.x, 9.x• Red Hat Enterprise Linux (RHEL) 7.x–8.x, 9.x, 10.x• Rocky Linux 8.x, 9.x

Sistema operativo	Informazioni
	<ul style="list-style-type: none">• SUSE Linux Enterprise Server 15.3 e versioni successive• Ubuntu Server 18.04 LTS, 20.04 LTS, 22.04 LTS, 24.04 LTS e 25.04

Sistema operativo	Informazioni
macOS	<p>macOS è supportato solo per le istanze Amazon EC2.</p> <p>13.0-13.5 (Ventura)</p> <p>14.x (Sonoma)</p> <p>15.x (Sequoia)</p> <p>macOS Aggiornamenti del sistema operativo</p> <p>Patch Manager non supporta gli aggiornamenti del sistema operativo (OS) o quelli per macOS, ad esempio dalle versioni 13.1 a 13.2. Per eseguire gli aggiornamenti della versione del sistema operativo su macOS, consigliamo di utilizzare i meccanismi di aggiornamento del sistema operativo integrati di Apple. Per ulteriori informazioni, consulta Gestione del dispositivo sul sito Web della documentazione Apple Developer.</p> <p>Supporto Homebrew</p> <p>Patch Manager richiede l'installazione di Homebrew, il sistema di gestione dei pacchetti software open source, in una delle seguenti posizioni di installazione predefinite:</p> <ul style="list-style-type: none">• /usr/local/bin• /opt/homebrew/bin <p>Le operazioni di patching che utilizzano Patch Manager non funzionano correttamente quando Homebrew non è installato.</p> <p>Supporto delle Regioni</p>

Sistema operativo	Informazioni
	<p>macOS non è supportato in tutte le Regioni AWS. Per ulteriori informazioni sul supporto di Amazon EC2 per macOS, consulta Istanze Amazon EC2 Mac nella Guida per l'utente di Amazon EC2.</p> <p>macOS dispositivi edge</p> <p>SSM Agent per i dispositivi AWS IoT Greengrass principali non è supportato su macOS. Non è possibile utilizzare Patch Manager per applicare patch macOS Dispositivi Edge.</p>
Windows	<p>Da Windows Server 2012 a Windows Server 2025, incluse le versioni R2.</p> <div data-bbox="829 909 1507 1272"> <p> Note</p> <p>SSM Agent per i dispositivi di AWS IoT Greengrass base non è supportato in Windows 10. Non è possibile utilizzare Patch Manager per applicare patch ai dispositivi edge Windows 10.</p> </div> <p>Windows Server Supporto per 2012 e 2012 R2</p> <p>Windows Server 2012 e 2012 R2 hanno raggiunto la fine del supporto il 10 ottobre 2023. Per utilizzare Patch Manager con queste versioni, si consiglia di utilizzare anche gli Extended Security Updates (ESU) di Microsoft. Per ulteriori informazioni, consulta Raggiungi mento della fine del supporto di Windows Server 2012 e 2012 R2 sul sito Web di Microsoft.</p>

In che modo Patch Manager operazioni funzionano

Questa sezione fornisce i dettagli tecnici che illustrano come Patch Manager, uno strumento di AWS Systems Manager, determina le patch da installare e come vengono installate in ciascun sistema operativo supportato. Per i sistemi operativi Linux, fornisce inoltre informazioni su come specificare un repository di origine, in una baseline delle patch personalizzata, relativamente alle patch diverse da quella predefinita configurata in un nodo gestito. Questa sezione fornisce inoltre dettagli sulle regole della baseline delle patch in varie distribuzioni del sistema operativo Linux.

Note

Le informazioni contenute negli argomenti seguenti si applicano indipendentemente dal metodo o dal tipo di configurazione utilizzato per le operazioni di applicazione di patch:

- Una policy di patch configurata in Quick Setup
- Un'opzione di gestione host configurata in Quick Setup
- Una finestra di manutenzione per eseguire un'attività Scan o Install di patch
- Un'operazione Patch now (Applica subito una patch) on demand

Il modo in cui vengono calcolate le date di rilascio e di aggiornamento dei pacchetti

Important

Le informazioni in questa pagina si applicano ai sistemi operativi Amazon Linux 2 e Amazon Linux 2023 per istanze Amazon Elastic Compute Cloud (Amazon EC2). I pacchetti per questi tipi di sistema operativo sono creati e gestiti da Amazon Web Services. Il modo in cui i produttori di altri sistemi operativi gestiscono pacchetti e repository influisce sul modo in cui vengono calcolate le date di rilascio e di aggiornamento. Per sistemi operativi diversi da Amazon Linux 2 e Amazon Linux 2023, come Red Hat Enterprise Linux, consulta la documentazione del produttore per informazioni sul modo in cui i loro pacchetti vengono aggiornati e mantenuti.

Nelle impostazioni per le linee di base delle patch [personalizzate](#) che crei, per la maggior parte dei tipi di sistema operativo, puoi specificare che le patch vengano approvate automaticamente per l'installazione dopo un determinato numero di giorni. AWS fornisce diverse baseline predefinite delle patch che includono date di approvazione automatica di 7 giorni.

Il ritardo è il numero di giorni di attesa dopo il rilascio della patch, prima che questa venga automaticamente approvata per l'applicazione. Ad esempio, si crea una regola utilizzando la classificazione `CriticalUpdates` e si configura per un ritardo di approvazione automatica di 7 giorni. Di conseguenza, una nuova patch critica con una data di rilascio o l'ultimo aggiornamento al 7 luglio viene approvata automaticamente il 14 luglio.

Per evitare risultati imprevisti dovuti a ritardi nell'approvazione automatica su Amazon Linux 2 e Amazon Linux 2023, è importante capire il modo in cui vengono calcolate le date di rilascio e di aggiornamento.

Note

Se un repository Amazon Linux 2 o Amazon Linux 2023 non fornisce informazioni sulla data di rilascio per pacchetti, Patch Manager utilizza il tempo di compilazione del pacchetto come la data dell'approvazione automatica. Se non è possibile determinare il tempo di compilazione del pacchetto, Patch Manager utilizza una data predefinita del 1° gennaio 1970. Ciò comporta l'aggiornamento di qualsiasi specifica della data di approvazione automatica nelle baseline delle patch configurate per approvare le patch per qualsiasi data successiva al 1° gennaio 1970.

In genere, il tempo di attesa dell'approvazione automatica prima dell'installazione delle patch viene calcolato in base a un valore inserito, non a un `Updated Date` valore. `updateinfo.xml` Release Date Di seguito sono riportati dettagli importanti sui calcoli della data:

- **Release Date** è la data in cui viene rilasciato un avviso. Non significa che il pacchetto sia ancora necessariamente disponibile nei repository associati.
- **Update Date** è l'ultima data in cui l'avviso è stato aggiornato. Un aggiornamento a un avviso può rappresentare qualcosa di piccolo come aggiornamenti di testo o di descrizione. Non significa che il pacchetto sia stato rilasciato a partire da tale data o che sia ancora necessariamente disponibile nei repository associati.

Ciò significa che un pacchetto potrebbe avere un valore **Update Date** del 7 luglio ma non essere disponibile per l'installazione fino al 13 luglio (ad esempio). Supponiamo che, in questo caso, una baseline delle patch che specifichi un ritardo di approvazione automatica di 7 giorni venga eseguita in un'operazione `Install` il 14 luglio. Poiché il **Update Date** valore è 7 giorni prima della data di esecuzione, le patch e gli aggiornamenti del pacchetto vengono installati il 14 luglio.

L'installazione avviene anche se è passato solo 1 giorno da quando il pacchetto risulta disponibile per l'installazione effettiva.

- Un pacchetto con le patch del sistema operativo o dell'applicazione può essere aggiornato più di una volta dopo il rilascio iniziale.
- Un pacchetto può essere rilasciato nei repository AWS gestiti ma poi ripristinato se in seguito vengono rilevati problemi con esso.

In alcune operazioni di applicazione di patch, questi fattori potrebbero non essere rilevanti. Ad esempio, se una baseline delle patch è configurata per installare una patch con valori di gravità di Low e Medium, e una classificazione di Recommended, qualsiasi ritardo nell'approvazione automatica potrebbe avere un impatto minimo sulle tue operazioni.

Tuttavia, nei casi in cui la tempistica delle patch critiche o con alto livello di gravità è più importante, potrebbe essere opportuno esercitare un maggiore controllo sul momento in cui le patch vengono installate. Il metodo suggerito per questa operazione consiste nell'utilizzare repository alternativi di origine delle patch anziché i repository predefiniti per le operazioni di applicazione di patch su un nodo gestito.

È possibile specificare repository alternativi di origine delle patch al momento della creazione di una baseline delle patch personalizzata. In ciascuna baseline delle patch personalizzata, è possibile specificare le configurazioni di origine delle patch per un massimo di 20 versioni di un sistema operativo Linux supportato. Per ulteriori informazioni, consulta [Come specificare un repository alternativo di origine delle patch \(Linux\)](#).

Come vengono selezionate le patch di sicurezza

L'obiettivo principale di Patch Manager è l'installazione degli aggiornamenti relativi alla sicurezza dei sistemi operativi sui nodi gestiti. Per impostazione predefinita, Patch Manager non installa tutte le patch disponibili, ma solo una serie limitata di patch relative alla sicurezza.

Per impostazione predefinita, Patch Manager non sostituisce un pacchetto contrassegnato come obsoleto in un archivio di pacchetti con pacchetti sostitutivi con nomi diversi, a meno che tale sostituzione non sia richiesta dall'installazione di un altro aggiornamento del pacchetto. Invece, per i comandi che aggiornano un pacchetto, segnala e installa Patch Manager solo gli aggiornamenti mancanti per il pacchetto installato ma obsoleto. Questo perché la sostituzione di un pacchetto obsoleto richiede in genere la disinstallazione di un pacchetto esistente e l'installazione del pacchetto sostitutivo. La sostituzione del pacchetto obsoleto potrebbe introdurre modifiche sostanziali o funzionalità aggiuntive non previste.

Questo comportamento è coerente con il comando `update-minimal` di YUM e DNF, che si concentra sugli aggiornamenti di sicurezza piuttosto che sugli quelli delle funzionalità. Per ulteriori informazioni, consulta [Come vengono installate le patch](#).

Note

Quando si utilizza il `ApproveUntilDate` parametro o il `ApproveAfterDays` parametro in una regola di base della patch, Patch Manager valuta le date di rilascio delle patch utilizzando il Coordinated Universal Time (UTC).

Ad esempio, se si specifica una `dataApproveUntilDate`, ad esempio `2025-11-16`, le patch rilasciate tra `2025-11-16T00:00:00Z` e `2025-11-16T23:59:59Z` saranno approvate.

Tieni presente che le date di rilascio delle patch visualizzate dai gestori di pacchetti nativi sui nodi gestiti possono mostrare orari diversi in base al fuso orario locale del sistema, ma utilizzano Patch Manager sempre la data e l'ora UTC per i calcoli di approvazione. Ciò garantisce la coerenza con le date di rilascio delle patch pubblicate sui siti Web ufficiali di avviso di sicurezza.

Per i tipi di sistema Linux-based operativo che segnalano un livello di gravità per le patch, Patch Manager utilizza il livello di gravità riportato dal produttore del software per l'avviso di aggiornamento o la singola patch. Patch Manager non deriva i livelli di gravità da fonti di terze parti, come il [Common Vulnerability Scoring System](#) (CVSS), o dalle metriche rilasciate dal National Vulnerability Database (NVD). <https://nvd.nist.gov/vuln>

Note

Su tutti i Linux-based sistemi supportati da Patch Manager, è possibile scegliere un repository di origine diverso configurato per il nodo gestito, in genere per installare aggiornamenti non di sicurezza. Per informazioni, consulta [Come specificare un repository alternativo di origine delle patch \(Linux\)](#).

Nella parte restante di questa sezione viene illustrato come Patch Manager seleziona le patch di sicurezza per i vari sistemi operativi supportati.

Amazon Linux 2 and Amazon Linux 2023

I repository preconfigurati vengono gestiti in modo diverso su Amazon Linux 2 rispetto a Amazon Linux 2023.

In Amazon Linux 2, il servizio della baseline delle patch di Systems Manager utilizza repository preconfigurati nel nodo gestito. In genere in un nodo sono disponibili due repository (repo) preconfigurati:

Su Amazon Linux 2

- ID repository: `amzn2-core/2/architecture`

Nome repository: Amazon Linux 2 core repository

- ID repository: `amzn2extra-docker/2/architecture`

Nome repository: Amazon Extras repo for docker

Note

architecture può essere `x86_64` o (per i processori Graviton) `aarch64`.

Quando crei un'istanza di Amazon Linux 2023 (AL2023), questa contiene gli aggiornamenti che erano disponibili nella versione di AL2023 e le AMI specifiche selezionate. Per impostazione predefinita, l'istanza AL2023 non riceve automaticamente aggiornamenti di sicurezza critici e importanti aggiuntivi al momento dell'avvio. Invece, con la funzionalità degli aggiornamenti deterministici tramite repository con versioni supportate per AL2023, attivata per impostazione predefinita, è possibile applicare gli aggiornamenti in base a una pianificazione che soddisfi le tue esigenze specifiche. Per ulteriori informazioni, consulta [Aggiornamenti deterministici tramite repository con versioni](#) nella Guida per l'utente di Amazon Linux 2023.

Su AL 2023, il repository preconfigurato è il seguente:

- ID repository: `amazonlinux`

Nome del repository: repository Amazon Linux 2023

Su Amazon Linux 2023 (rilascio in anteprima), i repository preconfigurati sono legati a versioni bloccate degli aggiornamenti dei pacchetti. Quando vengono rilasciate nuove Amazon Machine Images (AMIs) per AL2023, queste vengono bloccate a una versione specifica. Per gli aggiornamenti delle patch, Patch Manager recupera l'ultima versione bloccata del repository degli aggiornamenti delle patch, quindi aggiorna i pacchetti sul nodo gestito in base al contenuto di quella versione bloccata.

Funzionalità di gestione dei pacchetti.

I nodi gestiti da Amazon Linux 2 utilizzano Yum come gestore di pacchetti. Amazon Linux 2023 utilizza DNF come gestore di pacchetti.

Entrambi i gestori di pacchetti utilizzano il concetto di avviso di aggiornamento come un file denominato `updateinfo.xml`. Un avviso di aggiornamento è semplicemente una raccolta di pacchetti per la risoluzione di problemi specifici. Tutti i pacchetti di un avviso di aggiornamento sono considerati di sicurezza da Patch Manager. Ai singoli pacchetti non vengono assegnati classificazioni o livelli di gravità. Per questo motivo, Patch Manager assegna gli attributi di un avviso di aggiornamento ai pacchetti correlati.

Note

Se si seleziona la casella di controllo Includi aggiornamenti non critici nella pagina Crea baseline delle patch, i pacchetti non classificati in un file `updateinfo.xml` (o in un pacchetto che contiene un file per il quale i valori relativi a classificazione, gravità e data non sono formattati in modo appropriato) possono essere inclusi nell'elenco di patch prefiltrato. Tuttavia, per applicare una patch, la patch deve comunque soddisfare le regole di base della patch specificate dall'utente.

Per ulteriori informazioni sull'opzione Includi aggiornamenti non critici, consulta [Come vengono installate le patch](#) e [Come funzionano le regole di base delle patch sui sistemi Linux-based](#).

CentOS Stream

In CentOS Stream, il servizio della baseline delle patch di Systems Manager utilizza repository preconfigurati (repository) nel nodo gestito. L'elenco seguente fornisce esempi per un fittizio CentOS 9.2 Amazon Machine Image (AMI):

- ID repository: `example-centos-9.2-base`

Nome repository: `Example CentOS-9.2 - Base`

- ID repository: `example-centos-9.2-extras`

Nome repository: `Example CentOS-9.2 - Extras`

- ID repository: `example-centos-9.2-updates`

Nome repository: `Example CentOS-9.2 - Updates`

- ID repository: `example-centos-9.x-exemplerepo`

Nome repository: `Example CentOS-9.x - Example Repo Packages`

 Note

Tutti gli aggiornamenti vengono scaricati dai repo remoti configurati nel nodo. Pertanto, il nodo deve disporre dell'accesso in uscita a Internet per connettersi ai repository in modo da poter eseguire l'applicazione delle patch.

I nodi CentOS Stream utilizzano DNF come gestore di pacchetti. Entrambi i gestori di pacchetti utilizzano il concetto di avviso degli aggiornamenti. Un avviso di aggiornamento è semplicemente una raccolta di pacchetti per la risoluzione di problemi specifici.

Tuttavia, i repository CentOS Stream predefiniti non sono configurati con un avviso degli aggiornamenti. Ciò significa che Patch Manager non è in grado di rilevare i pacchetti in un repository CentOS Stream predefinito. Per abilitare Patch Manager all'elaborazione di pacchetti non sono contenuti in un avviso di aggiornamento, dovrai abilitare il flag `EnableNonSecurity` nelle regole di baseline delle patch.

 Note

Gli avvisi degli aggiornamenti CentOS Stream sono supportati. Potrai scaricare i repo con avvisi di aggiornamento dopo l'avvio.

Debian Server

In Debian Server, il servizio della baseline delle patch di Systems Manager utilizza repository preconfigurati (repository) nell'istanza. Questi repo preconfigurati vengono utilizzati per estrarre un elenco aggiornato degli aggiornamenti dei pacchetti disponibili. A tale scopo, Systems Manager esegue l'equivalente di un comando `sudo apt-get update`.

I pacchetti vengono quindi filtrati da repo `debian-security` *codename*. Ciò significa che in ogni versione di Debian Server, Patch Manager identifica solo gli aggiornamenti che fanno parte del repository associato a quella versione, come segue:

- Debian Server11: `debian-security bullseye`
- Debian Server12: `debian-security bookworm`

Oracle Linux

In Oracle Linux, il servizio della baseline delle patch di Systems Manager utilizza repository preconfigurati (repository) nel nodo gestito. In genere in un nodo sono disponibili due repo preconfigurati:

Oracle Linux 7:

- ID repository: `o17_UEKR5/x86_64`

Nome repository: `Latest Unbreakable Enterprise Kernel Release 5 for Oracle Linux 7Server (x86_64)`

- ID repository: `o17_latest/x86_64`

Nome repository: `Oracle Linux 7Server Latest (x86_64)`

Oracle Linux 8:

- ID repository: `o18_baseos_latest`

Nome repository: `Oracle Linux 8 BaseOS Latest (x86_64)`

- ID repository: `o18_appstream`

Nome repository: `Oracle Linux 8 Application Stream (x86_64)`

- ID repository: `o18_UEKR6`

Nome repository: Latest Unbreakable Enterprise Kernel Release 6 for Oracle Linux 8 (x86_64)

Oracle Linux 9:

- ID repository: ol9_baseos_latest

Nome repository: Oracle Linux 9 BaseOS Latest (x86_64)

- ID repository: ol9_appstream

Nome repository: Oracle Linux 9 Application Stream Packages(x86_64)

- ID repository: ol9_UEKR7

Nome repository: Oracle Linux UEK Release 7 (x86_64)

Note

Tutti gli aggiornamenti vengono scaricati dai repo remoti configurati nel nodo. Pertanto, il nodo deve avere accesso in uscita a Internet per connettersi ai repository in modo da poter eseguire l'applicazione delle patch.

I nodi gestiti di Oracle Linux utilizzano Yum come programma di gestione dei pacchetti e Yum si avvale del principio dell'avviso di aggiornamento sotto forma di file denominato `updateinfo.xml`. Un avviso di aggiornamento è semplicemente una raccolta di pacchetti per la risoluzione di problemi specifici. Ai singoli pacchetti non vengono assegnati classificazioni o livelli di gravità. Per questo motivo, Patch Manager assegna gli attributi di un avviso di aggiornamento ai pacchetti correlati e installa i pacchetti in base ai filtri di classificazione specificati nella baseline delle patch.

Note

Se si seleziona la casella di controllo Includi aggiornamenti non critici nella pagina Crea baseline delle patch, i pacchetti non classificati in un file `updateinfo.xml` (o in un pacchetto che contiene un file per il quale i valori relativi a classificazione, gravità e data non sono formattati in modo appropriato) possono essere inclusi nell'elenco di patch

prefiltrato. Tuttavia, per applicare una patch, la patch deve comunque soddisfare le regole di base della patch specificate dall'utente.

AlmaLinux, RHEL, and Rocky Linux

Attivato AlmaLinuxRed Hat Enterprise Linux, e Rocky Linux il servizio di base delle patch di Systems Manager utilizza repository preconfigurati (repository) sul nodo gestito. In genere in un nodo sono disponibili tre repo preconfigurati:

Tutti gli aggiornamenti vengono scaricati dai repo remoti configurati nel nodo. Pertanto, il nodo deve avere accesso in uscita a Internet per connettersi ai repository in modo da poter eseguire l'applicazione delle patch.

Note

Se si seleziona la casella di controllo Includi aggiornamenti non critici nella pagina Crea baseline delle patch, i pacchetti non classificati in un file `updateinfo.xml` (o in un pacchetto che contiene un file per il quale i valori relativi a classificazione, gravità e data non sono formattati in modo appropriato) possono essere inclusi nell'elenco di patch prefiltrato. Tuttavia, per applicare una patch, la patch deve comunque soddisfare le regole di base della patch specificate dall'utente.

Red Hat Enterprise Linux7 nodi gestiti utilizzano Yum come gestore di pacchetti. AlmaLinux, Red Hat Enterprise Linux 8 e i nodi Rocky Linux gestiti utilizzano DNF come gestore di pacchetti. Entrambi i gestori di pacchetti utilizzano il concetto di avviso di aggiornamento come file denominato `updateinfo.xml`. Un avviso di aggiornamento è semplicemente una raccolta di pacchetti per la risoluzione di problemi specifici. Ai singoli pacchetti non vengono assegnati classificazioni o livelli di gravità. Per questo motivo, Patch Manager assegna gli attributi di un avviso di aggiornamento ai pacchetti correlati e installa i pacchetti in base ai filtri di classificazione specificati nella baseline delle patch.

Note

Su AlmaLinux e Rocky Linux, i repository non possono conservare le versioni precedenti di un pacchetto una volta rilasciata una versione più recente con lo stesso nome di pacchetto. Se un avviso di aggiornamento fa riferimento a una versione che non è più disponibile nel repository, Patch Manager valuta l'installazione della versione più

recente utilizzando i metadati di avviso pubblicati per la versione non più disponibile. Ciò garantisce che le patch in sospeso vengano applicate quando la versione non disponibile non è più presente nel repository.

Ciò può Patch Manager comportare l'installazione di versioni più recenti del pacchetto anche se l'avviso associato è stato rilasciato dopo la configurazione o.

`ApproveUntilDate ApproveAfterDays`

RHEL 7

Note

I seguenti ID repository sono associati a RHUI 2. RHUI 3 è stato lanciato nel dicembre 2019 e ha introdotto un diverso schema di denominazione per gli ID repository Yum. A seconda del tipo da RHEL-7 AMI cui vengono creati i nodi gestiti, potrebbe essere necessario aggiornare i comandi. Per ulteriori informazioni, consultate [Repository ID for RHEL 7 in AWS Have Changed](#) sul Red Hat Customer Portal.

- ID repository: `rhui-REGION-client-config-server-7/x86_64`

Nome repository: Red Hat Update Infrastructure 2.0 Client Configuration Server 7

- ID repository: `rhui-REGION-rhel-server-releases/7Server/x86_64`

Nome repository: Red Hat Enterprise Linux Server 7 (RPMs)

- ID repository: `rhui-REGION-rhel-server-rh-common/7Server/x86_64`

Nome repository: Red Hat Enterprise Linux Server 7 RH Common (RPMs)

AlmaLinux, 8, RHEL 8 e Rocky Linux 8

- ID repository: `rhel-8-appstream-rhui-rpms`

Nome repository: Red Hat Enterprise Linux 8 for x86_64 - AppStream from RHUI (RPMs)

- ID repository: `rhel-8-baseos-rhui-rpms`

Nome repository: Red Hat Enterprise Linux 8 for x86_64 - BaseOS from RHUI (RPMs)

- ID repository: `rhui-client-config-server-8`

Nome repository: Red Hat Update Infrastructure 3 Client Configuration Server 8

AlmaLinux 9, RHEL 9 e Rocky Linux 9

- ID repository: `rhel-9-appstream-rhui-rpms`

Nome repository: Red Hat Enterprise Linux 9 for x86_64 - AppStream from RHUI (RPMs)

- ID repository: `rhel-9-baseos-rhui-rpms`

Nome repository: Red Hat Enterprise Linux 9 for x86_64 - BaseOS from RHUI (RPMs)

- ID repository: `rhui-client-config-server-9`

Nome repository: Red Hat Enterprise Linux 9 Client Configuration

SLES

Nei nodi gestiti SUSE Linux Enterprise Server (SLES), la libreria ZYPP ottiene l'elenco delle patch disponibili (una raccolta di pacchetti) dai seguenti percorsi:

- Elenco di repository: `etc/zypp/repos.d/*`
- Informazioni sui pacchetti: `/var/cache/zypp/raw/*`

I nodi gestiti SLES utilizzano Zypper come programma di gestione dei pacchetti e Zypper si avvale del principio di una patch. Una patch è semplicemente una raccolta di pacchetti per la risoluzione di un problema specifico. Patch Manager gestisce tutti i pacchetti a cui fa riferimento in una patch come correlati alla sicurezza. Poiché ai singoli pacchetti non viene attribuita alcuna classificazione o gravità, Patch Manager assegna ai pacchetti gli attributi della patch a cui appartengono.

Ubuntu Server

In Ubuntu Server, il servizio della baseline delle patch di Systems Manager utilizza repository preconfigurati (repository) nel nodo gestito. Questi repo preconfigurati vengono utilizzati per estrarre un elenco aggiornato degli aggiornamenti dei pacchetti disponibili. A tale scopo, Systems Manager esegue l'equivalente di un comando `sudo apt-get update`.

I pacchetti vengono quindi filtrati dai *codename*-security repository, dove il nome in codice è univoco per la versione di rilascio, ad esempio per 25.04. plucky Ubuntu Server Patch Manager identifica solo gli aggiornamenti che fanno parte di questi repository:

- Ubuntu Server 18.04 LTS: bionic-security
- Ubuntu Server 20.04 LTS: focal-security
- Ubuntu Server 22.04 LTS: jammy-security
- Ubuntu Server 24.04 LTS: noble-security
- Ubuntu Server 25.04: plucky-security

Windows Server

Nei sistemi operativi Microsoft Windows, Patch Manager consente di recuperare l'elenco degli aggiornamenti disponibili pubblicati da Microsoft e sono automaticamente disponibili su Windows Server Update Services (WSUS).

Note

Patch Manager rende disponibili esclusivamente le patch disponibili per le versioni del sistema operativo Windows Server che sono supportate per Patch Manager. Ad esempio, Patch Manager non può essere utilizzato per applicare patch a Windows RT.

Patch Manager effettua un monitoraggio continuo per nuovi aggiornamenti in ogni Regione AWS. L'elenco degli aggiornamenti disponibili viene aggiornato in ciascuna regione almeno una volta al giorno. Man mano che Microsoft elabora le informazioni sulle patch, Patch Manager rimuove dall'elenco gli aggiornamenti che sono stati sostituiti da quelli successivi. Pertanto, viene visualizzato e può essere installato solo l'aggiornamento più recente. Ad esempio, se KB4012214 sostituisce KB3135456, solo KB4012214 viene reso disponibile come aggiornamento in Patch Manager.

Allo stesso modo, Patch Manager installa solo le patch disponibili sul nodo gestito durante l'operazione di applicazione di patch. Per impostazione predefinita, Windows Server 2019 e Windows Server 2022 rimuovono gli aggiornamenti che vengono sostituiti da quelli successivi. Di conseguenza, quando si utilizza il parametro `ApproveUntilDate` in una baseline delle patch di Windows Server, ma la data selezionata nel parametro `ApproveUntilDate` è precedente alla data dell'ultima patch, si verifica lo scenario seguente:

- La patch sostituita viene rimossa dal nodo e pertanto non è in grado di essere installata utilizzando Patch Manager.
- La patch sostitutiva più recente è presente sul nodo ma non è ancora stata approvata per l'installazione in base alla data specificata dal parametro `ApproveUntilDate`.

 Le patch sostituite possono creare una lacuna di conformità

Il nodo gestito potrebbe dichiararsi conforme per le operazioni di Systems Manager anche se non è installata una patch critica del mese precedente. Questo scenario può verificarsi anche con il `ApproveAfterDays` parametro.

A causa del comportamento delle patch sostituite da Microsoft, è possibile impostare un valore (in genere maggiore di 30) in modo che le patch per non Windows Server vengano mai installate se Microsoft rilascia la patch più recente prima che sia trascorso quel numero di giorni. In questa situazione, il nodo gestito potrebbe risultare conforme anche se non sono installate patch di sicurezza critiche.

Ad esempio, impostato su `ApproveAfterDays 45`. Se Microsoft rilascia una patch sostitutiva il giorno 30, il sistema rimuove la patch originale. La nuova patch non viene approvata fino al giorno 45, lasciando una finestra di 15 giorni in cui nessuna delle patch è installata.

Questo comportamento non si applica se hai modificato le impostazioni di Windows Group Policy Object (GPO) per rendere disponibile la patch sostituita nei nodi gestiti.

 Note

In alcuni casi, Microsoft rilascia patch per applicazioni che non specificano una data e un'ora aggiornate. In questi casi, una data e un'ora aggiornate di 01/01/1970 viene fornito per impostazione predefinita.

Come specificare un repository alternativo di origine delle patch (Linux)

Quando utilizzi i repository predefiniti configurati su un nodo gestito per le operazioni di applicazione delle patch, cerca o installa le patch Patch Manager relative alla sicurezza. Questo è il comportamento predefinito per Patch Manager. Per informazioni dettagliate sulle modalità in cui

Patch Manager seleziona e installa le patch di sicurezza, consulta [Come vengono selezionate le patch di sicurezza](#).

Nei sistemi Linux, tuttavia, è possibile anche usare Patch Manager per installare patch non correlate alla sicurezza o che si trovano in un repository di origine diverso da quello di default configurato nel nodo gestito. È possibile specificare repository alternativi di origine delle patch al momento della creazione di una baseline delle patch personalizzata. In ciascuna baseline delle patch personalizzata, è possibile specificare le configurazioni di origine delle patch per un massimo di 20 versioni di un sistema operativo Linux supportato.

Ad esempio, supponiamo che il tuo parco istanze Ubuntu Server includa anche nodi Ubuntu Server 25.04 gestiti. In questo caso è possibile specificare repository alternativi per ciascuna versione nella stessa baseline delle patch personalizzata. Per ciascuna versione, sarà necessario specificare un nome, il tipo di versione del sistema operativo (prodotto) e fornire una configurazione del repository. È possibile anche specificare un singolo repository di origine alternativo valido per tutte le versioni di un sistema operativo supportato.

Note

L'esecuzione di una baseline delle patch di base personalizzata che specifica repository di patch alternativi per un nodo gestito non li rende i nuovi repository di default del sistema operativo. Al termine dell'operazione di applicazione di patch, i repository precedentemente definiti come valori predefiniti del sistema operativo del nodo rimangono valori predefiniti.

Per un elenco di scenari di esempio per l'utilizzo di questa opzione, consulta [Utilizzi di esempio per repository alternativi di origine delle patch](#) più avanti in questo argomento.

Per informazioni sulle baseline delle patch predefinite e personalizzate, consulta [Baseline delle patch predefinite e personalizzate](#).

Esempio: utilizzo della console

Per specificare repository alternativi di origine delle patch con la console Systems Manager, utilizza la sezione Origini patch della pagina Creazione di una baseline delle patch. Per ulteriori informazioni sull'utilizzo delle opzioni Patch sources (Origini patch), consulta [Creazione di una baseline delle patch personalizzata per Linux](#).

Esempio: utilizzo di AWS CLI

Per un esempio di utilizzo dell'opzione `--sources` con AWS Command Line Interface (AWS CLI), consulta [Creazione di una baseline delle patch con repository personalizzati per varie versioni dei sistemi operativi](#).

Considerazioni importanti sui repository alternativi

Durante la pianificazione della strategia di applicazione di patch con repository alternativi, tieni presente quanto segue:

Applica le verifiche degli aggiornamenti dei repository (YUM e DNF)

Una configurazione predefinita per un gestore di pacchetti su una distribuzione Linux potrebbe essere impostata per ignorare un repository di pacchetti irraggiungibile se non è possibile stabilire la connessione al repository. Per imporre la verifica degli aggiornamenti del repository, aggiungili alla configurazione del repository. `skip_if_unavailable=False`

Per ulteriori informazioni sull'opzione `skip_if_available`, consulta [Connettività all'origine della patch](#).

Per l'applicazione di patch vengono utilizzati solo i repository specificati

La specifica di repository alternativi non comporta l'aggiunta di altri repository. È possibile scegliere di specificare repository diversi da quelli configurati come predefiniti in un nodo gestito. Tuttavia, per fare in modo che vengano applicati i relativi aggiornamenti, dovrai anche specificare i repository predefiniti come parte della configurazione dell'origine delle patch alternativa.

Ad esempio, su tutti i nodi gestiti Amazon Linux 2, i repository di default sono `amzn2-core` e `amzn2extra-docker`. Se desideri includere il repository Extra Packages for Enterprise Linux (EPEL) nelle operazioni di applicazione di patch, dovrai specificare tutti i tre repository come repository alternativi.

Note

L'esecuzione di baseline delle patch personalizzata che specifica repository di patch alternativi per un nodo gestito non li rende nuovi repository predefiniti del sistema operativo. Al termine dell'operazione di applicazione di patch, i repository precedentemente definiti come valori predefiniti del sistema operativo del nodo rimangono valori predefiniti.

Il comportamento di applicazione delle patch per le YUM-based distribuzioni dipende dal manifesto `updateinfo.xml`

Quando si specificano repository di patch alternativi per le YUM-based distribuzioni, come Amazon Linux 2, oRed Hat Enterprise Linux, il comportamento di applicazione delle patch dipende dal fatto che il repository includa un manifesto di aggiornamento sotto forma di file completo e formattato correttamente. `updateinfo.xml` Questo file specifica la data di rilascio, le classificazioni e le gravità dei vari pacchetti. Una qualsiasi delle seguenti attività inciderà sul comportamento dell'applicazione di patch:

- Se applichi filtri in base alla classificazione e alla gravità, ma queste non sono specificate in `updateinfo.xml`, il pacchetto non verrà incluso dal filtro. Ciò significa anche che i pacchetti senza un file `updateinfo.xml` non saranno inclusi nell'applicazione di patch.
- Se si filtra su `ApprovalAfterDays`, ma la data di rilascio del pacchetto non è in formato Unix Epoch (o non è specificata una data di rilascio), il pacchetto non verrà incluso dal filtro.
- Si verifica un'eccezione se selezioni la casella di controllo Includi aggiornamenti non critici nella pagina Crea baseline delle patch. In questo caso, i pacchetti senza un file `updateinfo.xml` (o quelli contenenti questo file senza i valori Classification (Classificazione), Severity (Gravità) e Date (Data) formattati correttamente) saranno inclusi nell'elenco prefiltrato delle patch. (Devono comunque soddisfare gli altri requisiti delle regole di base delle patch per essere installati.)

Utilizzi di esempio per repository alternativi di origine delle patch

Esempio 1: aggiornamenti non di sicurezza per Ubuntu Server

Lo stai già utilizzando Patch Manager per installare patch di sicurezza su una flotta di nodi Ubuntu Server gestiti utilizzando la linea di base delle patch predefinita AWS fornita. `AWS-UbuntuDefaultPatchBaseline` È possibile creare una nuova baseline delle patch basata su quella predefinita, specificando però nelle regole di approvazione che desideri installare anche aggiornamenti non correlati alla sicurezza che fanno parte della distribuzione predefinita. Quando questa baseline delle patch viene eseguita nei tuoi nodi, vengono applicate le patch sia per le problematiche relative alla sicurezza sia per quelle di altro tipo. È possibile scegliere di approvare le patch non correlate alla sicurezza anche nelle eccezioni specificate per una baseline.

Esempio 2 - Personal Package Archives (PPA) per Ubuntu Server

I nodi gestiti di Ubuntu Server eseguono un software distribuito tramite un [Personal Package Archives \(PPA\) per Ubuntu](#). In questo caso, devi creare una baseline delle patch che specifichi un repository PPA configurato nei nodi gestiti come repository di origine per l'applicazione di patch. Sarà quindi possibile utilizzare Run Command per eseguire il documento della baseline delle patch nei nodi.

Esempio 3: applicazioni aziendali interne in versioni Amazon Linux supportate

Nei nodi gestiti Amazon Linux, devi eseguire alcune applicazioni necessarie per la conformità normativa del settore. È possibile configurare un repository per queste applicazioni nei nodi, utilizzare YUM per installare inizialmente le applicazioni, quindi aggiornare o creare una nuova baseline delle patch per includere il nuovo repository aziendale. Successivamente, potrai utilizzare Run Command per eseguire il documento AWS-RunPatchBaseline con l'opzione Scan per assicurarti che il pacchetto aziendale sia elencato tra quelli installati e sia aggiornato nel nodo gestito. Se non è aggiornato, è possibile eseguire nuovamente il documento con l'opzione Install per aggiornare le applicazioni.

Come vengono installate le patch

Patch Manager utilizza il gestore di pacchetti integrato nel sistema operativo per installare gli aggiornamenti sui nodi gestiti. Ad esempio, utilizza l'API di Windows Update su Windows Server e DNF su Amazon Linux 2023. Patch Manager rispetta le configurazioni esistenti del gestore di pacchetti e del repository sui nodi, incluse impostazioni come lo stato del repository, gli URL mirror, la verifica GPG e opzioni simili. `skip_if_unavailable`

Patch Manager non installa un nuovo pacchetto che sostituisce uno obsoleto attualmente installato. (Eccezioni: il nuovo pacchetto è una dipendenza di un altro pacchetto in fase di aggiornamento che è stato installato oppure il nuovo pacchetto ha lo stesso nome del pacchetto obsoleto.) Al contrario, Patch Manager segnala e installa gli aggiornamenti disponibili per i pacchetti installati. Questo approccio aiuta a prevenire modifiche impreviste alla funzionalità del sistema che potrebbero verificarsi quando un pacchetto ne sostituisce un altro.

Se è necessario disinstallare un pacchetto divenuto obsoleto e installarne il sostituto, potrebbe essere necessario utilizzare uno script personalizzato o utilizzare comandi di gestione del pacchetto al di fuori delle operazioni Patch Manager standard.

Nella parte restante di questa sezione viene illustrato come Patch Manager installa le patch in un sistema operativo.

Amazon Linux 2 and Amazon Linux 2023

Di seguito è riportato il flusso di lavoro di installazione delle patch nei nodi gestiti da Amazon Linux 2 e Amazon Linux 2023:

1. Se un elenco delle patch viene specificato utilizzando un URL https o un URL in stile percorso Amazon Simple Storage Service (Amazon S3) utilizzando il parametro

`InstallOverrideList` per i documenti `AWS-RunPatchBaseline` o `AWS-RunPatchBaselineAssociation`, vengono installate le patch elencate e vengono ignorate le fasi 2-7.

2. Applicare [GlobalFilters](#) come specificato nella baseline delle patch, mantenendo solo i pacchetti qualificati per un'ulteriore elaborazione.
3. Applica [ApprovalRules](#) come specificato nella baseline delle patch. Ciascuna regola di approvazione è in grado di definire un pacchetto come approvato.

Le norme di approvazione, tuttavia, sono anche soggette al fatto che la casella di spunta `Includi aggiornamenti non correlati alla protezione` è stata selezionata durante la creazione o l'ultimo aggiornamento di una baseline delle patch.

Se sono esclusi aggiornamenti non di sicurezza, viene applicata una regola implicita per selezionare solo i pacchetti con gli aggiornamenti nei repo di sicurezza. Per ciascun pacchetto, la versione candidata (in genere, quella più recente) deve fare parte di un repo di sicurezza.

Se sono inclusi aggiornamenti non correlati alla protezione, vengono prese in considerazione anche le patch di altri repository.

4. Applica [ApprovedPatches](#) come specificato nella baseline delle patch. Le patch vengono approvate per l'aggiornamento anche se sono ignorate da [GlobalFilters](#) o se nessuna regola di approvazione specificata in [ApprovalRules](#) concede l'approvazione.
5. Applica [RejectedPatches](#) come specificato nella baseline delle patch. Le patch rifiutate vengono rimosse dall'elenco di quelle approvate e non saranno applicate.
6. Se vengono approvate più versioni di una patch, verrà applicata quella più recente.
7. L'API di aggiornamento YUM (Amazon Linux 2) o l'API di aggiornamento DNF (Amazon Linux 2023) viene applicata alle patch approvate come segue:
 - Per le baseline delle patch predefinite fornite da AWS, vengono applicate solo le patch specificate in `updateinfo.xml` (solo aggiornamenti correlati alla sicurezza). Questo perché la casella di controllo `Includi aggiornamenti non critici` non è selezionata. Le baseline predefinite sono equivalenti a una baseline personalizzata con quanto segue:
 - La casella di controllo `Includi aggiornamenti non critici` non è selezionata
 - Un elenco di GRAVITÀ di `[Critical, Important]`
 - Un elenco di CLASSIFICAZIONE di `[Security, Bugfix]`

Per Amazon Linux 2, il comando `yum` equivalente per questo flusso di lavoro è:

```
sudo yum update-minimal --sec-severity=Critical,Important --bugfix -y
```

Per Amazon Linux 2023, il comando dnf equivalente per questo flusso di lavoro è:

```
sudo dnf upgrade-minimal --sec-severity=Critical --sec-severity=Important --bugfix -y
```

Quando la casella di controllo **Includi aggiornamenti non critici** è selezionata, vengono applicate entrambe le patch, quelle presenti in `updateinfo.xml` e quelle non presenti in `updateinfo.xml` (gli aggiornamenti correlati alla sicurezza e quelli non correlati alla sicurezza).

Per Amazon Linux 2, se è selezionata una linea di base con **Includi aggiornamenti non di sicurezza** e ha un elenco di SEVERITY [Critical, Important] e un elenco CLASSIFICATION di, il comando yum equivalente è: [Security, Bugfix]

```
sudo yum update --security --sec-severity=Critical,Important --bugfix -y
```

Per Amazon Linux 2023, il comando dnf equivalente è:

```
sudo dnf upgrade --security --sec-severity=Critical --sec-severity=Important --bugfix -y
```

Note

I nuovi pacchetti che sostituiscono quelli ormai obsoleti con nomi diversi vengono installati se si eseguono questi comandi yum o dnf all'esterno di Patch Manager. Tuttavia, non vengono installati con operazioni di Patch Manager equivalenti.

Dettagli di patch aggiuntivi per Amazon Linux 2023

Supporto per il livello di gravità 'Nessuno'

Amazon Linux 2023 supporta anche il livello None di gravità delle patch, riconosciuto dal gestore di pacchetti DNF.

Supporto per il livello di gravità 'Medio'

Per Amazon Linux 2023, un livello di gravità delle patch pari a Medium è equivalente a una gravità di Moderate, che potrebbe essere definita in alcuni repository esterni. Se includi le patch di gravità Medium nella baseline delle patch, sulle istanze vengono installate anche le patch di gravità Moderate di quelle esterne.

Quando esegui una query per i dati di conformità utilizzando l'operazione API [DescribeInstancePatches](#), il filtro per il livello di gravità Medium riporta le patch con entrambi i livelli di gravità Medium e Moderate.

Gestione delle dipendenze transitive per Amazon Linux 2023

Per Amazon Linux 2023, Patch Manager potrebbe installare versioni diverse di dipendenze transitive rispetto all'installazione di comandi `dnf` equivalenti. Le dipendenze transitive sono pacchetti installati automaticamente per soddisfare i requisiti di altri pacchetti (dipendenze di dipendenze).

Ad esempio, `dnf upgrade-minimal --security` installa le versioni minime delle dipendenze transitive necessarie per risolvere problemi di sicurezza noti, mentre Patch Manager installa le versioni più recenti disponibili delle stesse dipendenze transitive.

8. Se sono stati installati aggiornamenti, il nodo gestito viene riavviato. (Eccezione: se il parametro `RebootOption` è impostato su `NoReboot` nel documento `AWS-RunPatchBaseline`, il nodo non viene riavviato dopo l'esecuzione di Patch Manager. Per ulteriori informazioni, consulta [Nome parametro: RebootOption](#).)

Note

Una configurazione predefinita per un gestore di pacchetti su una distribuzione Linux potrebbe essere impostata per ignorare un repository di pacchetti irraggiungibile senza errori. In questi casi, la relativa operazione di patching procede senza installare gli aggiornamenti dal repository e si conclude con successo. Per applicare gli aggiornamenti del repository, aggiungili alla configurazione del repository.

`skip_if_unavailable=False`

Per ulteriori informazioni sull'opzione `skip_if_available`, consulta [Connettività all'origine della patch](#).

CentOS Stream

Sui nodi gestiti CentOS Stream, il flusso di lavoro di installazione delle patch funziona come riportato:

1. Se un elenco delle patch viene specificato utilizzando un URL https o un URL in stile percorso Amazon Simple Storage Service (Amazon S3) utilizzando il parametro `InstallOverrideList` per i documenti `AWS-RunPatchBaseline` o `AWS-RunPatchBaselineAssociation`, vengono installate le patch elencate e vengono ignorate le fasi 2-7.

Applicare [GlobalFilters](#) come specificato nella baseline delle patch, mantenendo solo i pacchetti qualificati per un'ulteriore elaborazione.

2. Applica [ApprovalRules](#) come specificato nella baseline delle patch. Ciascuna regola di approvazione è in grado di definire un pacchetto come approvato.

Le norme di approvazione, tuttavia, sono anche soggette al fatto che la casella di spunta `Includi aggiornamenti non correlati alla protezione` è stata selezionata durante la creazione o l'ultimo aggiornamento di una baseline delle patch.

Se sono esclusi aggiornamenti non di sicurezza, viene applicata una regola implicita per selezionare solo i pacchetti con gli aggiornamenti nei repo di sicurezza. Per ciascun pacchetto, la versione candidata (in genere, quella più recente) deve fare parte di un repo di sicurezza.

Se sono inclusi aggiornamenti non correlati alla protezione, vengono prese in considerazione anche le patch di altri repository.

3. Applica [ApprovedPatches](#) come specificato nella baseline delle patch. Le patch vengono approvate per l'aggiornamento anche se sono ignorate da [GlobalFilters](#) o se nessuna regola di approvazione specificata in [ApprovalRules](#) concede l'approvazione.
4. Applica [RejectedPatches](#) come specificato nella baseline delle patch. Le patch rifiutate vengono rimosse dall'elenco di quelle approvate e non saranno applicate.
5. Se vengono approvate più versioni di una patch, verrà applicata quella più recente.
6. L'aggiornamento DNF su CentOS Stream viene applicato alle patch approvate.

Note

Per CentOS Stream, Patch Manager potrebbe installare versioni diverse delle dipendenze transitive rispetto all'installazione di comandi `dnf` equivalenti. Le

dipendenze transitive sono pacchetti installati automaticamente per soddisfare i requisiti di altri pacchetti (dipendenze di dipendenze).

Ad esempio, `dnf upgrade-minimal --security` installa le versioni minime delle dipendenze transitive necessarie per risolvere problemi di sicurezza noti, mentre Patch Manager installa le versioni più recenti disponibili delle stesse dipendenze transitive.

7. Se sono stati installati aggiornamenti, il nodo gestito viene riavviato. (Eccezione: se il parametro `RebootOption` è impostato su `NoReboot` nel documento `AWS-RunPatchBaseline`, il nodo non viene riavviato dopo l'esecuzione di Patch Manager. Per ulteriori informazioni, consulta [Nome parametro: RebootOption](#).)

Debian Server

Di seguito è riportato il flusso di lavoro di installazione delle patch nelle istanze Debian Server:

1. Se un elenco delle patch viene specificato utilizzando un URL `https` o un URL in stile percorso Servizio di archiviazione semplice Amazon (Amazon S3) utilizzando il parametro `InstallOverrideList` per i documenti `AWS-RunPatchBaseline` o `AWS-RunPatchBaselineAssociation`, vengono installate le patch elencate e vengono ignorati i passaggi 2-7.
2. Se è disponibile un aggiornamento per `python3-apt` (un'interfaccia di libreria Python per `libapt`), viene aggiornato alla versione più recente. (Questo pacchetto non correlato alla sicurezza viene aggiornato anche se non è stata selezionata l'opzione `Includi aggiornamenti non correlati alla protezione`).
3. Applicare [GlobalFilters](#) come specificato nella baseline delle patch, mantenendo solo i pacchetti qualificati per un'ulteriore elaborazione.
4. Applica [ApprovalRules](#) come specificato nella baseline delle patch. Ciascuna regola di approvazione è in grado di definire un pacchetto come approvato.

Note

Poiché non è possibile determinare in modo affidabile le date di rilascio dei pacchetti di aggiornamento per Debian Server, le opzioni di approvazione automatica non sono supportate per questo sistema operativo.

Le norme di approvazione, tuttavia, sono anche soggette al fatto che la casella di spunta **Includi aggiornamenti non correlati alla protezione** è stata selezionata durante la creazione o l'ultimo aggiornamento di una baseline delle patch.

Se sono esclusi aggiornamenti non di sicurezza, viene applicata una regola implicita per selezionare solo i pacchetti con gli aggiornamenti nei repo di sicurezza. Per ciascun pacchetto, la versione candidata (in genere, quella più recente) deve fare parte di un repo di sicurezza.

Se sono inclusi aggiornamenti non correlati alla protezione, vengono prese in considerazione anche le patch di altri repository.

 Note

Per Debian Server, le versioni candidate alle patch sono limitate alle patch incluse in `debian-security`.

5. Applica [ApprovedPatches](#) come specificato nella baseline delle patch. Le patch vengono approvate per l'aggiornamento anche se sono ignorate da [GlobalFilters](#) o se nessuna regola di approvazione specificata in [ApprovalRules](#) concede l'approvazione.
6. Applica [RejectedPatches](#) come specificato nella baseline delle patch. Le patch rifiutate vengono rimosse dall'elenco di quelle approvate e non saranno applicate.
7. La libreria APT viene utilizzata per aggiornare i pacchetti.

 Note

Patch Manager non supporta l'uso dell'opzione `Pin-Priority` APT per assegnare priorità ai pacchetti. Patch Manager aggrega gli aggiornamenti disponibili da tutti gli archivi abilitati e seleziona l'aggiornamento più recente che corrisponde alla baseline per ogni pacchetto installato.

8. Se sono stati installati aggiornamenti, il nodo gestito viene riavviato. (Eccezione: se il parametro `RebootOption` è impostato su `NoReboot` nel documento `AWS-RunPatchBaseline`, il nodo non viene riavviato dopo l'esecuzione di Patch Manager. Per ulteriori informazioni, consulta [Nome parametro: RebootOption](#).)

macOS

Sui nodi gestiti macOS, il flusso di lavoro di installazione delle patch funziona come riportato:

1. L'elenco di proprietà `/Library/Receipts/InstallHistory.plist` è un record del software che è stato installato e aggiornato utilizzando la Gestione dei pacchetti `softwareupdate` e `installer`. Utilizzando lo strumento a riga di comando `pkgutil` (`perinstaller`) e il gestore di pacchetti `softwareupdate`, i comandi CLI vengono eseguiti per analizzare questo elenco.

Per `installer`, la risposta ai comandi CLI include `package name`, `version`, `volume`, `location`, e i dettagli `install-time`, ma solo `package name` e `version` sono utilizzati da Patch Manager.

Per `softwareupdate`, la risposta ai comandi CLI include il nome del pacchetto (`display name`), `version`, e `date`, ma solo il nome e la versione del pacchetto vengono utilizzati da Patch Manager.

Per Brew e Brew Cask, Homebrew non supporta i suoi comandi eseguiti sotto l'utente root. Di conseguenza, Patch Manager esegue query ed esegue i comandi Homebrew come proprietario della directory Homebrew o come utente valido appartenente al gruppo proprietario della directory Homebrew. I comandi sono simili a `softwareupdate` e `installer` vengono eseguiti attraverso un sottoprocesso Python per raccogliere i dati del pacchetto, e il risultato viene analizzato per identificare i nomi e le versioni dei pacchetti.

2. Applicare [GlobalFilters](#) come specificato nella baseline delle patch, mantenendo solo i pacchetti qualificati per un'ulteriore elaborazione.
3. Applica [ApprovalRules](#) come specificato nella baseline delle patch. Ciascuna regola di approvazione è in grado di definire un pacchetto come approvato.
4. Applica [ApprovedPatches](#) come specificato nella baseline delle patch. Le patch vengono approvate per l'aggiornamento anche se sono ignorate da [GlobalFilters](#) o se nessuna regola di approvazione specificata in [ApprovalRules](#) concede l'approvazione.
5. Applica [RejectedPatches](#) come specificato nella baseline delle patch. Le patch rifiutate vengono rimosse dall'elenco di quelle approvate e non saranno applicate.
6. Se vengono approvate più versioni di una patch, verrà applicata quella più recente.
7. Richiama l'interfaccia CLI del pacchetto idoneo sul nodo gestito per elaborare le patch approvate nel modo seguente:

 Note

`installer` manca della funzionalità per verificare e installare gli aggiornamenti. Pertanto, per `installer`, Patch Manager riportare solo i pacchetti che sono installati. Di conseguenza, i pacchetti `installer` non vengono mai segnalati come Missing.

- Per le baseline delle patch predefinite fornite da AWS e per le baseline delle patch personalizzate in cui la casella di controllo Includi aggiornamenti non critici non è selezionata vengono applicati solo gli aggiornamenti correlati alla sicurezza.
 - Per le baseline delle patch personalizzate in cui la casella di controllo Includi aggiornamenti non critici è selezionata vengono applicati solo gli aggiornamenti correlati alla sicurezza.
8. Se sono stati installati aggiornamenti, il nodo gestito viene riavviato. (Eccezione: se il parametro `RebootOption` è impostato su `NoReboot` nel documento `AWS-RunPatchBaseline`, il nodo non viene riavviato dopo l'esecuzione di Patch Manager. Per ulteriori informazioni, consulta [Nome parametro: RebootOption](#).)

Oracle Linux

Sui nodi gestiti Oracle Linux, il flusso di lavoro di installazione delle patch funziona come riportato:

1. Se un elenco delle patch viene specificato utilizzando un URL `https` o un URL in stile percorso Amazon Simple Storage Service (Amazon S3) utilizzando il parametro `InstallOverrideList` per i documenti `AWS-RunPatchBaseline` o `AWS-RunPatchBaselineAssociation`, vengono installate le patch elencate e vengono ignorate le fasi 2-7.
2. Applicare [GlobalFilters](#) come specificato nella baseline delle patch, mantenendo solo i pacchetti qualificati per un'ulteriore elaborazione.
3. Applica [ApprovalRules](#) come specificato nella baseline delle patch. Ciascuna regola di approvazione è in grado di definire un pacchetto come approvato.

Le norme di approvazione, tuttavia, sono anche soggette al fatto che la casella di spunta Includi aggiornamenti non correlati alla protezione è stata selezionata durante la creazione o l'ultimo aggiornamento di una baseline delle patch.

Se sono esclusi aggiornamenti non di sicurezza, viene applicata una regola implicita per selezionare solo i pacchetti con gli aggiornamenti nei repo di sicurezza. Per ciascun pacchetto, la versione candidata (in genere, quella più recente) deve fare parte di un repo di sicurezza.

Se sono inclusi aggiornamenti non correlati alla protezione, vengono prese in considerazione anche le patch di altri repository.

4. Applica [ApprovedPatches](#) come specificato nella baseline delle patch. Le patch vengono approvate per l'aggiornamento anche se sono ignorate da [GlobalFilters](#) o se nessuna regola di approvazione specificata in [ApprovalRules](#) concede l'approvazione.
5. Applica [RejectedPatches](#) come specificato nella baseline delle patch. Le patch rifiutate vengono rimosse dall'elenco di quelle approvate e non saranno applicate.
6. Se vengono approvate più versioni di una patch, verrà applicata quella più recente.
7. Sui nodi gestiti della versione 7, l'API di aggiornamento YUM viene applicata alle patch approvate come segue:
 - Per le baseline delle patch predefinite fornite da AWS e per le baseline delle patch personalizzate in cui la casella di controllo Includi aggiornamenti non critici non è selezionata vengono applicate solo le patch specificate in `updateinfo.xml` (solo gli aggiornamenti correlati alla sicurezza).

Il comando yum equivalente per questo flusso di lavoro è:

```
sudo yum update-minimal --sec-severity=Important,Moderate --bugfix -y
```

- Per le baseline delle patch personalizzate in cui la casella di controllo Includi aggiornamenti non critici è selezionata vengono applicate entrambe le patch, quelle presenti in `updateinfo.xml` e quelle non presenti in `updateinfo.xml` (gli aggiornamenti correlati alla sicurezza e quelli non correlati alla sicurezza).

Il comando yum equivalente per questo flusso di lavoro è:

```
sudo yum update --security --bugfix -y
```

Nei nodi gestiti della versione 8 e 9, l'API di aggiornamento DNF viene applicata alle patch approvate come segue:

- Per le baseline di patch predefinite fornite da AWS e per le baseline delle patch personalizzate in cui la casella di controllo Includi aggiornamenti non relativi alla

sicurezza non è selezionata, vengono applicate solo le patch specificate in (solo aggiornamenti di sicurezza). `updateinfo.xml`

Il comando yum equivalente per questo flusso di lavoro è:

```
sudo dnf upgrade-minimal --security --sec-severity=Moderate --sec-severity=Important
```

Note

Per Oracle Linux, Patch Manager potrebbe installare versioni diverse delle dipendenze transitive rispetto all'installazione di comandi dnf equivalenti. Le dipendenze transitive sono pacchetti installati automaticamente per soddisfare i requisiti di altri pacchetti (dipendenze di dipendenze).

Ad esempio, `dnf upgrade-minimal --security` installa le versioni minime delle dipendenze transitive necessarie per risolvere problemi di sicurezza noti, mentre Patch Manager installa le versioni più recenti disponibili delle stesse dipendenze transitive.

- Per le baseline delle patch personalizzate in cui la casella di controllo Includi aggiornamenti non critici è selezionata vengono applicate entrambe le patch, quelle presenti in `updateinfo.xml` e quelle non presenti in `updateinfo.xml` (gli aggiornamenti correlati alla sicurezza e quelli non correlati alla sicurezza).

Il comando yum equivalente per questo flusso di lavoro è:

```
sudo dnf upgrade --security --bugfix
```

Note

I nuovi pacchetti che sostituiscono quelli ormai obsoleti con nomi diversi vengono installati se si eseguono questi comandi yum o dnf all'esterno di Patch Manager. Tuttavia, non vengono installati con operazioni di Patch Manager equivalenti.

8. Se sono stati installati aggiornamenti, il nodo gestito viene riavviato. (Eccezione: se il parametro `RebootOption` è impostato su `NoReboot` nel documento `AWS-RunPatchBaseline`, il nodo non viene riavviato dopo l'esecuzione di Patch Manager. Per ulteriori informazioni, consulta [Nome parametro: RebootOption](#).)

 Note

Una configurazione predefinita per un gestore di pacchetti su una distribuzione Linux potrebbe essere impostata per ignorare un repository di pacchetti irraggiungibile senza errori. In questi casi, la relativa operazione di patching procede senza installare gli aggiornamenti dal repository e si conclude con successo. Per applicare gli aggiornamenti del repository, aggiungili alla configurazione del repository.

`skip_if_unavailable=False`

Per ulteriori informazioni sull'opzione `skip_if_available`, consulta [Connettività all'origine della patch](#).

AlmaLinux, RHEL, and Rocky Linux

AlmaLinuxSui nodi Rocky Linux gestiti e gestiti, il flusso di lavoro di installazione delle patch è il seguente: Red Hat Enterprise Linux

1. Se un elenco delle patch viene specificato utilizzando un URL https o un URL in stile percorso Amazon Simple Storage Service (Amazon S3) utilizzando il parametro `InstallOverrideList` per i documenti `AWS-RunPatchBaseline` o `AWS-RunPatchBaselineAssociation`, vengono installate le patch elencate e vengono ignorate le fasi 2-7.
2. Applicare [GlobalFilters](#) come specificato nella baseline delle patch, mantenendo solo i pacchetti qualificati per un'ulteriore elaborazione.
3. Applica [ApprovalRules](#) come specificato nella baseline delle patch. Ciascuna regola di approvazione è in grado di definire un pacchetto come approvato.

Le norme di approvazione, tuttavia, sono anche soggette al fatto che la casella di spunta `Includi aggiornamenti non correlati alla protezione` è stata selezionata durante la creazione o l'ultimo aggiornamento di una baseline delle patch.

Se sono esclusi aggiornamenti non di sicurezza, viene applicata una regola implicita per selezionare solo i pacchetti con gli aggiornamenti nei repo di sicurezza. Per ciascun pacchetto, la versione candidata (in genere, quella più recente) deve fare parte di un repo di sicurezza.

Se sono inclusi aggiornamenti non correlati alla protezione, vengono prese in considerazione anche le patch di altri repository.

4. Applica [ApprovedPatches](#) come specificato nella baseline delle patch. Le patch vengono approvate per l'aggiornamento anche se sono ignorate da [GlobalFilters](#) o se nessuna regola di approvazione specificata in [ApprovalRules](#) concede l'approvazione.
5. Applica [RejectedPatches](#) come specificato nella baseline delle patch. Le patch rifiutate vengono rimosse dall'elenco di quelle approvate e non saranno applicate.
6. Se vengono approvate più versioni di una patch, verrà applicata quella più recente.
7. L'API di aggiornamento YUM (su RHEL 7) o l'API di aggiornamento DNF (su AlmaLinux 8 e 9, RHEL 8, 9 e 10 e Rocky Linux 8 e 9) viene applicata alle patch approvate in base alle seguenti regole:

Scenario 1: aggiornamenti esclusi Non-security

- Si applica a: linee di base predefinite delle patch fornite da AWS e linee di base delle patch personalizzate.
- Casella di controllo Includi aggiornamenti non critici: non è selezionata.
- Patch applicate: le patch specificate in `updateinfo.xml` (solo aggiornamenti di sicurezza) vengono applicate solo se entrambe corrispondono alla configurazione di baseline delle patch e si trovano nei repository configurati.

In alcuni casi, una patch specificata in `updateinfo.xml` potrebbe non essere più disponibile in un repository configurato. I repository configurati di solito hanno solo la versione più recente di una patch, che è un riepilogo sommario di tutti gli aggiornamenti precedenti, ma la versione più recente potrebbe non corrispondere alle baseline delle patch e viene omessa dall'operazione di applicazione di patch.

- Comandi: per RHEL 7, il comando yum equivalente per questo flusso di lavoro è:

```
sudo yum update-minimal --sec-severity=Critical,Important --bugfix -y
```

Per AlmaLinux, RHEL 8 e Rocky Linux, i comandi dnf equivalenti per questo flusso di lavoro sono:

```
sudo dnf update-minimal --sec-severity=Critical --bugfix -y ; \  
sudo dnf update-minimal --sec-severity=Important --bugfix -y
```

 Note

For AlmaLinuxRHEL, e Rocky Linux Rocky Linux, Patch Manager potrebbero installare versioni di dipendenze transitive diverse da quelle installate con i comandi equivalenti `dnf`. Le dipendenze transitive sono pacchetti installati automaticamente per soddisfare i requisiti di altri pacchetti (dipendenze di dipendenze).

Ad esempio, `dnf upgrade-minimal --security` installa le versioni minime delle dipendenze transitive necessarie per risolvere problemi di sicurezza noti, mentre Patch Manager installa le versioni più recenti disponibili delle stesse dipendenze transitive.

Scenario 2: aggiornamenti inclusi Non-security

- Si applica a: baseline delle patch personalizzate.
- Casella di controllo Includi aggiornamenti non critici: selezionata.
- Patch applicate: vengono applicate le patch in `updateinfo.xml` e quelle non incluse in `updateinfo.xml` (aggiornamenti di sicurezza e non critici).
- Comandi: per RHEL 7, il comando `yum` equivalente per questo flusso di lavoro è:

```
sudo yum update --security --bugfix -y
```

Per AlmaLinux 8 e 9, RHEL 8 e 9 e Rocky Linux 8 e 9, il comando `dnf` equivalente per questo flusso di lavoro è:

```
sudo dnf update --security --bugfix -y
```

 Note

I nuovi pacchetti che sostituiscono quelli ormai obsoleti con nomi diversi vengono installati se si eseguono questi comandi `yum` o `dnf` all'esterno di Patch Manager. Tuttavia, non vengono installati con operazioni di Patch Manager equivalenti.

8. Se sono stati installati aggiornamenti, il nodo gestito viene riavviato. (Eccezione: se il parametro `RebootOption` è impostato su `NoReboot` nel documento `AWS-RunPatchBaseline`, il nodo non viene riavviato dopo l'esecuzione di Patch Manager. Per ulteriori informazioni, consulta [Nome parametro: RebootOption](#).)

Note

Una configurazione predefinita per un gestore di pacchetti su una distribuzione Linux potrebbe essere impostata per ignorare un repository di pacchetti irraggiungibile senza errori. In questi casi, la relativa operazione di patching procede senza installare gli aggiornamenti dal repository e si conclude con successo. Per applicare gli aggiornamenti del repository, aggiungili alla configurazione del repository.

`skip_if_unavailable=False`

Per ulteriori informazioni sull'opzione `skip_if_available`, consulta [Connettività all'origine della patch](#).

SLES

Sui nodi gestiti SUSE Linux Enterprise Server (SLES), è riportato il flusso di lavoro di installazione delle patch come segue:

1. Se un elenco delle patch viene specificato utilizzando un URL https o un URL in stile percorso Amazon Simple Storage Service (Amazon S3) utilizzando il parametro `InstallOverrideList` per i documenti `AWS-RunPatchBaseline` o `AWS-RunPatchBaselineAssociation`, vengono installate le patch elencate e vengono ignorate le fasi 2-7.
2. Applicare [GlobalFilters](#) come specificato nella baseline delle patch, mantenendo solo i pacchetti qualificati per un'ulteriore elaborazione.
3. Applica [ApprovalRules](#) come specificato nella baseline delle patch. Ciascuna regola di approvazione è in grado di definire un pacchetto come approvato.

Le norme di approvazione, tuttavia, sono anche soggette al fatto che la casella di spunta **Includi aggiornamenti non correlati alla protezione** è stata selezionata durante la creazione o l'ultimo aggiornamento di una baseline delle patch.

Se sono esclusi aggiornamenti non di sicurezza, viene applicata una regola implicita per selezionare solo i pacchetti con gli aggiornamenti nei repo di sicurezza. Per ciascun pacchetto, la versione candidata (in genere, quella più recente) deve fare parte di un repo di sicurezza.

Se sono inclusi aggiornamenti non correlati alla protezione, vengono prese in considerazione anche le patch di altri repository.

4. Applica [ApprovedPatches](#) come specificato nella baseline delle patch. Le patch vengono approvate per l'aggiornamento anche se sono ignorate da [GlobalFilters](#) o se nessuna regola di approvazione specificata in [ApprovalRules](#) concede l'approvazione.
5. Applica [RejectedPatches](#) come specificato nella baseline delle patch. Le patch rifiutate vengono rimosse dall'elenco di quelle approvate e non saranno applicate.
6. Se vengono approvate più versioni di una patch, verrà applicata quella più recente.
7. L'API di aggiornamento Zypper viene applicata alle patch approvate.
8. Se sono stati installati aggiornamenti, il nodo gestito viene riavviato. (Eccezione: se il parametro `RebootOption` è impostato su `NoReboot` nel documento `AWS-RunPatchBaseline`, il nodo non viene riavviato dopo l'esecuzione di Patch Manager. Per ulteriori informazioni, consulta [Nome parametro: RebootOption](#).)

Ubuntu Server

Sui nodi gestiti Ubuntu Server, il flusso di lavoro di installazione delle patch funziona come riportato:

1. Se un elenco delle patch viene specificato utilizzando un URL https o un URL in stile percorso Amazon Simple Storage Service (Amazon S3) utilizzando il parametro `InstallOverrideList` per i documenti `AWS-RunPatchBaseline` o `AWS-RunPatchBaselineAssociation`, vengono installate le patch elencate e vengono ignorati i passaggi 2-7.
2. Se è disponibile un aggiornamento per `python3-apt` (un'interfaccia di libreria Python per `libapt`), viene aggiornato alla versione più recente. (Questo pacchetto non correlato alla sicurezza viene aggiornato anche se non è stata selezionata l'opzione `Includi aggiornamenti non correlati alla protezione`).
3. Applicare [GlobalFilters](#) come specificato nella baseline delle patch, mantenendo solo i pacchetti qualificati per un'ulteriore elaborazione.
4. Applica [ApprovalRules](#) come specificato nella baseline delle patch. Ciascuna regola di approvazione è in grado di definire un pacchetto come approvato.

 Note

Poiché non è possibile determinare in modo affidabile le date di rilascio dei pacchetti di aggiornamento per Ubuntu Server, le opzioni di approvazione automatica non sono supportate per questo sistema operativo.

Le norme di approvazione, tuttavia, sono anche soggette al fatto che la casella di spunta **Includi aggiornamenti non correlati alla protezione** è stata selezionata durante la creazione o l'ultimo aggiornamento di una baseline delle patch.

Se sono esclusi aggiornamenti non di sicurezza, viene applicata una regola implicita per selezionare solo i pacchetti con gli aggiornamenti nei repo di sicurezza. Per ciascun pacchetto, la versione candidata (in genere, quella più recente) deve fare parte di un repo di sicurezza.

Se sono inclusi aggiornamenti non correlati alla protezione, vengono prese in considerazione anche le patch di altri repository.

Le norme di approvazione, tuttavia, sono anche soggette al fatto che la casella di spunta **Includi aggiornamenti non correlati alla protezione** è stata selezionata durante la creazione o l'ultimo aggiornamento di una baseline delle patch.

 Note

Per ogni versione di Ubuntu Server, le versioni patch candidate sono limitate alle patch che fanno parte del repository associato a quella versione, come segue:

- Ubuntu Server 18.04 LTS: `bionic-security`
- Ubuntu Server 20.04 LTS: `focal-security`
- Ubuntu Server 22.04 LTS: `jammy-security`
- Ubuntu Server 24.04 LTS: `noble-security`
- Ubuntu Server 25.04: `plucky-security`

5. Applica [ApprovedPatches](#) come specificato nella baseline delle patch. Le patch vengono approvate per l'aggiornamento anche se sono ignorate da [GlobalFilters](#) o se nessuna regola di approvazione specificata in [ApprovalRules](#) concede l'approvazione.

6. Applica [RejectedPatches](#) come specificato nella baseline delle patch. Le patch rifiutate vengono rimosse dall'elenco di quelle approvate e non saranno applicate.
7. La libreria APT viene utilizzata per aggiornare i pacchetti.

 Note

Patch Manager non supporta l'uso dell'opzione Pin-Priority APT per assegnare priorità ai pacchetti. Patch Manager aggrega gli aggiornamenti disponibili da tutti gli archivi abilitati e seleziona l'aggiornamento più recente che corrisponde alla baseline per ogni pacchetto installato.

8. Se sono stati installati aggiornamenti, il nodo gestito viene riavviato. (Eccezione: se il parametro `RebootOption` è impostato su `NoReboot` nel documento `AWS-RunPatchBaseline`, il nodo non viene riavviato dopo l'esecuzione di Patch Manager. Per ulteriori informazioni, consulta [Nome parametro: RebootOption](#).)

Windows Server

Se l'operazione di applicazione delle patch viene eseguita in un nodo gestito Windows Server, il nodo richiede uno snapshot della baseline delle patch appropriata da Systems Manager. Tale snapshot contiene l'elenco di tutti gli aggiornamenti disponibili nella baseline delle patch che sono stati approvati per la distribuzione. Questo elenco di aggiornamenti viene inviato all'API di Windows Update, che determinerà quali aggiornamenti sono applicabili al nodo gestito e li installerà in base alle esigenze. Windows consente l'installazione solo dell'ultima versione disponibile di un KB. Patch Manager installa la versione più recente di un KB quando questa, o qualsiasi versione precedente del KB, corrisponde alla baseline delle patch applicata. Se vengono installati eventuali aggiornamenti, il nodo gestito verrà riavviato tutte le volte necessarie per completare l'applicazione di tutte le patch richieste. (Eccezione: se il parametro `RebootOption` è impostato su `NoReboot` nel documento `AWS-RunPatchBaseline`, il nodo non viene riavviato dopo l'esecuzione di Patch Manager. Per ulteriori informazioni, consulta [Nome parametro: RebootOption](#).) Il riepilogo dell'applicazione di patch è disponibile nell'output della richiesta `Run Command`. I log aggiuntivi sono disponibili nel nodo gestito della cartella `%PROGRAMDATA%\Amazon\PatchBaselineOperations\Logs`.

Poiché l'API di Windows Update viene utilizzata per scaricare e installare i KB, vengono rispettate tutte le impostazioni delle policy di gruppo per Windows Update. Non è necessaria alcuna impostazione dei Criteri di gruppo per l'utilizzo Patch Manager, ma verranno applicate tutte le

impostazioni definite, ad esempio per indirizzare i nodi gestiti a un server Windows Server Update Services (WSUS).

 Note

Per impostazione predefinita, Windows scarica tutti i KB dal sito Windows Update di Microsoft poiché Patch Manager utilizza l'API di Windows Update per gestire i relativi download e l'installazione. Di conseguenza, il nodo gestito deve essere in grado di raggiungere il sito di Microsoft Windows Update o l'applicazione della patch non andrà a buon fine. In alternativa, è possibile configurare un server WSUS che funga da repository di KB e configurare i nodi gestiti che abbiano come target tale server WSUS anziché l'utilizzo delle policy di gruppo.

Patch Manager potrebbe fare riferimento agli ID KB durante la creazione di baseline delle patch personalizzate per Windows Server, ad esempio quando un elenco di patch approvate o di patch rifiutate è incluso nella configurazione della baseline. Vengono installati solo gli aggiornamenti a cui è assegnato un ID KB in Microsoft Windows Update o in un server WSUS da Patch Manager. Gli aggiornamenti privi di un ID KB non sono inclusi nelle operazioni di applicazione di patch.

Per informazioni sulla creazione di baseline delle patch personalizzate, consulta i seguenti argomenti:

- [Creazione di una baseline di patch personalizzata per Windows Server](#)
- [Creare una baseline delle patch \(CLI\)](#)
- [Formati dei nomi dei pacchetti per sistemi operativi Windows](#)

Come funzionano le regole di base delle patch sui sistemi Linux-based

Le regole di una baseline delle patch nelle distribuzioni Linux operano in modo diverso in base al tipo di distribuzione. A differenza degli aggiornamenti delle patch sui nodi Windows Server gestiti, le regole vengono valutate su ogni nodo per prendere in considerazione i repository configurati sull'istanza. Patch Manager utilizza il gestore di pacchetti nativo per guidare l'installazione delle patch approvate dalla patch baseline.

Per i tipi di sistema Linux-based operativo che segnalano un livello di gravità per le patch, Patch Manager utilizza il livello di gravità riportato dal produttore del software per l'avviso di aggiornamento o la singola patch. Patch Manager non deriva i livelli di gravità da fonti di terze parti, come il [Common](#)

[Vulnerability Scoring System](#) (CVSS), o dalle metriche rilasciate dal National Vulnerability Database (NVD). <https://nvd.nist.gov/vuln>

Funzionamento della baseline delle patch in Amazon Linux 2 e Amazon Linux 2023

Note

Amazon Linux 2023 (AL2023) utilizza repository con versioni che possono essere bloccati su una versione specifica tramite una o più impostazioni di sistema. Per tutte le operazioni di patching sulle istanze AL2023 EC2Patch Manager, utilizza le versioni più recenti del repository, indipendentemente dalla configurazione del sistema. Per ulteriori informazioni, consulta [Aggiornamenti deterministici tramite repository con versioni](#) nella Guida per l'utente di Amazon Linux 2023.

Su Amazon Linux 2 e Amazon Linux 2023, il processo di selezione delle patch è il seguente:

1. Sul nodo gestito, la libreria YUM (Amazon Linux 2) o la libreria DNF (Amazon Linux 2023) accede al file `updateinfo.xml` per ogni repository configurato.

Se non viene trovato alcun `updateinfo.xml` file, l'installazione delle patch dipende dalle impostazioni per Includi aggiornamenti non di sicurezza e. Auto-approval Ad esempio, se gli aggiornamenti non relativi alla protezione sono consentiti, vengono installati quando arriva l'ora di approvazione automatica.

2. Ogni avviso di aggiornamento di `updateinfo.xml` include vari attributi che denotano le proprietà dei pacchetti dell'avviso, come descritto nella seguente tabella.

Attributi degli avvisi di aggiornamento

Attributo	Description
tipo	<p>Corrisponde al valore dell'attributo chiave Classification nel tipo di dati PatchFilter della baseline delle patch. Indica il tipo di pacchetto incluso nell'avviso di aggiornamento.</p> <p>È possibile visualizzare l'elenco dei valori supportati utilizzando il AWS CLI comando describe-patch-properties o l'operazione</p>

Attributo	Description
	<p>API. DescribePatchProperties È anche possibile visualizzare l'elenco nell'area Norme di approvazione della pagina Create patch baseline (Creazione di una baseline delle patch) della pagina Edit patch baseline (Modifica della baseline delle patch) nella console Systems Manager.</p>
severity	<p>Corrisponde al valore dell'attributo chiave Severity nel tipo di dati PatchFilter della baseline delle patch. Indica il tipo di gravità dei pacchetti inclusi nell'avviso di aggiornamento. Generalmente applicabile solo per gli avvisi di aggiornamento Security.</p> <p>È possibile visualizzare l'elenco dei valori supportati utilizzando il AWS CLI comando describe-patch-properties o l'operazione API DescribePatchProperties. È anche possibile visualizzare l'elenco nell'area Norme di approvazione della pagina Create patch baseline (Creazione di una baseline delle patch) della pagina Edit patch baseline (Modifica della baseline delle patch) nella console Systems Manager.</p>
update_id	<p>Indica l'ID dell'avviso, ad esempio. ALAS-2017-867 L'ID consulenza può essere utilizzato nell'attributo ApprovedPatches o RejectedPatches della baseline delle patch.</p>

Attributo	Description
referimenti	Contiene informazioni aggiuntive sull'avviso di aggiornamento, ad esempio un ID CVE (formato:). CVE-2017-1234567 L'ID CVE può essere utilizzato nell'attributo ApprovedPatches o RejectedPatches della baseline delle patch.
emesso	Corrisponde a ApproveAfterDays nella baseline delle patch. Indica la data di rilascio (data di emissione) dei pacchetti inclusi nell'avviso di aggiornamento. Per stabilire se la patch è approvata per la distribuzione, si effettua un confronto tra il timestamp corrente e il valore di questo attributo più <code>ApproveAfterDays</code> .

Per informazioni sui formati accettati per gli elenchi delle patch approvate e di quelle rifiutate, consulta [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#).

- Il prodotto del nodo gestito è determinato da SSM Agent. Questo attributo corrisponde al valore dell'attributo chiave Product nel tipo di dati [PatchFilter](#) della baseline delle patch.
- La selezione dei pacchetti per l'aggiornamento si basa sulle seguenti linee guida.

Opzione di sicurezza	Selezione di patch
Pre-defined linee di base delle patch predefinite fornite da AWS e linee di base delle patch personalizzate in cui la casella di controllo Includi aggiornamenti non relativi alla sicurezza non è selezionata	<p>Per ogni avviso di aggiornamento in <code>updateinfo.xml</code>, la baseline delle patch viene utilizzata come filtro, per includere nell'aggiornamento solo i pacchetti qualificati. Se più pacchetti sono applicabili dopo l'applicazione della definizione della baseline delle patch, verrà utilizzata la versione più recente.</p> <p>Per Amazon Linux 2, il comando yum equivalente per questo flusso di lavoro è:</p>

Opzione di sicurezza	Selezione di patch
	<pre data-bbox="868 226 1425 346">sudo yum update-minimal --sec-severity=Critical,Important --bugfix -y</pre> <p data-bbox="850 405 1430 489">Per Amazon Linux 2023, il comando dnf equivalente per questo flusso di lavoro è:</p> <pre data-bbox="868 548 1414 667">sudo dnf upgrade-minimal --sec-severity=Critical --sec-severity=Important --bugfix -y</pre>

Opzione di sicurezza	Selezione di patch
<p>Baseline delle patch personalizzate in cui è selezionata la casella di controllo Includi aggiornamenti non critici con un elenco di GRAVITÀ [Critical, Important] e un elenco di CLASSIFICAZIONE [Security, Bugfix]</p>	<p>Oltre ad applicare gli aggiornamenti di sicurezza selezionati in <code>updateinfo.xml</code>, Patch Manager applica gli aggiornamenti non di sicurezza che altrimenti soddisfano le regole di filtro delle patch.</p> <p>Per Amazon Linux 2, il comando <code>yum</code> equivalente per questo flusso di lavoro è:</p> <pre>sudo yum update --security --sec-severity=Critical,Important --bugfix -y</pre> <p>Per Amazon Linux 2023, il comando <code>dnf</code> equivalente per questo flusso di lavoro è:</p> <pre>sudo dnf upgrade --security --sec-severity=Critical --sec-severity=Important --bugfix -y</pre> <div data-bbox="850 1129 1507 1581"> <p> Note</p> <p>I nuovi pacchetti che sostituiscono quelli ormai obsoleti con nomi diversi vengono installati se si eseguono questi comandi <code>yum</code> o <code>dnf</code> all'esterno di Patch Manager. Tuttavia, non vengono installati con operazioni di Patch Manager equivalenti.</p> </div>

Per informazioni sui valori dello stato di conformità delle patch, consulta [Valori dello stato di conformità delle patch](#).

Come funzionano le regole di base delle patch CentOS Stream

I repository CentOS Stream predefiniti non includono un file `updateinfo.xml`. Tuttavia, i repository personalizzati creati o utilizzati potrebbero includere questo file. In questo argomento, i riferimenti a `updateinfo.xml` si applicano solo a questi repository personalizzati.

Di seguito è riportato processo di selezione delle patch in CentOS Stream:

1. Nel nodo gestito, la libreria DNF accede al `updateinfo.xml` file, qualora esistesse in un repository personalizzato, per ciascun repository configurato.

Se non viene `updateinfo.xml` trovata alcuna soluzione, che include sempre i repository predefiniti, l'installazione delle patch dipende dalle impostazioni per `Includi aggiornamenti non di sicurezza e Auto-approval`. Ad esempio, se gli aggiornamenti non relativi alla protezione sono consentiti, vengono installati quando arriva l'ora di approvazione automatica.

2. Quando `updateinfo.xml` è presente, ogni avviso di aggiornamento nel file include vari attributi che denotano le proprietà dei pacchetti dell'avviso, come descritto nella seguente tabella.

Attributi degli avvisi di aggiornamento

Attributo	Description
tipo	<p>Corrisponde al valore dell'attributo chiave <code>Classification</code> nel tipo di dati PatchFilter della baseline delle patch. Indica il tipo di pacchetto incluso nell'avviso di aggiornamento.</p> <p>È possibile visualizzare l'elenco dei valori supportati utilizzando il AWS CLI comando describe-patch-properties o l'operazione API. DescribePatchProperties È anche possibile visualizzare l'elenco nell'area Norme di approvazione della pagina Create patch baseline (Creazione di una baseline delle patch) della pagina Edit patch baseline (Modifica della baseline delle patch) nella console Systems Manager.</p>

Attributo	Description
severity	<p>Corrisponde al valore dell'attributo chiave Severity nel tipo di dati PatchFilter della baseline delle patch. Indica il tipo di gravità dei pacchetti inclusi nell'avviso di aggiornamento. Generalmente applicabile solo per gli avvisi di aggiornamento Security.</p> <p>È possibile visualizzare l'elenco dei valori supportati utilizzando il AWS CLI comando describe-patch-properties o l'operazione API DescribePatchProperties. È anche possibile visualizzare l'elenco nell'area Norme di approvazione della pagina Create patch baseline (Creazione di una baseline delle patch) della pagina Edit patch baseline (Modifica della baseline delle patch) nella console Systems Manager.</p>
update_id	<p>Indica l'ID dell'avviso, ad esempio. CVE-2019-17055 L'ID consulenza può essere utilizzato nell'attributo ApprovedPatches o RejectedPatches della baseline delle patch.</p>
referimenti	<p>Contiene informazioni aggiuntive sull'avviso di aggiornamento, come un ID CVE (formato: CVE-2019-17055) o un ID Bugzilla (formato: 1463241). L'ID CVE e l'ID Bugzilla possono essere utilizzati nell'attributo ApprovedPatches o RejectedPatches della baseline delle patch.</p>

Attributo	Description
emesso	Corrisponde a ApproveAfterDays nella baseline delle patch. Indica la data di rilascio (data di emissione) dei pacchetti inclusi nell'avviso di aggiornamento. Per stabilire se la patch è approvata per la distribuzione, si effettua un confronto tra il timestamp corrente e il valore di questo attributo più <code>ApproveAfterDays</code> .

Per informazioni sui formati accettati per gli elenchi delle patch approvate e di quelle rifiutate, consulta [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#).

- In tutti i casi, Il prodotto del nodo gestito è determinato da SSM Agent. Questo attributo corrisponde al valore dell'attributo chiave Product nel tipo di dati [PatchFilter](#) della baseline delle patch.
- La selezione dei pacchetti per l'aggiornamento si basa sulle seguenti linee guida.

Opzione di sicurezza	Selezione di patch
Pre-defined linee di base delle patch predefinite fornite da AWS e linee di base delle patch personalizzate in cui la casella di controllo <code>Includi aggiornamenti non relativi alla sicurezza</code> non è selezionata	<p>Per ogni avviso di aggiornamento in <code>updateinfo.xml</code>, qualora esistesse in un repository personalizzato, la baseline delle patch viene utilizzata come filtro, per includere nell'aggiornamento solo i pacchetti qualificati. Se più pacchetti sono applicabili dopo l'applicazione della definizione della baseline delle patch, verrà utilizzata la versione più recente.</p> <p>Per CentOS Stream in cui <code>updateinfo.xml</code> è presente, il comando <code>dnf</code> equivalente per questo flusso di lavoro è:</p>

Opzione di sicurezza	Selezione di patch
	<pre>sudo dnf upgrade-minimal --sec-severity=Critical --sec-severity=Important --bugfix -y</pre>

Opzione di sicurezza	Selezione di patch
<p>Baseline delle patch personalizzate in cui è selezionata la casella di controllo Includi aggiornamenti non critici con un elenco di GRAVITÀ [Critical, Important] e un elenco di CLASSIFICAZIONE [Security, Bugfix]</p>	<p>Oltre ad applicare gli aggiornamenti di sicurezza selezionati in <code>updateinfo.xml</code>, se presenti in un repository personalizzato, Patch Manager applica gli aggiornamenti non di sicurezza che altrimenti soddisfano le regole di filtro delle patch.</p> <p>Per CentOS Stream in cui <code>updateinfo.xml</code> è presente, il comando <code>dnf</code> equivalente per questo flusso di lavoro è:</p> <pre>sudo dnf upgrade --security --sec-severity=Critical --sec-severity=Important --bugfix -y</pre> <p>Per i repository predefiniti e i repository personalizzati senza <code>updateinfo.xml</code>, è necessario selezionare la casella di controllo Includi aggiornamenti non relativi alla sicurezza per aggiornare i pacchetti del sistema operativo (OS).</p> <div data-bbox="850 1226 1507 1686"> <p>Note</p> <p>I nuovi pacchetti che sostituiscono quelli ormai obsoleti con nomi diversi vengono installati se si eseguono questi comandi <code>yum</code> o <code>dnf</code> all'esterno di Patch Manager. Tuttavia, non vengono installati con operazioni di Patch Manager equivalenti.</p> </div>

Per informazioni sui valori dello stato di conformità delle patch, consulta [Valori dello stato di conformità delle patch](#).

Come funzionano le regole di base delle patch Debian Server

In Debian Server, il servizio delle baseline delle patch offre l'applicazione di filtri nei campi Priorità e Sezione. Questi campi sono in genere presenti per tutti pacchetti Debian Server. Per determinare se una patch è stata selezionata dalla baseline delle patch, Patch Manager effettua quanto segue:

1. Nei sistemi Debian Server, viene eseguito l'equivalente di `sudo apt-get update` per aggiornare l'elenco dei pacchetti disponibili. I repo non vengono configurati e i dati vengono estratti dai repo configurati in un elenco `sources`.
2. Se è disponibile un aggiornamento per `python3-apt` (un'interfaccia di libreria Python per `libapt`), viene aggiornato alla versione più recente. (Questo pacchetto non correlato alla sicurezza viene aggiornato anche se non è stata selezionata l'opzione `Includi aggiornamenti non correlati alla protezione`).
3. Quindi, vengono applicati gli elenchi [GlobalFilters](#), [ApprovalRules](#), [ApprovedPatches](#) e [RejectedPatches](#).

Note

Poiché non è possibile determinare in modo affidabile le date di rilascio dei pacchetti di aggiornamento per Debian Server, le opzioni di approvazione automatica non sono supportate per questo sistema operativo.

Le norme di approvazione, tuttavia, sono anche soggette al fatto che la casella di spunta `Includi aggiornamenti non correlati alla protezione` è stata selezionata durante la creazione o l'ultimo aggiornamento di una baseline delle patch.

Se sono esclusi aggiornamenti non di sicurezza, viene applicata una regola implicita per selezionare solo i pacchetti con gli aggiornamenti nei repo di sicurezza. Per ciascun pacchetto, la versione candidata (in genere, quella più recente) deve fare parte di un repo di sicurezza. In questo caso, per Debian Server, le versioni candidate alle patch sono limitate alle patch incluse nei seguenti repository:

Questi repository sono denominati come segue:

- Debian Server11: `debian-security bullseye`
- Debian Server12: `debian-security bookworm`

Se sono inclusi aggiornamenti non correlati alla protezione, vengono prese in considerazione anche le patch di altri repository.

Per informazioni sui formati accettati per gli elenchi delle patch approvate e di quelle rifiutate, consulta [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#).

Per visualizzare i contenuti dei campi Priority (Priorità) e Section (Sezione), eseguire il seguente comando aptitude:

 Note

Potrebbe essere necessario installare prima Aptitude nei sistemi Debian Server.

```
aptitude search -F '%p %P %s %t %V#' '~U'
```

Nella risposta a questo comando, tutti i pacchetti aggiornabili vengono specificati in questo formato:

```
name, priority, section, archive, candidate version
```

Per informazioni sui valori dello stato di conformità delle patch, consulta [Valori dello stato di conformità delle patch](#).

Come funzionano le regole di base delle patch macOS

Di seguito è riportato processo di selezione delle patch in macOS:

1. Sul nodo gestito, Patch Manager accede al contenuto analizzato del file `InstallHistory.plist` e identifica i nomi e le versioni dei pacchetti.

Per dettagli sul processo di analisi, consulta la sezione macOS in [Come vengono installate le patch](#).

2. Il prodotto del nodo gestito è determinato da SSM Agent. Questo attributo corrisponde al valore dell'attributo chiave Product nel tipo di dati [PatchFilter](#) della baseline delle patch.
3. La selezione dei pacchetti per l'aggiornamento si basa sulle seguenti linee guida.

Opzione di sicurezza	Selezione di patch
Pre-defined linee di base delle patch predefinite fornite da AWS e linee di base delle patch personalizzate in cui la casella di controllo <code>Includi aggiornamenti non relativi alla sicurezza</code> non è selezionata	Per ogni aggiornamento di pacchetto disponibile, la baseline delle patch viene utilizzata come filtro, per includere nell'aggiornamento solo i pacchetti qualificati. Se più pacchetti sono applicabili dopo l'applicazione della definizione della baseline delle patch, verrà utilizzata la versione più recente.
Baseline delle patch personalizzate in cui è selezionata la casella di controllo <code>Includi aggiornamenti non critici</code>	Oltre ad applicare gli aggiornamenti di sicurezza identificati utilizzando <code>InstallHistory.plist</code> , Patch Manager applica gli aggiornamenti non di sicurezza che altrimenti soddisfano le regole di filtro delle patch.

Per informazioni sui valori dello stato di conformità delle patch, consulta [Valori dello stato di conformità delle patch](#).

Come funzionano le regole di base delle patch Oracle Linux

Di seguito è riportato processo di selezione delle patch in Oracle Linux:

1. Nel nodo gestito, la libreria YUM accede al file `updateinfo.xml` per ciascun repo configurato.

Note

Il file `updateinfo.xml` potrebbe non essere disponibile se il repo non è gestito da Oracle Linux. Se non viene trovato `updateinfo.xml`, l'eventuale installazione delle patch dipende dalle impostazioni per `Includi aggiornamenti non di sicurezza` e `Auto-approval`. Ad esempio, se gli aggiornamenti non relativi alla protezione sono consentiti, vengono installati quando arriva l'ora di approvazione automatica.

2. Ogni avviso di aggiornamento di `updateinfo.xml` include vari attributi che denotano le proprietà dei pacchetti dell'avviso, come descritto nella seguente tabella.

Attributi degli avvisi di aggiornamento

Attributo	Description
tipo	<p>Corrisponde al valore dell'attributo chiave Classification nel tipo di dati PatchFilter della baseline delle patch. Indica il tipo di pacchetto incluso nell'avviso di aggiornamento.</p> <p>È possibile visualizzare l'elenco dei valori supportati utilizzando il AWS CLI comando describe-patch-properties o l'operazione API DescribePatchProperties. È anche possibile visualizzare l'elenco nell'area Norme di approvazione della pagina Create patch baseline (Creazione di una baseline delle patch) della pagina Edit patch baseline (Modifica della baseline delle patch) nella console Systems Manager.</p>
severity	<p>Corrisponde al valore dell'attributo chiave Severity nel tipo di dati PatchFilter della baseline delle patch. Indica il tipo di gravità dei pacchetti inclusi nell'avviso di aggiornamento. Generalmente applicabile solo per gli avvisi di aggiornamento Security.</p> <p>È possibile visualizzare l'elenco dei valori supportati utilizzando il AWS CLI comando describe-patch-properties o l'operazione API DescribePatchProperties. È anche possibile visualizzare l'elenco nell'area Norme di approvazione della pagina Create patch baseline (Creazione di una baseline delle patch) della pagina Edit patch baseline (Modifica della baseline delle patch) nella console Systems Manager.</p>

Attributo	Description
update_id	Indica l'ID dell'avviso, ad esempio. CVE-2019-17055 L'ID consulenza può essere utilizzato nell'attributo ApprovedPatches o RejectedPatches della baseline delle patch.
riferimenti	Contiene informazioni aggiuntive sull'avviso di aggiornamento, come un ID CVE (formato: CVE-2019-17055) o un ID Bugzilla (formato: 1463241). L'ID CVE e l'ID Bugzilla possono essere utilizzati nell'attributo ApprovedPatches o RejectedPatches della baseline delle patch.
emesso	Corrisponde a ApproveAfterDays nella baseline delle patch. Indica la data di rilascio (data di emissione) dei pacchetti inclusi nell'avviso di aggiornamento. Per stabilire se la patch è approvata per la distribuzione, si effettua un confronto tra il timestamp corrente e il valore di questo attributo più <code>ApproveAfterDays</code> .

Per informazioni sui formati accettati per gli elenchi delle patch approvate e di quelle rifiutate, consulta [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#).

- Il prodotto del nodo gestito è determinato da SSM Agent. Questo attributo corrisponde al valore dell'attributo chiave Product nel tipo di dati [PatchFilter](#) della baseline delle patch.
- La selezione dei pacchetti per l'aggiornamento si basa sulle seguenti linee guida.

Opzione di sicurezza	Selezione di patch
Pre-defined linee di base delle patch predefinite fornite da AWS e linee di base delle patch personalizzate in cui la casella di	Per ogni avviso di aggiornamento in <code>updateinfo.xml</code> , la baseline delle patch viene utilizzata come filtro, per includere nell'aggiornamento solo i pacchetti qualificati.

Opzione di sicurezza	Selezione di patch
<p>controllo Includi aggiornamenti non relativi alla sicurezza non è selezionata</p>	<p>Se più pacchetti sono applicabili dopo l'applicazione della definizione della baseline delle patch, verrà utilizzata la versione più recente.</p> <p>Per i nodi gestiti della versione 7, il comando yum equivalente per questo flusso di lavoro è:</p> <pre data-bbox="852 506 1507 663">sudo yum update-minimal --sec-severity=Important,Moderate --bugfix -y</pre> <p>Per i nodi gestiti della versione 8 e 9, il comando dnf equivalente per questo flusso di lavoro è:</p> <pre data-bbox="852 869 1507 1026">sudo dnf upgrade-minimal --security --sec-severity=Moderate --sec-severity=Important</pre>

Opzione di sicurezza	Selezione di patch
<p>Baseline delle patch personalizzate in cui è selezionata la casella di controllo Includi aggiornamenti non critici con un elenco di GRAVITÀ [Critical, Important] e un elenco di CLASSIFICAZIONE [Security, Bugfix]</p>	<p>Oltre ad applicare gli aggiornamenti di sicurezza selezionati in <code>updateinfo.xml</code>, Patch Manager applica gli aggiornamenti non di sicurezza che altrimenti soddisfano le regole di filtro delle patch.</p> <p>Per i nodi gestiti della versione 7, il comando yum equivalente per questo flusso di lavoro è:</p> <pre>sudo yum update --security --sec-severity=Critical,Important --bugfix -y</pre> <p>Per i nodi gestiti della versione 8 e 9, il comando dnf equivalente per questo flusso di lavoro è:</p> <pre>sudo dnf upgrade --security --sec-severity=Critical, --sec-severity=Important --bugfix y</pre> <div data-bbox="850 1178 1507 1633"> <p> Note</p> <p>I nuovi pacchetti che sostituiscono quelli ormai obsoleti con nomi diversi vengono installati se si eseguono questi comandi yum o dnf all'esterno di Patch Manager. Tuttavia, non vengono installati con operazioni di Patch Manager equivalenti.</p> </div>

Per informazioni sui valori dello stato di conformità delle patch, consulta [Valori dello stato di conformità delle patch](#).

Come funzionano le regole di base delle patch su, AlmaLinux RHEL e Rocky Linux

Su AlmaLinux, Red Hat Enterprise Linux (RHEL) e Rocky Linux, il processo di selezione delle patch è il seguente:

1. Sul nodo gestito, la libreria YUM (RHEL7) o la libreria DNF (AlmaLinux 8 e 9, RHEL 8, 9 e 10 e Rocky Linux 8 e 9) accede al `updateinfo.xml` file per ogni repository configurato.

Note

Il file `updateinfo.xml` potrebbe non essere disponibile se il repo non è gestito da Red Hat. Se non viene trovato alcun `updateinfo.xml`, l'eventuale installazione delle patch dipende dalle impostazioni per `Includi aggiornamenti non di sicurezza e. Auto-approval`. Ad esempio, se gli aggiornamenti non relativi alla protezione sono consentiti, vengono installati quando arriva l'ora di approvazione automatica.

2. Ogni avviso di aggiornamento di `updateinfo.xml` include vari attributi che denotano le proprietà dei pacchetti dell'avviso, come descritto nella seguente tabella.

Attributi degli avvisi di aggiornamento

Attributo	Description
tipo	<p>Corrisponde al valore dell'attributo chiave <code>Classification</code> nel tipo di dati PatchFilter della baseline delle patch. Indica il tipo di pacchetto incluso nell'avviso di aggiornamento.</p> <p>È possibile visualizzare l'elenco dei valori supportati utilizzando il AWS CLI comando describe-patch-properties o l'operazione API. DescribePatchProperties. È anche possibile visualizzare l'elenco nell'area Norme di approvazione della pagina Create patch baseline (Creazione di una baseline delle patch) della pagina Edit patch baseline (Modifica della baseline delle patch) nella console Systems Manager.</p>

Attributo	Description
severity	<p>Corrisponde al valore dell'attributo chiave Severity nel tipo di dati PatchFilter della baseline delle patch. Indica il tipo di gravità dei pacchetti inclusi nell'avviso di aggiornamento. Generalmente applicabile solo per gli avvisi di aggiornamento Security.</p> <p>È possibile visualizzare l'elenco dei valori supportati utilizzando il AWS CLI comando describe-patch-properties o l'operazione API DescribePatchProperties. È anche possibile visualizzare l'elenco nell'area Norme di approvazione della pagina Create patch baseline (Creazione di una baseline delle patch) della pagina Edit patch baseline (Modifica della baseline delle patch) nella console Systems Manager.</p>
update_id	<p>Indica l'ID dell'avviso, ad esempio. RHSA-2017:0864 L'ID consulenza può essere utilizzato nell'attributo ApprovedPatches o RejectedPatches della baseline delle patch.</p>
referimenti	<p>Contiene informazioni aggiuntive sull'avviso di aggiornamento, come un ID CVE (formato: CVE-2017-1000371) o un ID Bugzilla (formato: 1463241). L'ID CVE e l'ID Bugzilla possono essere utilizzati nell'attributo ApprovedPatches o RejectedPatches della baseline delle patch.</p>

Attributo	Description
emesso	Corrisponde a ApproveAfterDays nella baseline delle patch. Indica la data di rilascio (data di emissione) dei pacchetti inclusi nell'avviso di aggiornamento. Per stabilire se la patch è approvata per la distribuzione, si effettua un confronto tra il timestamp corrente e il valore di questo attributo più <code>ApproveAfterDays</code> .

Per informazioni sui formati accettati per gli elenchi delle patch approvate e di quelle rifiutate, consulta [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#).

- Il prodotto del nodo gestito è determinato da SSM Agent. Questo attributo corrisponde al valore dell'attributo chiave `Product` nel tipo di dati [PatchFilter](#) della baseline delle patch.
- La selezione dei pacchetti per l'aggiornamento si basa sulle seguenti linee guida.

Opzione di sicurezza	Selezione di patch
Pre-defined linee di base delle patch predefinite fornite da AWS e linee di base delle patch personalizzate in cui la casella di controllo <code>Includi aggiornamenti non relativi alla sicurezza</code> non è selezionata in nessuna regola	<p>Per ogni avviso di aggiornamento in <code>updateinfo.xml</code>, la baseline delle patch viene utilizzata come filtro, per includere nell'aggiornamento solo i pacchetti qualificati. Se più pacchetti sono applicabili dopo l'applicazione della definizione della baseline delle patch, verrà utilizzata la versione più recente.</p> <p>For RHEL 7, il comando <code>yum</code> equivalente per questo flusso di lavoro è:</p> <pre>sudo yum update-minimal --sec-severity=Critical,Important --bugfix -y</pre>

Opzione di sicurezza	Selezione di patch
	<p>Per AlmaLinux 8 e 9, RHEL 8, 9 e 10 e Rocky Linux 8 e 9, il comando dnf equivalente per questo flusso di lavoro è:</p> <pre data-bbox="852 380 1508 537">sudo dnf upgrade-minimal --sec-severity=Critical --sec-severity=Important --bugfix -y</pre>

Opzione di sicurezza	Selezione di patch
<p>Baseline delle patch personalizzate in cui è selezionata la casella di controllo Includi aggiornamenti non critici con un elenco di GRAVITÀ [Critical, Important] e un elenco di CLASSIFICAZIONE [Security, Bugfix]</p>	<p>Oltre ad applicare gli aggiornamenti di sicurezza selezionati in <code>updateinfo.xml</code>, Patch Manager applica gli aggiornamenti non di sicurezza che altrimenti soddisfano le regole di filtraggio delle patch.</p> <p>For RHEL 7, il comando yum equivalente per questo flusso di lavoro è:</p> <pre>sudo yum update --security --sec-severity=Critical,Important --bugfix -y</pre> <p>Per AlmaLinux 8 e 9, RHEL 8, 9 e 10 e Rocky Linux 8 e 9, il comando dnf equivalente per questo flusso di lavoro è:</p> <pre>sudo dnf upgrade --sec-severity=Critical --sec-severity=Important --bugfix -y</pre> <div data-bbox="850 1178 1507 1633"> <p> Note</p> <p>I nuovi pacchetti che sostituiscono quelli ormai obsoleti con nomi diversi vengono installati se si eseguono questi comandi yum o dnf all'esterno di Patch Manager. Tuttavia, non vengono installati con operazioni di Patch Manager equivalenti.</p> </div>

Per informazioni sui valori dello stato di conformità delle patch, consulta [Valori dello stato di conformità delle patch](#).

Come funzionano le regole di base delle patch su SUSE Linux Enterprise Server

In SLES, ogni patch include i seguenti attributi che denotano le proprietà dei pacchetti della patch:

- **Category:** corrisponde al valore dell'attributo chiave Classification nel tipo di dati [PatchFilter](#) della baseline delle patch. Indica il tipo di patch incluso nell'avviso di aggiornamento.

È possibile visualizzare l'elenco dei valori supportati utilizzando il AWS CLI comando [describe-patch-properties](#) o l'operazione [DescribePatchProperties](#) API. È anche possibile visualizzare l'elenco nell'area Norme di approvazione della pagina Create patch baseline (Creazione di una baseline delle patch) della pagina Edit patch baseline (Modifica della baseline delle patch) nella console Systems Manager.

- **Gravità:** corrisponde al valore dell'attributo chiave Gravità nel tipo di dati [PatchFilter](#) della baseline delle patch. Indica la gravità delle patch.

È possibile visualizzare l'elenco dei valori supportati utilizzando il AWS CLI comando [describe-patch-properties](#) o l'operazione API [DescribePatchProperties](#). È anche possibile visualizzare l'elenco nell'area Norme di approvazione della pagina Create patch baseline (Creazione di una baseline delle patch) della pagina Edit patch baseline (Modifica della baseline delle patch) nella console Systems Manager.

Il prodotto del nodo gestito è determinato da SSM Agent. Questo attributo corrisponde al valore dell'attributo chiave Product nel tipo di dati [PatchFilter](#) della baseline delle patch.

Per ogni patch, la baseline delle patch viene utilizzata come filtro, per includere nell'aggiornamento solo i pacchetti qualificati. Se più pacchetti sono applicabili dopo l'applicazione della definizione della baseline delle patch, verrà utilizzata la versione più recente.

Per informazioni sui formati accettati per gli elenchi delle patch approvate e di quelle rifiutate, consulta [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#).

Come funzionano le regole di base delle patch Ubuntu Server

In Ubuntu Server, il servizio delle baseline delle patch offre l'applicazione di filtri nei campi Priorità e Sezione. Questi campi sono in genere presenti per tutti pacchetti Ubuntu Server. Per determinare se una patch è stata selezionata dalla baseline delle patch, Patch Manager effettua quanto segue:

1. Nei sistemi Ubuntu Server, viene eseguito l'equivalente di `sudo apt-get update` per aggiornare l'elenco dei pacchetti disponibili. I repo non vengono configurati e i dati vengono estratti dai repo configurati in un elenco `sources`.

2. Se è disponibile un aggiornamento per python3-apt (un'interfaccia di libreria Python per libapt), viene aggiornato alla versione più recente. (Questo pacchetto non correlato alla sicurezza viene aggiornato anche se non è stata selezionata l'opzione Includi aggiornamenti non correlati alla protezione).
3. Quindi, vengono applicati gli elenchi [GlobalFilters](#), [ApprovalRules](#), [ApprovedPatches](#) e [RejectedPatches](#).

 Note

Poiché non è possibile determinare in modo affidabile le date di rilascio dei pacchetti di aggiornamento per Ubuntu Server, le opzioni di approvazione automatica non sono supportate per questo sistema operativo.

Le norme di approvazione, tuttavia, sono anche soggette al fatto che la casella di spunta `Includi aggiornamenti non correlati alla protezione` è stata selezionata durante la creazione o l'ultimo aggiornamento di una baseline delle patch.

Se sono esclusi aggiornamenti non di sicurezza, viene applicata una regola implicita per selezionare solo i pacchetti con gli aggiornamenti nei repo di sicurezza. Per ciascun pacchetto, la versione candidata (in genere, quella più recente) deve fare parte di un repo di sicurezza. In questo caso, per Ubuntu Server, le versioni candidate alle patch sono limitate alle patch incluse nei seguenti repository:

- Ubuntu Server 18.04 LTS: `bionic-security`
- Ubuntu Server 20.04 LTS: `focal-security`
- Ubuntu Server 22.04 LTS: `jammy-security`
- Ubuntu Server 24.04 LTS: `noble-security`
- Ubuntu Server 25.04: `plucky-security`

Se sono inclusi aggiornamenti non correlati alla protezione, vengono prese in considerazione anche le patch di altri repository.

Per informazioni sui formati accettati per gli elenchi delle patch approvate e di quelle rifiutate, consulta [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#).

Per visualizzare i contenuti dei campi Priority (Priorità) e Section (Sezione), eseguire il seguente comando aptitude:

 Note

Potrebbe essere necessario installare prima Aptitude nei sistemi Ubuntu Server 16.

```
aptitude search -F '%p %P %s %t %V#' '~U'
```

Nella risposta a questo comando, tutti i pacchetti aggiornabili vengono specificati in questo formato:

```
name, priority, section, archive, candidate version
```

Per informazioni sui valori dello stato di conformità delle patch, consulta [Valori dello stato di conformità delle patch](#).

Differenze nelle operazioni di patching tra Linux e Windows Server

Questo argomento descrive le differenze importanti tra Linux e l'applicazione delle Windows Server patch. Patch Manager

 Note

Per applicare patch ai nodi gestiti Linux, i nodi devono essere in esecuzione la versione 2.0.834.0 SSM Agent o successive.

Una versione aggiornata di SSM Agent viene distribuita ogni volta che vengono aggiunti nuovi strumenti a Systems Manager o eseguiti aggiornamenti degli strumenti esistenti. Il mancato utilizzo della versione più recente dell'agente può impedire al nodo gestito di utilizzare vari strumenti e funzionalità di Systems Manager. Per questo motivo, ti consigliamo di automatizzare il processo di aggiornamento di SSM Agent sulle macchine. Per informazioni, consulta [Automatizzazione degli aggiornamenti a Agente SSM](#). Iscriviti alla pagina [Note di rilascio di SSM Agent](#) su GitHub per ricevere notifiche sugli aggiornamenti di SSM Agent.

Differenza 1: valutazione delle patch

Patch Manager utilizza diversi processi sui nodi gestiti da Windows e sui nodi gestiti da Linux per valutare quali patch devono essere presenti.

Linux

Per l'applicazione di patch in Linux, Systems Manager valuta le regole della baseline delle patch e l'elenco delle patch approvate e rifiutate in ciascun nodo gestito. Systems Manager deve valutare l'applicazione di patch in ogni nodo perché il servizio recupera l'elenco delle patch e aggiornamenti noti dai repository configurati nel nodo gestito.

Windows

Per l'applicazione di patch in Windows, Systems Manager valuta le regole della baseline delle patch e l'elenco delle patch approvate e rifiutate direttamente nel servizio. Può eseguire questa operazione perché le patch di Windows vengono estratte da un unico repository (Windows Update).

Differenza 2: **patch non applicabili**

A causa del numero elevato di pacchetti disponibili per i sistemi operativi Linux, Systems Manager non indica i dettagli delle patch con lo stato Not Applicable. Una patch Not Applicable è, ad esempio, una patch per il software Apache quando nell'istanza non è installato Apache. Systems Manager riporta il numero di Not Applicable patch nel riepilogo, ma se si chiama l'[DescribeInstancePatches](#) API per un nodo gestito, i dati restituiti non includono le patch con uno stato di Not Applicable. Questo comportamento è diverso da quello in Windows.

Differenza 3: supporto dei documenti SSM

Il documento Systems Manager AWS-ApplyPatchBaseline (documento SSM) non supporta i nodi gestiti di Linux. Per l'applicazione di baseline delle patch a entrambi i nodi gestiti a Linux, macOS, e Windows Server, il documento SSM consigliato è AWS-RunPatchBaseline. Per ulteriori informazioni, consulta [Documenti sul comando SSM per l'applicazione di patch a nodi gestiti](#) e [Documento di comando SSM per l'applicazione di patch: AWS-RunPatchBaseline](#).

Differenza 4: patch di applicazione

L'obiettivo principale di Patch Manager è l'applicazione di patch ai sistemi operativi. Tuttavia può essere utilizzato Patch Manager anche per applicare patch ad alcune applicazioni nei propri nodi gestiti.

Linux

Nei sistemi operativi Linux Patch Manager usa il repository configurato per gli aggiornamenti e non fa differenze tra le patch dei sistemi operativi e quelle di applicazione. È possibile utilizzare Patch Manager per specificare da quali repository recuperare gli aggiornamenti. Per ulteriori informazioni, consulta [Come specificare un repository alternativo di origine delle patch \(Linux\)](#).

Windows

Sui nodi Windows Server gestiti, è possibile applicare regole di approvazione ed eccezioni alle patch approvate e rifiutate per le applicazioni rilasciate da Microsoft, come Microsoft Word 2016 e Microsoft Exchange Server 2016. Per ulteriori informazioni, consulta [Utilizzo delle baseline delle patch personalizzate](#).

Differenza 5: opzioni dell'elenco delle patch rifiutate nelle baseline delle patch personalizzate

Quando si crea una baseline delle patch personalizzata, è possibile specificare una o più patch per un elenco di Patch rifiutate. Per i nodi gestiti da Linux, è possibile anche scegliere di consentirne l'installazione nel caso siano dipendenze per un'altra patch consentita dalla baseline.

Windows Server, tuttavia, non supporta il concetto di dipendenze dalle patch. È possibile aggiungere una patch all'elenco delle patch rifiutate in una linea di base personalizzata per Windows Server, ma il risultato dipende da (1) se la patch rifiutata è già installata su un nodo gestito e (2) dall'opzione scelta per l'azione Patch rifiutate.

Patch rifiutate negli aggiornamenti di Windows in bundle

Microsoft combina alcuni aggiornamenti di Windows in un unico aggiornamento con un ID Microsoft Knowledge Base (KB) principale. Questo aggiornamento contiene più aggiornamenti dei componenti (ID KB secondari) e installa il componente applicabile al nodo gestito.

Windows Server Attivato, Patch Manager applica l'elenco delle patch rifiutate all'aggiornamento reso disponibile da Windows Update, ovvero l'aggiornamento principale. Se si aggiunge solo un KB secondario all'elenco delle patch rifiutate mentre l'aggiornamento principale è approvato dalla baseline, Patch Manager approva l'aggiornamento principale. Windows Update installa quindi il componente figlio applicabile come parte dell'aggiornamento principale.

Fai riferimento alla tabella seguente per i dettagli sulle opzioni di patch rifiutate su Windows Server.

Stato di installazione	Opzione: "Consenti come dipendenza"	Opzione: "Blocco"
La patch è già installata	Stato segnalato: INSTALLED _OTHER	Stato segnalato: INSTALLED _REJECTED

Stato di installazione	Opzione: "Consenti come dipendenza"	Opzione: "Blocco"
La patch non è già installata	Patch ignorata	Patch ignorata

Ogni patch per Windows Server che viene rilasciata da Microsoft contiene in genere tutte le informazioni necessarie per il corretto completamento dell'installazione. A volte, tuttavia, è necessario un pacchetto prerequisito, da installare manualmente. Patch Manager non riporta informazioni su questi prerequisiti. Per informazioni correlate, consulta la sezione [Risoluzione dei problemi di Windows Update](#) sul sito web di Microsoft.

Documenti sul comando SSM per l'applicazione di patch a nodi gestiti

Questo argomento descrive gli otto documenti di Systems Manager (documenti SSM) attualmente disponibili, utili per assicurarti che i nodi gestiti vengano applicati patch mediante gli aggiornamenti più recenti correlati alla sicurezza.

Consigliamo di utilizzare solo cinque di questi documenti per le applicazione di patch. Questi cinque documenti SSM offrono una gamma completa di opzioni di applicazione di patch utilizzando AWS Systems Manager. Quattro di questi documenti sono stati rilasciati successivamente ai quattro documenti SSM legacy che sostituiscono e rappresentano espansioni o consolidamenti di funzionalità.

Documenti SSM consigliati per l'applicazione di patch

Consigliamo di utilizzare i cinque documenti SSM seguenti per le operazioni di applicazione di patch.

- AWS-ConfigureWindowsUpdate
- AWS-InstallWindowsUpdates
- AWS-RunPatchBaseline
- AWS-RunPatchBaselineAssociation
- AWS-RunPatchBaselineWithHooks

Documenti SSM legacy per l'applicazione di patch

I seguenti quattro documenti SSM legacy rimangono disponibili in alcune Regioni AWS ma non sono più aggiornati o supportati. Non è garantito il funzionamento di questi documenti in ambienti IPv6

e supportano solo IPv4. Non è possibile garantire che funzionino in tutti gli scenari e potrebbero perdere supporto in futuro. Si consiglia di non utilizzare questi documenti per le operazioni di applicazione di patch.

- `AWS-ApplyPatchBaseline`
- `AWS-FindWindowsUpdates`
- `AWS-InstallMissingWindowsUpdates`
- `AWS-InstallSpecificWindowsUpdates`

Per i passaggi per configurare le operazioni di patching in un ambiente che supporta solo IPv6, consulta. [Tutorial: applicare patch a un server in un ambiente solo IPv6](#)

Per ulteriori informazioni sull'uso di questi documenti SSM nelle operazioni di applicazione di patch, consulta le seguenti sezioni.

Documenti SSM consigliati per i nodi gestiti di applicazione di patch

I seguenti cinque documenti SSM sono consigliati per l'uso nelle operazioni di applicazioni di patch nei nodi gestiti.

Documenti SSM consigliati

- [AWS-ConfigureWindowsUpdate](#)
- [AWS-InstallWindowsUpdates](#)
- [AWS-RunPatchBaseline](#)
- [AWS-RunPatchBaselineAssociation](#)
- [AWS-RunPatchBaselineWithHooks](#)

AWS-ConfigureWindowsUpdate

Supporta la configurazione di funzioni Windows Update di base e il relativo utilizzo per l'installazione automatica degli aggiornamenti (o per disabilitare gli aggiornamenti automatici). Disponibile in tutte le Regioni AWS.

Questo documento SSM richiede a Windows Update di scaricare e installare gli aggiornamenti specificati e di riavviare i nodi gestiti in base alle esigenze. Usa questo documento con State Manager per assicurarti che Windows Update mantenga la sua configurazione. Puoi anche eseguirlo manualmente con Run Command per modificare la configurazione di Windows Update.

I parametri disponibili in questo documento consentono di specificare una categoria di aggiornamenti da installare (o se disattivare gli aggiornamenti automatici) e di specificare il giorno della settimana e l'ora del giorno in cui eseguire le operazioni di applicazione delle patch. Questo documento SSM è utile in particolare se non devi controllare rigidamente gli aggiornamenti Windows e se non devi raccogliere le informazioni sulla conformità.

Sostituisce i seguenti documenti SSM legacy:

- Nessuno

AWS-InstallWindowsUpdates

Installa gli aggiornamenti su un nodo gestito Windows Server. Disponibile in tutte le Regioni AWS.

Questo documento SSM offre le funzionalità delle basi di patch nel caso desiderassi installare un aggiornamento specifico (utilizzando il parametro `Include Kbs`) o installare le patch con specifiche classificazioni o categorie, senza necessità di avere le informazioni sulla conformità delle patch.

Sostituisce i seguenti documenti SSM legacy:

- AWS-FindWindowsUpdates
- AWS-InstallMissingWindowsUpdates
- AWS-InstallSpecificWindowsUpdates

I tre documenti precedenti svolgono funzioni diverse. Tuttavia, è possibile ottenere gli stessi risultati utilizzando impostazioni dei parametri diverse con il documento SSM più recente. `AWS-InstallWindowsUpdates` Tali impostazioni dei parametri sono descritte in [Documenti SSM legacy per l'applicazione di patch a nodi gestiti](#).

AWS-RunPatchBaseline

Consente di installare patch nei nodi gestiti o analizza i nodi per stabilire se eventuali patch qualificate risultano mancanti. Disponibile in tutte le Regioni AWS.

`AWS-RunPatchBaseline` consente di controllare l'approvazione delle patch utilizzando la baseline delle patch specificata come «predefinita» per un tipo di sistema operativo. Fornisce le informazioni sulla conformità delle patch visualizzabili con gli strumenti di conformità di Systems Manager. Questi strumenti offrono approfondimenti sullo stato di conformità delle patch dei nodi gestiti, ad esempio a quali nodi mancano le patch e quali sono tali patch. Quando si utilizza `AWS-`

RunPatchBaseline, le informazioni sulla conformità delle patch vengono registrate utilizzando il comando `APIPutInventory`. Per i sistemi operativi Linux, le informazioni sulla conformità vengono fornite per le patch dal repository di fonte di default configurato in un nodo gestito e da qualsiasi repository di origine alternativo specificato in una baseline delle patch personalizzata. Per ulteriori informazioni sui repository di origine alternativi, consulta [Come specificare un repository alternativo di origine delle patch \(Linux\)](#). Per ulteriori informazioni sugli strumenti di conformità di Systems Manager, consulta [AWS Systems Manager Conformità](#).

Sostituisce i seguenti documenti legacy:

- AWS-ApplyPatchBaseline

Il documento legacy AWS-ApplyPatchBaseline è valido solo per i nodi gestiti Windows Server e non fornisce supporto per l'applicazione di patch alle applicazioni. Il più recente AWS-RunPatchBaseline offre lo stesso supporto per i sistemi Windows e Linux. La versione 2.0.834.0 o successiva deve utilizzare il documento. SSM Agent AWS-RunPatchBaseline

Per ulteriori informazioni sull'utilizzo del documento SSM AWS-RunPatchBaseline, consulta [Documento di comando SSM per l'applicazione di patch: AWS-RunPatchBaseline](#).

AWS-RunPatchBaselineAssociation

Consente di installare patch nelle istanze o analizza le istanze per stabilire se eventuali patch qualificate risultano mancanti. Disponibile in tutte le Regioni AWS commerciali.

AWS-RunPatchBaselineAssociation differisce da AWS-RunPatchBaseline in alcuni modi importanti:

- AWS-RunPatchBaselineAssociation è destinato all'uso principalmente con associazioni State Manager create utilizzando Quick Setup, uno strumento di AWS Systems Manager. In particolare, quando utilizzi il tipo di configurazione di gestione host Quick Setup, scegliendo l'opzione Scan instances for missing patches daily (Scansiona le istanze per le patch mancanti ogni giorno), il sistema utilizza AWS-RunPatchBaselineAssociation per l'operazione.

Di solito, tuttavia, quando si impostano le proprie operazioni di patching, è necessario scegliere [AWS-RunPatchBaseline](#) o invece di [AWS-RunPatchBaselineWithHooks](#) AWS-RunPatchBaselineAssociation

Per ulteriori informazioni, consulta i seguenti argomenti:

- [AWS Systems Manager Configurazione rapida](#)
- [Documento di comando SSM per l'applicazione di patch: AWS-RunPatchBaselineAssociation](#)
- AWS-RunPatchBaselineAssociation supporta l'utilizzo di tag per identificare la baseline delle patch da utilizzare con un insieme di destinazioni durante l'esecuzione.
- Per le operazioni di applicazione di patch che utilizzano AWS-RunPatchBaselineAssociation, i dati di conformità delle patch vengono compilati in termini di un'associazione State Manager specifica. I dati di conformità delle patch raccolti quando AWS-RunPatchBaselineAssociation viene registrato utilizzando il comando PutComplianceItems al posto del comando PutInventory. Ciò impedisce che i dati di conformità non associati a questa particolare associazione vengano sovrascritti.

Per i sistemi operativi Linux, le informazioni sulla conformità vengono fornite per le patch dal repository di origine predefinito configurato in un'istanza e da qualsiasi repository di origine alternativo specificato in una baseline delle patch personalizzata. Per ulteriori informazioni sui repository di origine alternativi, consulta [Come specificare un repository alternativo di origine delle patch \(Linux\)](#). Per ulteriori informazioni sugli strumenti di conformità di Systems Manager, consulta [AWS Systems Manager Conformità](#).

Sostituisce i seguenti documenti legacy:

- Nessuno

Per ulteriori informazioni sull'utilizzo del documento SSM AWS-RunPatchBaselineAssociation, consulta [Documento di comando SSM per l'applicazione di patch: AWS-RunPatchBaselineAssociation](#).

AWS-RunPatchBaselineWithHooks

Consente di installare patch nei nodi gestiti o li analizza per determinare se eventuali patch qualificate risultano mancanti, con hook opzionali che è possibile utilizzare per eseguire i documenti SSM in tre punti durante il ciclo di applicazione di patch. Disponibile in tutte le Regioni AWS commerciali. Non supportato su macOS.

AWS-RunPatchBaselineWithHooks differisce da AWS-RunPatchBaseline nella sua operazione Install.

`AWS-RunPatchBaselineWithHooks` supporta gli hook del ciclo di vita che vengono eseguiti in punti designati durante l'applicazione di patch del nodo gestito. Poiché le installazioni di patch a volte richiedono il riavvio dei nodi gestiti, l'operazione di applicazione di patch è suddivisa in due eventi, per un totale di tre hook che supportano funzionalità personalizzate. Il primo hook è prima dell'operazione `Install with NoReboot`. Il secondo hook è dopo dell'operazione `Install with NoReboot`. Il terzo hook è disponibile dopo il riavvio del nodo.

Sostituisce i seguenti documenti legacy:

- Nessuno

Per ulteriori informazioni sull'utilizzo del documento SSM `AWS-RunPatchBaselineWithHooks`, consulta [Documento di comando SSM per l'applicazione di patch: AWS-RunPatchBaselineWithHooks](#).

Documenti SSM legacy per l'applicazione di patch a nodi gestiti

I seguenti quattro documenti SSM sono ancora disponibili in alcune Regioni AWS. Tuttavia, non sono più aggiornati e potrebbero non essere più supportati in futuro, pertanto ne sconsigliamo l'utilizzo. In sostituzione, usa i documenti descritti in [Documenti SSM consigliati per i nodi gestiti di applicazione di patch](#).

Documenti SSM legacy

- [AWS-ApplyPatchBaseline](#)
- [AWS-FindWindowsUpdates](#)
- [AWS-InstallMissingWindowsUpdates](#)
- [AWS-InstallSpecificWindowsUpdates](#)

AWS-ApplyPatchBaseline

Supporta solo i nodi gestiti Windows Server, ma non include il supporto per l'applicazione di patch alle applicazioni disponibili nel rispettivo documento sostitutivo `AWS-RunPatchBaseline`. Non disponibile in versione Regioni AWS lanciata dopo agosto 2017.

 Note

La sostituzione per questo documento SSM, `AWS-RunPatchBaseline`, richiede la versione 2.0.834.0 o una versione successiva di SSM Agent. È possibile utilizzare il documento `AWS-UpdateSSMAgent` per aggiornare i nodi gestiti alla versione più recente dell'agente.

AWS-FindWindowsUpdates

Sostituito da `AWS-InstallWindowsUpdates`, che è in grado di eseguire le stesse operazioni. Non disponibile in versione Regioni AWS lanciata dopo aprile 2017.

Per ottenere lo stesso risultato del documento SSM legacy, utilizza la seguente configurazione dei parametri con il documento sostitutivo consigliato, `AWS-InstallWindowsUpdates`:

- `Action = Scan`
- `Allow Reboot = False`

AWS-InstallMissingWindowsUpdates

Sostituito da `AWS-InstallWindowsUpdates`, che è in grado di eseguire le stesse operazioni. Non disponibile in nessun Regioni AWS lancio successivo ad aprile 2017.

Per ottenere lo stesso risultato del documento SSM legacy, utilizza la seguente configurazione dei parametri con il documento sostitutivo consigliato, `AWS-InstallWindowsUpdates`:

- `Action = Install`
- `Allow Reboot = True`

AWS-InstallSpecificWindowsUpdates

Sostituito da `AWS-InstallWindowsUpdates`, che è in grado di eseguire le stesse operazioni. Non disponibile in nessun Regioni AWS lancio successivo ad aprile 2017.

Per ottenere lo stesso risultato del documento SSM legacy, utilizza la seguente configurazione dei parametri con il documento sostitutivo consigliato, `AWS-InstallWindowsUpdates`:

- `Action = Install`
- `Allow Reboot = True`

- Include Kbs = *comma-separated list of KB articles*

Limitazioni note dei documenti SSM per l'applicazione di patch ai nodi gestiti

Interruzioni esterne al riavvio

Se il sistema sul nodo avvia un riavvio durante l'installazione della patch (ad esempio, per applicare aggiornamenti al firmware o a funzionalità simili SecureBoot), l'esecuzione del documento di applicazione delle patch potrebbe essere interrotta e contrassegnata come non riuscita anche se le patch sono state installate correttamente. Ciò si verifica perché l'agente SSM non può persistere e riprendere lo stato di esecuzione del documento dopo i riavvii esterni.

Per verificare lo stato di installazione della patch dopo un'esecuzione non riuscita, esegui un'operazione di Scan patching, quindi controlla i dati di conformità delle patch in Patch Manager per valutare lo stato di conformità attuale.

Documento di comando SSM per l'applicazione di patch: **AWS-RunPatchBaseline**

AWS Systems Manager supporta **AWS-RunPatchBaseline**, un documento Systems Manager (documento SSM) per Patch Manager. Questo documento SSM esegue operazioni di applicazione di patch nei nodi gestiti per aggiornamenti correlati alla sicurezza e di altro tipo. Quando il documento viene eseguito, utilizza la baseline delle patch specificata come “predefinita” per un tipo di sistema operativo se non è specificato alcun gruppo di patch. In caso contrario, utilizza la baseline delle patch associata al gruppo di patch. Per informazioni sui gruppi di patch, consulta [Gruppi di patch](#).

È possibile utilizzare il documento **AWS-RunPatchBaseline** per applicare patch ai sistemi operativi e alle applicazioni. (In Windows Server, il supporto delle applicazioni è limitato ai soli aggiornamenti delle applicazioni Microsoft).

Questo documento supporta Linux, macOS, e nodi gestiti Windows Server. Il documento eseguirà le operazioni adeguate per ciascuna piattaforma.

Note

Patch Manager supporta anche il documento SSM legacy **AWS-ApplyPatchBaseline**. Tuttavia, questo documento supporta l'applicazione di patch solo nei nodi gestiti Windows. Ti consigliamo di usare **AWS-RunPatchBaseline** perché supporta l'applicazione di patch nei nodi gestiti Linux macOS, e Windows Server. Per utilizzare il documento SSM Agent è necessaria la versione 2.0.834.0 o successiva. **AWS-RunPatchBaseline**

Windows Server

Sui nodi Windows Server gestiti, il `AWS-RunPatchBaseline` documento scarica e richiama un PowerShell modulo, che a sua volta scarica un'istantanea della baseline della patch che si applica al nodo gestito. Questa snapshot della baseline delle patch contiene un elenco di patch approvate compilate eseguendo una query sulla baseline delle patch su un server Windows Server Update Services (WSUS). Questo elenco viene trasferito all'API di Windows Update, che controlla il download e l'installazione delle patch approvate, in base alle necessità.

Linux

Nei nodi gestiti Linux, il documento `AWS-RunPatchBaseline` consente di richiamare un modulo Python, che a sua volta scarica una snapshot della baseline delle patch valida per il nodo gestito. Questa snapshot della baseline delle patch utilizza le regole e gli elenchi specificati delle patch approvate e bloccate per controllare il programma di gestione dei pacchetti adeguato per ciascun tipo di nodo:

- I nodi gestiti da Amazon Linux 2, Oracle Linux e RHEL 7 utilizzano YUM. Per le operazioni con YUM, Patch Manager richiede Python 2.6 o una versione supportata successiva (da 2.6 a 3.12). Amazon Linux 2023 utilizza DNF. Per le operazioni DNF, Patch Manager richiede una versione supportata di Python 2 o Python 3 (da 2.6 a 3.12).
- I nodi gestiti 8 RHEL utilizzano DNF. Per le operazioni DNF, Patch Manager richiede una versione supportata di Python 2 o Python 3 (da 2.6 a 3.12). (Nessuna versione è installata per impostazione predefinita su RHEL 8. È necessario installare l'una o l'altra manualmente).
- Le istanze Debian Server e Ubuntu Server utilizzano APT. Per le operazioni APT, Patch Manager richiede una versione supportata di Python 3 (da 3.0 a 3.12).

macOS

Nei nodi gestiti macOS, il documento `AWS-RunPatchBaseline` consente di scaricare e richiamare un modulo Python, che a sua volta scarica una snapshot della baseline delle patch valida per il nodo. Successivamente, un sottoprocesso Python richiama AWS Command Line Interface (AWS CLI) sul nodo per recuperare le informazioni di installazione e aggiornamento per i gestori di pacchetti specificati e per attivare il gestore di pacchetti appropriato per ogni pacchetto di aggiornamento.

Ogni istantanea è specifica per un gruppo di patch Account AWS, un sistema operativo e un ID di istantanea. Lo snapshot viene consegnato tramite un URL Amazon Simple Storage Service (Amazon

S3) prefirmato, che scade 24 ore dopo la creazione dello snapshot. Dopo la scadenza dell'URL, tuttavia, se desideri applicare lo stesso contenuto snapshot ad altri nodi gestiti, è possibile generare un nuovo URL Amazon S3 prefirmato fino a 3 giorni dopo la creazione della copia istantanea. Per farlo, utilizzare il comando [get-deployable-patch-snapshot-for-instance](#).

Dopo avere installato tutti gli aggiornamenti approvati e applicabili e dopo avere eseguito il riavvio, le informazioni sulla conformità delle patch vengono generate in un nodo gestito e trasferite a Patch Manager.

Note

Se il parametro `RebootOption` è impostato su `NoReboot` nel documento `AWS-RunPatchBaseline`, il nodo gestito non viene riavviato dopo l'esecuzione di Patch Manager. Per ulteriori informazioni, consulta [Nome parametro: RebootOption](#).

Per informazioni sulla visualizzazione dei dati di conformità delle patch, consulta [Informazioni sulla conformità delle patch](#).

Parametri **AWS-RunPatchBaseline**

`AWS-RunPatchBaseline` supporta sei parametri. Il parametro `Operation` è obbligatorio. I parametri `InstallOverrideList`, `BaselineOverride` e `RebootOption` sono facoltativi. `Snapshot-ID` è tecnicamente facoltativo, ma consigliamo di specificare un valore personalizzato quando si esegue `AWS-RunPatchBaseline` esternamente alla finestra di manutenzione. Patch Manager fornisce il valore automaticamente quando il documento viene eseguito come parte di un'operazione della finestra di manutenzione.

Parameters

- [Nome del parametro: operazione](#)
- [Nome parametro: AssociationId](#)
- [Nome del parametro: Snapshot ID](#)
- [Nome parametro: InstallOverrideList](#)
- [Nome parametro: RebootOption](#)
- [Nome parametro: BaselineOverride](#)
- [Nome parametro: StepTimeoutSeconds](#)

Nome del parametro: operazione

Utilizzo: obbligatorio.

Opzioni: Scan | Install.

Scan

Quando si sceglie l'opzione Scan, AWS-RunPatchBaseline determina lo stato di conformità delle patch del nodo gestito e riferisce queste informazioni a Patch Manager. Scan non richiede l'installazione degli aggiornamenti o il riavvio dei nodi gestiti. L'operazione identifica dove gli aggiornamenti approvati e applicabili al nodo risultano mancanti.

Installa

Quando si sceglie l'opzione Install, AWS-RunPatchBaseline tenta di installare gli aggiornamenti applicabili e approvati che risultano mancanti nel nodo gestito. Le informazioni sulla conformità delle patch generate in un'operazione Install non visualizzano gli aggiornamenti mancanti, ma sono in grado di specificare lo stato di errore degli aggiornamenti se per qualsiasi motivo l'installazione non è andata a buon fine. Ogni volta che viene installato un aggiornamento su un nodo gestito, il nodo viene riavviato per assicurarsi che l'aggiornamento sia installato e attivo. (Eccezione: se il parametro RebootOption è impostato su NoReboot nel documento AWS-RunPatchBaseline, il nodo non viene riavviato dopo l'esecuzione di Patch Manager. Per ulteriori informazioni, consulta [Nome parametro: RebootOption](#).)

Note

Se una patch specificata dalle regole di baseline viene installata prima che Patch Manager aggiorni il nodo gestito, è possibile che il sistema non venga riavviato come previsto. Ciò si verifica quando una patch viene installata manualmente da un utente o installata automaticamente da un altro programma, ad esempio il pacchetto unattended-upgrades su Ubuntu Server.

Nome parametro: **AssociationId**

Utilizzo: facoltativo.

AssociationId è l'ID di un'associazione esistente in State Manager. È utilizzato da Patch Manager per aggiungere i dati di conformità a un'associazione specificata. Tale associazione è correlata a un'operazione di applicazione di patch [configurata in una policy di patch in Quick Setup](#).

 Note

Con `AWS-RunPatchBaseline`, se viene fornito un valore `AssociationId` insieme a una sostituzione della baseline della policy di patch, l'applicazione di patch viene eseguita come un'operazione `PatchPolicy` e il valore `ExecutionType` riportato in `AWS:ComplianceItem` è anche `PatchPolicy`. Se non viene fornito alcun valore `AssociationId`, l'applicazione di patch viene eseguita come un'operazione `Command` e anche il valore `ExecutionType` riportato nel parametro `AWS:ComplianceItem` inviato è `Command`.

Se non disponi già di un'associazione da utilizzare, è possibile crearla eseguendo il comando [create-association](#).

Nome del parametro: **Snapshot ID**

Utilizzo: facoltativo.

Snapshot ID è un ID univoco (GUID) utilizzato da Patch Manager per assicurare che una serie di nodi gestiti a cui vengono applicate le patch in un'unica operazione abbiano la stessa serie di patch approvate. Sebbene il parametro sia definito facoltativo, le nostre best practice consigliate dipendono dal fatto che tu stia eseguendo `AWS-RunPatchBaseline` o meno una finestra di manutenzione, come descritto nella tabella seguente.

Best practice di **AWS-RunPatchBaseline**

Modalità	Best practice	Informazioni
In esecuzione <code>AWS-RunPatchBaseline</code> all'interno di una finestra di manutenzione	Non fornire un ID della snapshot. Patch Manager la fornirà automaticamente.	Quando utilizzi una finestra di manutenzione per eseguire <code>AWS-RunPatchBaseline</code> , non devi fornire l'ID della snapshot generata. In questo scenario, Systems Manager fornisce un valore GUID in base all'ID di esecuzione della finestra di manutenzione. In questo modo, si garantisce che venga utilizzat

Modalità	Best practice	Informazioni
		<p>o un ID corretto per tutte le invocazioni di <code>AWS-RunPatchBaseline</code> in tale finestra di manutenzione.</p> <p>Si noti che se si specifica un valore in questo scenario, la snapshot della baseline delle patch potrebbe non durare per più di 3 giorni. In seguito, verrà generata una nuova snapshot anche se hai specificato lo stesso ID dopo la scadenza della snapshot.</p>

Modalità	Best practice	Informazioni
In esecuzione AWS-RunPatchBaseline al di fuori di una finestra di manutenzione	Generare e specificare un valore GUID personalizzato per l'ID della snapshot.	<p>Se non utilizzi una finestra di manutenzione per eseguire AWS-RunPatchBaseline, ti consigliamo di generare e specificare un ID snapshot univoco per ogni baseline delle patch, soprattutto se stai eseguendo il documento AWS-RunPatchBaseline su più nodi gestiti nella stessa operazione. Se specifichi un ID in questo scenario, Systems Manager genera un altro ID snapshot per ciascun nodo gestito a cui viene inviato il comando. Di conseguenza, potrebbero venire specificate varie serie di patch fra i nodi gestiti.</p> <p>Ad esempio, supponiamo che tu stia eseguendo il AWS-RunPatchBaseline documento direttamente tramite Run Command e indirizzando un gruppo di 50 nodi gestiti. Specificando un ID snapshot personalizzato verrà creata una singola snapshot di baseline utilizzata per valutare le patch e tutti i nodi, per garantire che il relativo stato finale sia coerente.</p>

Modalità	Best practice	Informazioni
----------	---------------	--------------

¹ È possibile utilizzare qualsiasi strumento in grado di generare un GUID per ottenere il valore del parametro ID snapshot. Ad esempio, in PowerShell, è possibile utilizzare il `New-Guid` cmdlet per generare un GUID nel formato di. 12345699-9405-4f69-bc5e-9315aEXAMPLE

Nome parametro: **InstallOverrideList**

Utilizzo: facoltativo.

`InstallOverrideList` consente di specificare un URL `https` o un URL in stile percorso Amazon S3 per un elenco delle patch da installare. Questo elenco di installazione delle patch, gestito in formato YAML, sostituisce le patch specificate dalla baseline delle patch predefinita corrente. Ciò offre un controllo più granulare sulle patch installate nei nodi gestiti.

Important

Il nome del file `InstallOverrideList` non consente la presenza dei seguenti caratteri: backtick (`), virgolette singole ('), virgolette doppie (") e simbolo del dollaro (\$).

Il comportamento dell'applicazione di patch quando si utilizza il parametro `InstallOverrideList`, differisce tra nodi gestiti da Linux e macOS o da Windows Server. Su Linux e macOS, Patch Manager tenta di applicare le patch incluse nell'elenco `InstallOverrideList` delle patch presenti in qualsiasi repository abilitato sul nodo, indipendentemente dal fatto che corrispondano o meno alle regole della baseline delle patch. Sui nodi di Windows Server, tuttavia, le patch nell'elenco `InstallOverrideList` vengono applicate solo quando corrispondono anche alle regole della baseline delle patch.

Su Linux e sui nodi macOS gestiti, le patch specificate in `InstallOverrideList` vengono applicate solo come aggiornamenti ai pacchetti già installati sul nodo. Se `InstallOverrideList` include patch per pacchetti che non sono attualmente installati sul nodo, tali patch non vengono installate.

I report di conformità rispecchiano gli stati delle patch in base a quanto specificato nella baseline delle patch, non ciò che hai specificato in un elenco `InstallOverrideList` di patch. In altre parole, le operazioni di scansione ignorano il parametro `InstallOverrideList`. Questo serve a garantire

che i report di conformità riflettano in modo coerente lo stato delle patch in base alla policy e non a ciò che è stato approvato per una specifica operazione di patching.

Note

Quando applichi una patch a un nodo che utilizza solo IPv6, assicurati che l'URL fornito sia raggiungibile dal nodo. Se l'opzione di SSM Agent configurazione `UseDualStackEndpoint` è impostata su `true`, quando viene fornito un URL S3 viene utilizzato un client S3 dualstack. [the section called “Tutorial: applicare patch a un server in un ambiente solo IPv6”](#) Per ulteriori informazioni sulla configurazione dell'agente per l'utilizzo del dualstack, vedere.

Per una descrizione di come è possibile utilizzare il parametro `InstallOverrideList` per applicare diversi tipi di patch a un gruppo di destinazione in diverse pianificazioni delle finestre di manutenzione, pur utilizzando una singola baseline delle patch, consulta [Scenario di esempio per l'utilizzo del InstallOverrideList parametro in AWS-RunPatchBaseline o AWS-RunPatchBaselineAssociation](#).

Formati URL validi

Note

Se il file è archiviato in un bucket pubblicamente disponibile, è possibile inoltre specificare un formato URL `https` o un URL in stile percorso Amazon S3. Se il file è archiviato in un bucket privato, è necessario specificare un URL in stile percorso Amazon S3.

- formato URL `https`:

```
https://s3.aws-api-domain/amzn-s3-demo-bucket/my-windows-override-list.yaml
```

- URL in stile percorso Amazon S3:

```
s3://amzn-s3-demo-bucket/my-windows-override-list.yaml
```

Formati dei contenuti YAML validi

I formati utilizzati per specificare le patch nell'elenco variano in base al sistema operativo del tuo nodo gestito. Il formato generale, tuttavia, è quello riportato di seguito:

```
patches:
  -
    id: '{patch-d}'
    title: '{patch-title}'
    {additional-fields}:{values}
```

Benché sia possibile specificare altri campi nel file YAML, questi verranno ignorati durante le operazioni delle patch.

Inoltre, è consigliabile verificare che il formato del file YAML sia valido prima di aggiungere o aggiornare l'elenco nel bucket S3. Per ulteriori informazioni sul formato YAML, consulta yaml.org. Per le opzioni degli strumento di convalida, effettua la ricerca sul Web di “convalida formato yaml”.

Linux

id

Il campo id è obbligatorio. Utilizzalo per specificare le patch con l'architettura e il nome del pacchetto. Ad esempio: 'dhclient.x86_64'. Negli id, è possibile utilizzare i caratteri jolly per indicare più pacchetti. Ad esempio: 'dhcp*' ed 'dhcp*1.*'.

Titolo

Il campo titolo è facoltativo, ma nei sistemi Linux offre funzionalità di filtraggio aggiuntive. Quando utilizzi titolo, è necessario che il campo includa le informazioni sulla versione del pacchetto in uno dei seguenti formati:

YUM/SUSE Linux Enterprise Server (SLES):

```
{name}.{architecture}:{epoch}:{version}-{release}
```

APT

```
{name}.{architecture}:{version}
```

Per i titoli delle patch di Linux, è possibile utilizzare uno o più caratteri jolly in qualsiasi posizione per ampliare il numero di corrispondenze dei pacchetti. Ad esempio:

```
'*32:9.8.2-0.*.rc1.57.amzn1'
```

Ad esempio:

- Il pacchetto apt versione 1.2.25 è correntemente installato nel nodo gestito, ma ora è disponibile la versione 1.2.27.
- È possibile aggiungere apt.amd64 versione 1.2.27 all'elenco delle patch. Dipende da apt-utils.amd64 versione 1.2.27, ma apt-utils.amd64 versione 1.2.25 viene specificato nell'elenco.

In questo caso, la versione 1.2.27 di apt verrà bloccata dall'installazione e segnalata come «.»
Failed-NonCompliant

Windows Server

id

Il campo id è obbligatorio. Utilizzatelo per specificare le patch utilizzando gli ID della Microsoft Knowledge Base (ad esempio, KB2736693) e gli ID del Microsoft Security Bulletin (ad esempio, MS17-023).

Tutti gli altri campi che intendi fornire in un elenco di patch per Windows sono facoltativi e hanno unicamente scopo informativo. È possibile utilizzare altri campi, come title, classification, severity o qualsiasi altro per fornire informazioni più dettagliate sulle patch specificate.

macOS

id

Il campo id è obbligatorio. Il valore per il campo id viene fornito utilizzando un formato {package-name}. {package-version} o un formato {package_name}.

Elenchi di patch di esempio

- Amazon Linux 2

```
patches:
  -
    id: 'kernel.x86_64'
  -
    id: 'bind*.x86_64'
    title: '39.11.4-26.P2.amzn2.5.2'

    id: 'glibc*
```

```
-
  id: 'dhclient*'
  title: '*4.2.5-58.amzn2'
-
  id: 'dhcp*'
  title: '*4.2.5-77.amzn2'
```

- Debian Server

patches:

```
-
  id: 'apparmor.amd64'
  title: '2.10.95-0ubuntu2.9'
-
  id: 'cryptsetup.amd64'
  title: '*2:1.6.6-5ubuntu2.1'
-
  id: 'cryptsetup-bin.*'
  title: '*2:1.6.6-5ubuntu2.1'
-
  id: 'apt.amd64'
  title: '*1.2.27'
-
  id: 'apt-utils.amd64'
  title: '*1.2.25'
```

- macOS

patches:

```
-
  id: 'XProtectPlistConfigData'
-
  id: 'MRTConfigData.1.61'
-
  id: 'Command Line Tools for Xcode.11.5'
-
  id: 'Gatekeeper Configuration Data'
```

- Oracle Linux

patches:

```
-
  id: 'audit-libs.x86_64'
```

```

    title: '*2.8.5-4.el7'
  -
    id: 'curl.x86_64'
    title: '*.el7'
  -
    id: 'grub2.x86_64'
    title: 'grub2.x86_64:1:2.02-0.81.0.1.el7'
  -
    id: 'grub2.x86_64'
    title: 'grub2.x86_64:1:*-0.81.0.1.el7'

```

- Red Hat Enterprise Linux (RHEL)

patches:

```

  -
    id: 'NetworkManager.x86_64'
    title: '*1:1.10.2-14.el7_5'
  -
    id: 'NetworkManager-*.x86_64'
    title: '*1:1.10.2-14.el7_5'
  -
    id: 'audit.x86_64'
    title: '*0:2.8.1-3.el7'
  -
    id: 'dhclient.x86_64'
    title: '*.el7_5.1'
  -
    id: 'dhcp*.x86_64'
    title: '*12:5.2.5-68.el7'

```

- SUSE Linux Enterprise Server (SLES)

patches:

```

  -
    id: 'amazon-ssm-agent.x86_64'
  -
    id: 'binutils'
    title: '*0:2.26.1-9.12.1'
  -
    id: 'glibc*.x86_64'
    title: '*2.19*'
  -
    id: 'dhcp*'

```

```
    title: '0:4.3.3-9.1'
  -
    id: 'lib*'
```

- Ubuntu Server

```
patches:
  -
    id: 'apparmor.amd64'
    title: '2.10.95-0ubuntu2.9'
  -
    id: 'cryptsetup.amd64'
    title: '*2:1.6.6-5ubuntu2.1'
  -
    id: 'cryptsetup-bin.*'
    title: '*2:1.6.6-5ubuntu2.1'
  -
    id: 'apt.amd64'
    title: '*1.2.27'
  -
    id: 'apt-utils.amd64'
    title: '*1.2.25'
```

- Windows

```
patches:
  -
    id: 'KB4284819'
    title: '2018-06 Cumulative Update for Windows Server 2016 (1709) for x64-
based Systems (KB4284819)'
  -
    id: 'KB4284833'
  -
    id: 'KB4284835'
    title: '2018-06 Cumulative Update for Windows Server 2016 (1803) for x64-
based Systems (KB4284835)'
  -
    id: 'KB4284880'
  -
    id: 'KB4338814'
```

Nome parametro: **RebootOption**

Utilizzo: facoltativo.

Opzioni: `RebootIfNeeded` | `NoReboot`

Default: `RebootIfNeeded`

Warning

L'opzione predefinita è `RebootIfNeeded`. Assicurarsi di selezionare l'opzione corretta per il caso d'uso. Ad esempio, quando è necessario che i nodi gestiti vengano riavviati immediatamente per completare un processo di configurazione, scegli `RebootIfNeeded`. Oppure, quando è necessario mantenere la disponibilità dei nodi gestiti fino a un orario di riavvio pianificato, scegli `NoReboot`.

Important

Non è consigliabile utilizzarlo Patch Manager per applicare patch alle istanze di cluster in Amazon EMR (precedentemente chiamato Amazon Elastic). MapReduce In particolare, non selezionare l'opzione `RebootIfNeeded` per il parametro `RebootOption`. (Questa opzione è disponibile nei documenti del comando SSM per l'applicazione di patch `AWS-RunPatchBaseline`, `AWS-RunPatchBaselineAssociation` e `AWS-RunPatchBaselineWithHooks`).

I comandi sottostanti per applicare le patch tramite Patch Manager utilizzano i comandi `yum` e `dnf`. Pertanto, le operazioni generano incompatibilità a causa del modo in cui i pacchetti vengono installati. Per informazioni sui metodi preferiti per l'aggiornamento del software sui cluster Amazon EMR, consulta [Utilizzo dell'AMI predefinita per Amazon EMR](#) nella Guida per la gestione di Amazon EMR.

RebootIfNeeded

Quando si sceglie l'opzione `RebootIfNeeded`, il nodo gestito viene riavviato in uno dei seguenti casi:

- Patch Manager installato uno o più patch.

Patch Manager non valuta se un riavvio è obbligatorio per la patch. Il sistema viene riavviato anche se la patch non richiede il riavvio.

- Patch Manager rileva una o più patch con lo stato di `INSTALLED_PENDING_REBOOT` durante l'operazione `Install`.

Lo stato `INSTALLED_PENDING_REBOOT` indica che l'opzione `NoReboot` è stata selezionata l'ultima volta che l'operazione `Install` è stata eseguita, o che una patch è stata installata all'esterno di Patch Manager dall'ultimo riavvio del nodo gestito.

Il riavvio dei nodi gestiti in questi due casi garantisce che i pacchetti aggiornati vengano svuotati dalla memoria e mantengano coerenti il comportamento di patch e di riavvio in tutti i sistemi operativi.

NoReboot

Quando scegli l'opzione `NoReboot`, Patch Manager non riavvia il nodo gestito anche se ha installato patch durante l'operazione di `Install`. Questa opzione è utile se i nodi gestiti non richiedono il riavvio dopo l'applicazione di patch, oppure nel caso di applicazioni o processi in esecuzione su un nodo che non dovrebbero essere interrotti da un riavvio a seguito di un'operazione di applicazione di patch. È utile anche quando si necessita di un maggiore controllo sui tempi dei riavvii del nodo gestito, ad esempio utilizzando una finestra di manutenzione.

Quando si sceglie l'opzione `NoReboot` e viene installata una patch, alla patch viene assegnato lo stato `InstalledPendingReboot`. Il nodo gestito stesso, tuttavia, viene contrassegnato come `Non-Compliant`. Dopo che si verifica un riavvio e viene eseguita un'operazione `Scan`, lo stato del nodo gestito diventa `Compliant`.

Important

L'opzione `NoReboot` impedisce solo i riavvii a livello di sistema operativo. Service-level i riavvii possono ancora avvenire come parte del processo di applicazione delle patch. Ad esempio, quando Docker viene aggiornato, i servizi dipendenti come Amazon Elastic Container Service potrebbero riavviarsi automaticamente, anche con `NoReboot` abilitato. Se disponi di servizi critici, che non devono essere interrotti, prendi in considerazione misure aggiuntive come la rimozione temporanea delle istanze dal servizio o la pianificazione dell'applicazione di patch durante le finestre di manutenzione.

File di monitoraggio dell'installazione delle patch: per tenere traccia dell'installazione delle patch, in particolare delle patch installate dopo l'ultimo riavvio del sistema, Systems Manager mantiene un file nel nodo gestito.

 Important

Non eliminare o modificare il file di monitoraggio. Se questo file viene eliminato o danneggiato, il rapporto di conformità della patch per il nodo gestito non è accurato. In questo caso, riavvia il nodo ed esegui un'operazione di scansione della patch per ripristinare il file.

Questo file di monitoraggio viene archiviato nei seguenti percorsi nei nodi gestiti:

- Sistemi operativi Linux:
 - `/var/log/amazon/ssm/patch-configuration/patch-states-configuration.json`
 - `/var/log/amazon/ssm/patch-configuration/patch-inventory-from-last-operation.json`
- Windows Server sistema operativo:
 - `C:\ProgramData\Amazon\PatchBaselineOperations\State\PatchStatesConfiguration.json`
 - `C:\ProgramData\Amazon\PatchBaselineOperations\State\PatchInventoryFromLastOperation.json`

Nome parametro: **BaselineOverride**

Utilizzo: facoltativo.

È possibile definire le preferenze per l'applicazione di patch in runtime (tempo di esecuzione) utilizzando il parametro **BaselineOverride**. Questa sostituzione della baseline viene mantenuta come oggetto JSON in un bucket S3. Garantisce che le operazioni di applicazione di patch utilizzino le baseline fornite che corrispondono al sistema operativo host anziché applicare le norme dalla baseline delle patch predefinita

 Important

Il nome del file **BaselineOverride** non consente la presenza dei seguenti caratteri: backtick (`), virgolette singole ('), virgolette doppie (") e simbolo del dollaro (\$).

Per ulteriori informazioni su come utilizzare il parametro `BaselineOverride`, consulta [Utilizzo del `BaselineOverride` parametro](#).

Nome parametro: **StepTimeoutSeconds**

Utilizzo: facoltativo.

Il tempo in secondi, compreso tra 1 e 36.000 secondi (10 ore), entro cui un comando deve essere eseguito, prima che venga considerato non riuscito.

Documento di comando SSM per l'applicazione di patch: **AWS-RunPatchBaselineAssociation**

Come il documento `AWS-RunPatchBaseline`, `AWS-RunPatchBaselineAssociation` esegue operazioni di applicazione di patch sulle istanze per aggiornamenti correlati alla sicurezza e di altro tipo. È possibile utilizzare il documento `AWS-RunPatchBaselineAssociation` per applicare patch ai sistemi operativi e alle applicazioni. (In Windows Server, il supporto delle applicazioni è limitato ai soli aggiornamenti delle applicazioni Microsoft).

Questo documento supporta le istanze Amazon Elastic Compute Cloud (Amazon EC2) per Linux, macOS, e Windows Server. Non supporta nodi non EC2 in un ambiente [ibrido e multicloud](#). Il documento eseguirà le azioni appropriate per ciascuna piattaforma, richiamando un modulo Python su Linux e macOS istanze e un PowerShell modulo su istanze Windows.

`AWS-RunPatchBaselineAssociation`, tuttavia, differisce da `AWS-RunPatchBaseline` nei seguenti modi:

- `AWS-RunPatchBaselineAssociation` è destinato all'uso principalmente con associazioni State Manager create utilizzando [Quick Setup](#), uno strumento di AWS Systems Manager. In particolare, quando utilizzi il tipo di configurazione di gestione host Quick Setup, scegliendo l'opzione Scan instances for missing patches daily (Scansiona le istanze per le patch mancanti ogni giorno), il sistema utilizza `AWS-RunPatchBaselineAssociation` per l'operazione.

Di solito, tuttavia, quando si impostano le proprie operazioni di patching, è necessario scegliere o invece di. [AWS-RunPatchBaseline](#) [AWS-RunPatchBaselineWithHooks](#) `AWS-RunPatchBaselineAssociation`

- Quando utilizzi il documento `AWS-RunPatchBaselineAssociation`, è possibile specificare una coppia di chiavi di tag nel campo parametro `BaselineTags` del documento. Se una baseline di patch personalizzata in uso Account AWS condivide questi tag, Patch Manager utilizza tale baseline quando viene eseguita sulle istanze di destinazione anziché la baseline di patch «predefinita» attualmente specificata per il tipo di sistema operativo.

 Note

Quando si sceglie di utilizzare `AWS-RunPatchBaselineAssociation` nelle operazioni di applicazione di patch diverse da quelle configurate con Quick Setup, e si desidera utilizzare il suo parametro `BaselineTags` opzionale, è necessario fornire alcune autorizzazioni aggiuntive al [profilo dell'istanza](#) per istanze Amazon Elastic Compute Cloud (Amazon EC2). Per ulteriori informazioni, consulta [Nome parametro: BaselineTags](#).

Entrambi i formati seguenti sono validi per il parametro `BaselineTags`:

Key=*tag-key*,Values=*tag-value*

Key=*tag-key*,Values=*tag-value1*,*tag-value2*,*tag-value3*

 Important

Le chiavi e i valori dei tag non consentono la presenza dei seguenti caratteri: backtick (`), virgolette singole ('), virgolette doppie (") e simbolo del dollaro (\$).

- Quando viene eseguito `AWS-RunPatchBaselineAssociation`, i dati di conformità delle patch raccolti vengono registrati utilizzando il comando API di `PutComplianceItems` al posto del comando `PutInventory`, che viene utilizzato da `AWS-RunPatchBaseline`. Questa differenza indica che le informazioni sulla conformità delle patch che vengono archiviate e segnalate per una specifica associazione. I dati di conformità delle patch generati al di fuori di questa associazione non vengono sovrascritti.
- Le informazioni sulla conformità della patch riportate dopo l'esecuzione `AWS-RunPatchBaselineAssociation` indicano se un'istanza è conforme. Non include dettagli a livello di patch, come dimostrato dall'output del comando following AWS Command Line Interface (AWS CLI). Il comando filtra su `Association` come tipo di conformità:

```
aws ssm list-compliance-items \
  --resource-ids "i-02573cafcfEXAMPLE" \
  --resource-types "ManagedInstance" \
  --filters "Key=ComplianceType,Values=Association,Type=EQUAL" \
  --region us-east-2
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "ComplianceItems": [
    {
      "Status": "NON_COMPLIANT",
      "Severity": "UNSPECIFIED",
      "Title": "MyPatchAssociation",
      "ResourceType": "ManagedInstance",
      "ResourceId": "i-02573cafcfEXAMPLE",
      "ComplianceType": "Association",
      "Details": {
        "DocumentName": "AWS-RunPatchBaselineAssociation",
        "PatchBaselineId": "pb-0c10e65780EXAMPLE",
        "DocumentVersion": "1"
      },
      "ExecutionSummary": {
        "ExecutionTime": 1590698771.0
      },
      "Id": "3e5d5694-cd07-40f0-bbea-040e6EXAMPLE"
    }
  ]
}
```

Quando un valore di una coppia di chiavi di tag è stato specificato come parametro per il documento `AWS-RunPatchBaselineAssociation`, Patch Manager cerca una baseline delle patch personalizzata che corrisponda al tipo di sistema operativo ed è stata contrassegnata con la stessa coppia di chiavi di tag. Questa ricerca non è limitata alla baseline delle patch predefinita corrente specificata o alla base assegnata a un gruppo di patch. Quando non viene trovata alcuna baseline con i tag specificati, Patch Manager cerca un gruppo di patch, se ne è stato specificato uno nel comando che esegue `AWS-RunPatchBaselineAssociation`. Quando nessun gruppo di patch viene abbinato, Patch Manager torna alla baseline delle patch predefinita corrente per l'account del sistema operativo.

Se viene trovata più di una baseline della patch con i tag specificati nel `AWS-RunPatchBaselineAssociation` documento, Patch Manager restituisce un messaggio di errore che indica che solo una baseline della patch può essere contrassegnata con quella coppia chiave-valore affinché l'operazione proceda.

 Note

Sui nodi Linux, il gestore di pacchetti idonei per ogni tipo di nodo viene utilizzato per installare i pacchetti:

- Amazon Linux 2, Oracle Linux e le istanze RHEL utilizzano YUM. Per le operazioni con YUM, Patch Manager richiede Python 2.6 o una versione supportata successiva (da 2.6 a 3.12). Amazon Linux 2023 utilizza DNF. Per le operazioni DNF, Patch Manager richiede una versione supportata di Python 2 o Python 3 (da 2.6 a 3.12).
- Le istanze Debian Server e Ubuntu Server utilizzano APT. Per le operazioni APT, Patch Manager richiede una versione supportata di Python 3 (da 3.0 a 3.12).

Al termine di una scansione, o dopo che tutti gli aggiornamenti approvati e applicabili sono stati installati, con eventuali riavvii eseguiti, le informazioni sulla conformità delle patch sono generate su un'istanza e riportate al servizio Patch Compliance.

 Note

Quando il parametro `RebootOption` è impostato su `NoReboot` nel documento `AWS-RunPatchBaselineAssociation`, l'istanza non viene riavviata dopo l'esecuzione di Patch Manager. Per ulteriori informazioni, consulta [Nome parametro: RebootOption](#).

Per informazioni sulla visualizzazione dei dati di conformità delle patch, consulta [Informazioni sulla conformità delle patch](#).

Parametri **AWS-RunPatchBaselineAssociation**

AWS-RunPatchBaselineAssociation supporta cinque parametri. I parametri `Operation` e `AssociationId` sono obbligatori. I parametri `InstallOverrideList`, `RebootOption` e `BaselineTags` sono facoltativi.

Parameters

- [Nome del parametro: Operazione](#)
- [Nome parametro: BaselineTags](#)
- [Nome parametro: AssociationId](#)
- [Nome parametro: InstallOverrideList](#)

- [Nome parametro: RebootOption](#)

Nome del parametro: Operazione

Utilizzo: obbligatorio.

Opzioni: Scan | Install.

Scan

Quando si sceglie l'opzione Scan, AWS-RunPatchBaselineAssociation determina lo stato di conformità delle patch dell'istanza e riferisce queste informazioni a Patch Manager. Scan non richiede l'installazione degli aggiornamenti o il riavvio delle istanze. L'operazione identifica dove gli aggiornamenti approvati e applicabili all'istanza risultano mancanti.

Installa

Quando si sceglie l'opzione Install, AWS-RunPatchBaselineAssociation tenta di installare gli aggiornamenti applicabili e approvati che risultano mancanti nell'istanza. Le informazioni sulla conformità delle patch generate in un'operazione Install non visualizzano gli aggiornamenti mancanti, ma possono specificare lo stato di errore degli aggiornamenti se per qualsiasi motivo l'installazione non è andata a buon fine. Ogni volta che viene installato un aggiornamento su un'istanza, l'istanza viene riavviata per assicurarsi che l'aggiornamento sia installato e attivo. (Eccezione: se il parametro RebootOption è impostato su NoReboot nel documento AWS-RunPatchBaselineAssociation, l'istanza non viene riavviata dopo l'esecuzione di Patch Manager. Per ulteriori informazioni, consulta [Nome parametro: RebootOption](#)).

Note

Se una patch specificata dalle regole di baseline viene installata prima Patch Manager dell'aggiornamento dell'istanza di Gestione patch, è possibile che il sistema non venga riavviato come previsto. Ciò si verifica quando una patch viene installata manualmente da un utente o installata automaticamente da un altro programma, ad esempio il pacchetto unattended-upgrades su Ubuntu Server.

Nome parametro: **BaselineTags**

Utilizzo: facoltativo.

BaselineTags è un un key value di tag univoco, scelto e assegnato a una baseline delle patch personalizzata. È possibile specificare uno o più valori per questo parametro. Sono validi entrambi dei seguenti formati:

Key=*tag-key*, Values=*tag-value*

Key=*tag-key*, Values=*tag-value1*, *tag-value2*, *tag-value3*

 Important

Le chiavi e i valori dei tag non consentono la presenza dei seguenti caratteri: backtick (`), virgolette singole ('), virgolette doppie (") e simbolo del dollaro (\$).

Il BaselineTags valore viene utilizzato da Patch Manager per assicurarsi che un set di istanze a cui è stata applicata una patch in una singola operazione abbiano tutte lo stesso identico set di patch approvate. Quando viene eseguita l'operazione di patch, Patch Manager controlla se una baseline delle patch per il tipo di sistema operativo è contrassegnata con la stessa coppia di key value per BaselineTags. Se c'è una corrispondenza, viene utilizzata questa baseline delle patch personalizzata. Se non esiste una corrispondenza, una baseline delle patch viene identificata in base a qualsiasi gruppo di patch specificato per l'operazione di applicazione di patch. Se non ce ne sono, viene utilizzata la baseline di patch predefinita AWS gestita per quel sistema operativo.

Requisiti di permesso aggiuntivi

Se utilizzi AWS-RunPatchBaselineAssociation nelle operazioni di applicazione di patch diverse da quelle configurate utilizzando Quick Setup, e desideri utilizzare l'opzione opzionale BaselineTags, è necessario aggiungere le seguenti autorizzazioni al [profilo dell'istanza](#) per istanze Amazon Elastic Compute Cloud (Amazon EC2).

 Note

Quick Setup e AWS-RunPatchBaselineAssociation non supportano server on-premises e macchine virtuali (VM) locali.

```
{  
  "Effect": "Allow",
```

```

    "Action": [
        "ssm:DescribePatchBaselines",
        "tag:GetResources"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ssm:GetPatchBaseline",
        "ssm:DescribeEffectivePatchesForPatchBaseline"
    ],
    "Resource": "patch-baseline-arn"
}

```

Sostituisci *patch-baseline-arn* con Amazon Resource Name (ARN) della baseline della patch a cui desideri fornire l'accesso, nel formato. `arn:aws:ssm:us-east-2:123456789012:patchbaseline/pb-0c10e65780EXAMPLE`

Nome parametro: **AssociationId**

Utilizzo: obbligatorio.

AssociationId è l'ID di un'associazione esistente in State Manager. È usato da Patch Manager per aggiungere i dati di conformità a un'associazione specificata. Questa associazione è correlata a un'operazione Scan di patch abilitata in una [configurazione di gestione host creata in Quick Setup](#). Inviando i risultati dell'applicazione di patch come dati di conformità dell'associazione anziché dati di conformità dell'inventario, le informazioni di conformità dell'inventario esistenti per le istanze non vengono sovrascritte dopo un'operazione di applicazione di patch né per altri ID di associazione. Se non disponi già di un'associazione da utilizzare, è possibile crearla eseguendo il comando [create-association](#). Ad esempio:

Linux & macOS

```

aws ssm create-association \
    --name "AWS-RunPatchBaselineAssociation" \
    --association-name "MyPatchHostConfigAssociation" \
    --targets
    "Key=instanceids,Values=[i-02573cafcfEXAMPLE,i-07782c72faEXAMPLE,i-07782c72faEXAMPLE]" \
    --parameters "Operation=Scan" \
    --schedule-expression "cron(0 */30 * * * ? *)" \

```

```
--sync-compliance "MANUAL" \  
--region us-east-2
```

Windows Server

```
aws ssm create-association ^  
  --name "AWS-RunPatchBaselineAssociation" ^  
  --association-name "MyPatchHostConfigAssociation" ^  
  --targets  
  "Key=instanceids,Values=[i-02573cafcfEXAMPLE,i-07782c72faEXAMPLE,i-07782c72faEXAMPLE]"  
  ^  
  --parameters "Operation=Scan" ^  
  --schedule-expression "cron(0 */30 * * * ? *)" ^  
  --sync-compliance "MANUAL" ^  
  --region us-east-2
```

Nome parametro: **InstallOverrideList**

Utilizzo: facoltativo.

Utilizzando `InstallOverrideList`, è possibile specificare un URL https o un URL in stile percorso Amazon Simple Storage Service (Amazon S3) per un elenco delle patch da installare. Questo elenco di installazione delle patch, gestito in formato YAML, sostituisce le patch specificate dalla baseline delle patch predefinita corrente. Ciò consente di avere un controllo più granulare su quali patch vengono installate nelle istanze.

Important

Il nome del file `InstallOverrideList` non consente la presenza dei seguenti caratteri: backtick (`), virgolette singole ('), virgolette doppie (") e simbolo del dollaro (\$).

Il comportamento dell'applicazione di patch quando si utilizza il parametro `InstallOverrideList`, differisce tra nodi gestiti da Linux e macOS o da Windows Server. Su Linux e macOS, Patch Manager tenta di applicare le patch incluse nell'elenco `InstallOverrideList` delle patch presenti in qualsiasi repository abilitato sul nodo, indipendentemente dal fatto che corrispondano o meno alle regole della baseline delle patch. Sui nodi di Windows Server, tuttavia, le patch nell'elenco `InstallOverrideList` vengono applicate solo quando corrispondono anche alle regole della baseline delle patch.

Su Linux e sui nodi macOS gestiti, le patch specificate in `InstallOverrideList` vengono applicate solo come aggiornamenti ai pacchetti già installati sul nodo. Se `InstallOverrideList` include patch per pacchetti che non sono attualmente installati sul nodo, tali patch non vengono installate.

I report di conformità rispecchiano gli stati delle patch in base a quanto specificato nella baseline delle patch, non ciò che hai specificato in un elenco `InstallOverrideList` di patch. In altre parole, le operazioni di scansione ignorano il parametro `InstallOverrideList`. Questo serve a garantire che i report di conformità riflettano in modo coerente lo stato delle patch in base alla policy e non a ciò che è stato approvato per una specifica operazione di patching.

Formati URL validi

Note

Se il file è archiviato in un bucket pubblicamente disponibile, è possibile inoltre specificare un formato URL `https` o un URL in stile percorso Amazon S3. Se il file è archiviato in un bucket privato, è necessario specificare un URL in stile percorso Amazon S3.

- Esempio di formato URL `https`:

```
https://s3.amazonaws.com/amzn-s3-demo-bucket/my-windows-override-list.yaml
```

- Esempio di URL in stile percorso Amazon S3:

```
s3://amzn-s3-demo-bucket/my-windows-override-list.yaml
```

Formati dei contenuti YAML validi

I formati utilizzati per specificare le patch nell'elenco variano in base al sistema operativo dell'istanza. Il formato generale, tuttavia, è quello riportato di seguito:

```
patches:
  -
    id: '{patch-d}'
    title: '{patch-title}'
    {additional-fields}:{values}
```

Benché sia possibile specificare altri campi nel file YAML, questi verranno ignorati durante le operazioni delle patch.

Inoltre, è consigliabile verificare che il formato del file YAML sia valido prima di aggiungere o aggiornare l'elenco nel bucket S3. Per ulteriori informazioni sul formato YAML, consulta yaml.org. Per le opzioni degli strumento di convalida, effettua la ricerca sul Web di “convalida formato yaml”.

- Microsoft Windows

id

Il campo id è obbligatorio. Utilizzalo per specificare le patch utilizzando gli ID della Microsoft Knowledge Base (ad esempio, KB2736693) e gli ID del Microsoft Security Bulletin (ad esempio, MS17-023).

Tutti gli altri campi che intendi fornire in un elenco di patch per Windows sono facoltativi e hanno unicamente scopo informativo. È possibile utilizzare altri campi, come title, classification, severity o qualsiasi altro per fornire informazioni più dettagliate sulle patch specificate.

- Linux

id

Il campo id è obbligatorio. Utilizzalo per specificare le patch con l'architettura e il nome del pacchetto. Ad esempio: 'dhclient.x86_64'. Negli id, è possibile utilizzare i caratteri jolly per indicare più pacchetti. Ad esempio: 'dhcp*' ed 'dhcp*1.*'.

titolo

Il campo titolo è facoltativo, ma nei sistemi Linux offre funzionalità di filtraggio aggiuntive. Quando utilizzi titolo, è necessario che il campo includa le informazioni sulla versione del pacchetto in uno dei seguenti formati:

YUM/Red Hat Enterprise Linux (RHEL):

```
{name}.{architecture}:{epoch}:{version}-{release}
```

APT

```
{name}.{architecture}:{version}
```

Per i titoli delle patch di Linux, è possibile utilizzare uno o più caratteri jolly in qualsiasi posizione per ampliare il numero di corrispondenze dei pacchetti. Ad esempio:

```
'*32:9.8.2-0.*.rc1.57.amzn1'
```

Ad esempio:

- Il pacchetto apt versione 1.2.25 è correntemente installato nell'istanza, ma ora è disponibile la versione 1.2.27.
- È possibile aggiungere apt.amd64 versione 1.2.27 all'elenco delle patch. Dipende da apt-utils.amd64 versione 1.2.27, ma apt-utils.amd64 versione 1.2.25 viene specificato nell'elenco.

In questo caso, la versione 1.2.27 di apt verrà bloccata dall'installazione e segnalata come «.» Failed-NonCompliant

Altri campi

Tutti gli altri campi che intendi fornire in un elenco di patch per Linux sono facoltativi e hanno unicamente scopo informativo. È possibile utilizzare altri campi, come classification, severity o qualsiasi altro per fornire informazioni più dettagliate sulle patch specificate.

Elenchi di patch di esempio

- Windows

```
patches:
-
  id: 'KB4284819'
  title: '2018-06 Cumulative Update for Windows Server 2016 (1709) for x64-based Systems (KB4284819)'
-
  id: 'KB4284833'
-
  id: 'KB4284835'
  title: '2018-06 Cumulative Update for Windows Server 2016 (1803) for x64-based Systems (KB4284835)'
-
  id: 'KB4284880'
-
  id: 'KB4338814'
```

- APT

```
patches:
-
  id: 'apparmor.amd64'
  title: '2.10.95-0ubuntu2.9'
-
  id: 'cryptsetup.amd64'
  title: '*2:1.6.6-5ubuntu2.1'
-
  id: 'cryptsetup-bin.*'
  title: '*2:1.6.6-5ubuntu2.1'
-
  id: 'apt.amd64'
  title: '*1.2.27'
-
  id: 'apt-utils.amd64'
  title: '*1.2.25'
```

- Amazon Linux 2

```
patches:
-
  id: 'kernel.x86_64'
-
  id: 'bind*.x86_64'
  title: '39.11.4-26.P2.amzn2.5.2'
  id: 'glibc*'
-
  id: 'dhclient*'
  title: '*4.2.5-58.amzn2'
-
  id: 'dhcp*'
  title: '*4.2.5-77.amzn2'
```

- Red Hat Enterprise Linux (RHEL)

```
patches:
-
  id: 'NetworkManager.x86_64'
  title: '*1:1.10.2-14.el7_5'
-
  id: 'NetworkManager-*.x86_64'
```

```

    title: '*1:1.10.2-14.el7_5'
  -
    id: 'audit.x86_64'
    title: '*0:2.8.1-3.el7'
  -
    id: 'dhclient.x86_64'
    title: '*.el7_5.1'
  -
    id: 'dhcp*.x86_64'
    title: '*12:5.2.5-68.el7'

```

- SUSE Linux Enterprise Server (SLES)

patches:

```

  -
    id: 'amazon-ssm-agent.x86_64'
  -
    id: 'binutils'
    title: '*0:2.26.1-9.12.1'
  -
    id: 'glibc*.x86_64'
    title: '*2.19*'
  -
    id: 'dhcp*'
    title: '*0:4.3.3-9.1'
  -
    id: 'lib*'

```

- Ubuntu Server

patches:

```

  -
    id: 'apparmor.amd64'
    title: '2.10.95-0ubuntu2.9'
  -
    id: 'cryptsetup.amd64'
    title: '*2:1.6.6-5ubuntu2.1'
  -
    id: 'cryptsetup-bin.*'
    title: '*2:1.6.6-5ubuntu2.1'
  -

```

```
id: 'apt.amd64'
title: '*1.2.27'
-
id: 'apt-utils.amd64'
title: '*1.2.25'
```

- Windows

```
patches:
-
  id: 'KB4284819'
  title: '2018-06 Cumulative Update for Windows Server 2016 (1709) for x64-
based Systems (KB4284819)'
-
  id: 'KB4284833'
-
  id: 'KB4284835'
  title: '2018-06 Cumulative Update for Windows Server 2016 (1803) for x64-
based Systems (KB4284835)'
-
  id: 'KB4284880'
-
  id: 'KB4338814'
```

Nome parametro: **RebootOption**

Utilizzo: facoltativo.

Opzioni: RebootIfNeeded | NoReboot

Default: RebootIfNeeded

 Warning

L'opzione predefinita è RebootIfNeeded. Assicurarsi di selezionare l'opzione corretta per il caso d'uso. Ad esempio, quando è necessario che le istanze vengano riavviate immediatamente per completare un processo di configurazione, scegli RebootIfNeeded. Oppure, quando è necessario mantenere la disponibilità delle istanze fino a un orario di riavvio pianificato, scegli NoReboot.

 Important

L'NoReboot opzione impedisce solo i riavvii a livello di sistema operativo. Service-level i riavvii possono ancora avvenire come parte del processo di applicazione delle patch. Ad esempio, quando Docker viene aggiornato, i servizi dipendenti come Amazon Elastic Container Service potrebbero riavviarsi automaticamente, anche con NoReboot abilitato. Se disponi di servizi critici, che non devono essere interrotti, prendi in considerazione misure aggiuntive come la rimozione temporanea delle istanze dal servizio o la pianificazione dell'applicazione di patch durante le finestre di manutenzione.

 Important

Non è consigliabile utilizzarlo Patch Manager per applicare patch alle istanze di cluster in Amazon EMR (precedentemente chiamato Amazon Elastic). MapReduce In particolare, non selezionare l'opzione RebootIfNeeded per il parametro RebootOption. (Questa opzione è disponibile nei documenti del comando SSM per l'applicazione di patch AWS-RunPatchBaseline, AWS-RunPatchBaselineAssociation e AWS-RunPatchBaselineWithHooks).

I comandi sottostanti per applicare le patch tramite Patch Manager utilizzano i comandi yum e dnf. Pertanto, le operazioni generano incompatibilità a causa del modo in cui i pacchetti vengono installati. Per informazioni sui metodi preferiti per l'aggiornamento del software sui cluster Amazon EMR, consulta [Utilizzo dell'AMI predefinita per Amazon EMR](#) nella Guida per la gestione di Amazon EMR.

RebootIfNeeded

Quando si sceglie l'opzione RebootIfNeeded, l'istanza viene riavviata in uno dei seguenti casi:

- Patch Manager installato uno o più patch.

Patch Manager non valuta se un riavvio è obbligatorio per la patch. Il sistema viene riavviato anche se la patch non richiede il riavvio.

- Patch Manager rileva una o più patch con lo stato di `INSTALLED_PENDING_REBOOT` durante l'operazione `Install`.

Lo stato `INSTALLED_PENDING_REBOOT` indica che l'opzione `NoReboot` è stata selezionata l'ultima volta che l'operazione `Install` è stata eseguita, o che una patch è stata installata all'esterno di Patch Manager dall'ultimo riavvio del nodo gestito.

Il riavvio delle istanze in questi due casi garantisce che i pacchetti aggiornati vengano svuotati dalla memoria e mantengano coerenti il comportamento di patch e di riavvio in tutti i sistemi operativi.

NoReboot

Quando scegli l'opzione `NoReboot`, Patch Manager non riavvia l'istanza anche se ha installato patch durante l'operazione di `Install`. Questa opzione è utile se le istanze non richiedono il riavvio dopo l'applicazione di patch, oppure nel caso di applicazioni o processi in esecuzione su un'istanza che non dovrebbero essere interrotti da un riavvio a seguito di un'operazione di applicazione di patch. È utile anche quando vuoi un maggiore controllo sui tempi dei riavvii dell'istanza, ad esempio utilizzando una finestra di manutenzione.

File di monitoraggio dell'installazione delle patch: per tenere traccia dell'installazione delle patch, in particolare delle patch installate dopo l'ultimo riavvio del sistema, Systems Manager mantiene un file nell'istanza gestita.

Important

Non eliminare o modificare il file di monitoraggio. Quando questo file viene eliminato o danneggiato, il rapporto di conformità della patch per l'istanza non è accurato. In questo caso, riavvia l'istanza ed esegui un'operazione di scansione della patch per ripristinare il file.

Questo file di monitoraggio viene archiviato nei seguenti percorsi nelle istanze gestite:

- Sistemi operativi Linux:
 - `/var/log/amazon/ssm/patch-configuration/patch-states-configuration.json`
 - `/var/log/amazon/ssm/patch-configuration/patch-inventory-from-last-operation.json`
- Windows Server sistema operativo:
 - `C:\ProgramData\Amazon\PatchBaselineOperations\State\PatchStatesConfiguration.json`

- C:\ProgramData\Amazon\PatchBaselineOperations\State\PatchInventoryFromLastOperation.json

Documento di comando SSM per l'applicazione di patch: **AWS-RunPatchBaselineWithHooks**

AWS Systems Manager supporta **AWS-RunPatchBaselineWithHooks**, un documento Systems Manager (documento SSM) per Patch Manager. Questo documento SSM esegue operazioni di applicazione di patch nei nodi gestiti per aggiornamenti correlati alla sicurezza e di altro tipo.

AWS-RunPatchBaselineWithHooks differisce da **AWS-RunPatchBaseline** nei seguenti modi:

- Un documento wrapper – **AWS-RunPatchBaselineWithHooks** è un wrapper per **AWS-RunPatchBaseline** e si basa su **AWS-RunPatchBaseline** per alcune delle sue operazioni.
- L'operazione **Install** – **AWS-RunPatchBaselineWithHooks** supporta gli hook del ciclo di vita che vengono eseguiti in punti designati durante l'applicazione di patch del nodo gestito. Poiché le installazioni di patch a volte richiedono il riavvio dei nodi gestiti, l'operazione di applicazione di patch è suddivisa in due eventi, per un totale di tre hook che supportano funzionalità personalizzate. Il primo hook è prima dell'operazione **Install with NoReboot**. Il secondo hook è dopo dell'operazione **Install with NoReboot**. Il terzo hook è disponibile dopo il riavvio del nodo gestito.
- Nessun supporto per l'elenco di patch personalizzato – **AWS-RunPatchBaselineWithHooks** non supporta il parametro di **InstallOverrideList**.
- Il supporto SSM Agent – **AWS-RunPatchBaselineWithHooks** richiede che SSM Agent 3.0.502 o versione successiva deve essere installata sul nodo gestito di patch.

Quando il documento viene eseguito, utilizza la baseline delle patch attualmente specificata come “predefinita” per un tipo di sistema operativo se non è specificato alcun gruppo di patch. In caso contrario, vengono utilizzate le baseline delle patch associate al gruppo di patch. Per informazioni sui gruppi di patch, consulta [Gruppi di patch](#).

È possibile utilizzare il documento **AWS-RunPatchBaselineWithHooks** per applicare patch ai sistemi operativi e alle applicazioni. (In Windows Server, il supporto delle applicazioni è limitato ai soli aggiornamenti delle applicazioni Microsoft).

Questo documento supporta i nodi gestiti da Linux e Windows Server. Il documento eseguirà le operazioni adeguate per ciascuna piattaforma.

 Note

AWS-RunPatchBaselineWithHooks non è supportato su macOS.

Linux

Nei nodi gestiti Linux, il documento AWS-RunPatchBaselineWithHooks consente di richiamare un modulo Python, che a sua volta scarica una snapshot della baseline delle patch valida per il nodo gestito. Questa snapshot della baseline delle patch utilizza le regole e gli elenchi specificati delle patch approvate e bloccate per controllare il programma di gestione dei pacchetti adeguato per ciascun tipo di nodo:

- I nodi gestiti da Amazon Linux 2, Oracle Linux e RHEL 7 utilizzano YUM. Per le operazioni con YUM, Patch Manager richiede Python 2.6 o una versione supportata successiva (da 2.6 a 3.12). Amazon Linux 2023 utilizza DNF. Per le operazioni DNF, Patch Manager richiede una versione supportata di Python 2 o Python 3 (da 2.6 a 3.12).
- I nodi gestiti 8 RHEL utilizzano DNF. Per le operazioni DNF, Patch Manager richiede una versione supportata di Python 2 o Python 3 (da 2.6 a 3.12). (Nessuna versione è installata per impostazione predefinita su RHEL 8. È necessario installare l'una o l'altra manualmente).
- Le istanze Debian Server e Ubuntu Server utilizzano APT. Per le operazioni APT, Patch Manager richiede una versione supportata di Python 3 (da 3.0 a 3.12).

Windows Server

Sui nodi Windows Server gestiti, il AWS-RunPatchBaselineWithHooks documento scarica e richiama un PowerShell modulo, che a sua volta scarica un'istantanea della baseline della patch che si applica al nodo gestito. Questa snapshot della baseline delle patch contiene un elenco di patch approvate compilate eseguendo una query sulla baseline delle patch su un server Windows Server Update Services (WSUS). Questo elenco viene trasferito all'API di Windows Update, che controlla il download e l'installazione delle patch approvate, in base alle necessità.

Ogni istantanea è specifica per un gruppo di patch Account AWS, un sistema operativo e un ID di istantanea. Lo snapshot viene consegnato tramite un URL Amazon Simple Storage Service (Amazon S3) prefirato, che scade 24 ore dopo la creazione dello snapshot. Dopo la scadenza dell'URL, tuttavia, se desideri applicare lo stesso contenuto snapshot ad altri nodi gestiti, è possibile generare

un nuovo URL Amazon S3 prefirmato fino a tre giorni dopo la creazione della copia istantanea. Per farlo, utilizzare il comando [get-deployable-patch-snapshot-for-instance](#).

Dopo avere installato tutti gli aggiornamenti approvati e applicabili e dopo avere eseguito il riavvio, le informazioni sulla conformità delle patch vengono generate in un nodo gestito e trasferite a Patch Manager.

Se il parametro `RebootOption` è impostato su `NoReboot` nel documento `AWS-RunPatchBaselineWithHooks`, il nodo gestito non viene riavviato dopo l'esecuzione di Patch Manager. Per ulteriori informazioni, consulta [Nome parametro: RebootOption](#).

Important

Sebbene l'opzione di `NoReboot` impedisca il riavvio del sistema operativo, non impedisce i riavvii a livello di servizio, che potrebbero verificarsi quando determinati pacchetti vengono aggiornati. Ad esempio, l'aggiornamento di pacchetti come Docker può attivare il riavvio automatico dei servizi dipendenti (come i servizi di orchestrazione dei container), anche quando `NoReboot` viene specificato.

Per informazioni sulla visualizzazione dei dati di conformità delle patch, consulta [Informazioni sulla conformità delle patch](#).

Fasi operative di **AWS-RunPatchBaselineWithHooks**

Quando `AWS-RunPatchBaselineWithHooks` è in esecuzione, vengono portati a termine i seguenti passaggi:

1. Scan- Un'operazione di Scan utilizzando `AWS-RunPatchBaseline` viene eseguita sul nodo gestito e viene generato e caricato un report di conformità.
2. Verificare gli stati delle patch locali - Viene eseguito uno script per determinare quali passaggi verranno eseguiti in base all'operazione selezionata e al risultato di Scan della fase 1.
 - a. Se l'operazione selezionata è Scan, essa è contrassegnata come completata. L'operazione si conclude.
 - b. Se l'operazione selezionata è Install, Patch Manager valuta il risultato di Scan dal Passaggio 1 per determinare cosa eseguire dopo:

- i. Se non vengono rilevate patch mancanti e non sono necessari riavvii in sospeso, l'operazione procede direttamente al passaggio finale (Passaggio 8), che include un hook fornito. Tutti i passaggi intermedi vengono saltati.
 - ii. Se non vengono rilevate patch mancanti, ma sono necessari riavvii in sospeso e l'opzione di riavvio selezionata è NoReboot, l'operazione procede direttamente alla fase finale (Step 8), che include un hook fornito. Tutti i passaggi intermedi vengono saltati.
 - iii. Altrimenti, l'operazione passa alla fase successiva.
3. Pre-patch operazione di hook: il documento SSM fornito per il primo hook del ciclo di vita viene eseguito sul `PreInstallHookDocName` nodo gestito.
4. Installazione con NoReboot: viene `Install` eseguita un'operazione con l'opzione di riavvio da NoReboot utilizzare sul nodo gestito e `AWS-RunPatchBaseline` viene generato e caricato un report di conformità.
5. Post-install operazione hook: il documento SSM fornito per il secondo hook del ciclo di vita viene eseguito sul nodo gestito. `PostInstallHookDocName`
6. Verifica del riavvio - Viene eseguito uno script per determinare se è necessario un riavvio per il nodo gestito e quali passaggi eseguire:
 - a. Quando l'opzione di riavvio selezionata è NoReboot, essa procede direttamente alla fase finale (Step 8), che include un hook fornito. Tutti i passaggi intermedi vengono saltati.
 - b. Quando l'opzione di riavvio selezionata è RebootIfNeeded, Patch Manager verifica se sono necessari riavvii in sospeso dall'inventario raccolto al passaggio 4. Ciò significa che l'operazione continua nella fase 7 e il nodo gestito viene riavviato in uno dei seguenti casi:
 - i. Patch Manager ha installato una o più patch. (Patch Manager non valuta se un riavvio è obbligatorio per la patch. Il sistema viene riavviato anche se la patch non richiede il riavvio.)
 - ii. Patch Manager rileva una o più patch con lo stato di `INSTALLED_PENDING_REBOOT` durante l'operazione di installazione. Lo stato `INSTALLED_PENDING_REBOOT` indica che l'opzione NoReboot è stata selezionata l'ultima volta che l'operazione di installazione è stata eseguita, o che una patch è stata installata all'esterno di Patch Manager dall'ultimo riavvio del nodo gestito.

Quando non vengono rilevate patch che rispondono a questi criteri, l'operazione di applicazione della patch del nodo gestito viene completata e si passa direttamente alla fase finale (passaggio 8), che include un hook fornito. Tutti i passaggi intermedi vengono saltati.

7. Riavvio e report - Un'operazione di installazione con l'opzione di riavvio di `RebootIfNeeded` viene eseguito sul nodo gestito utilizzando `AWS-RunPatchBaseline` e viene generato e caricato un report sulla conformità.
8. Post-reboot operazione di aggancio: il documento SSM fornito per il terzo hook del ciclo di vita viene eseguito sul nodo `OnExitHookDocName` gestito.

Per un'operazione `Scan`, se il Passaggio 1 non va a buon fine, il processo di esecuzione del documento si interrompe e il passaggio viene segnalato come non andato a buon fine, anche se i passaggi successivi vengono segnalati come esito positivo.

Per un'operazione `Install`, se uno qualsiasi dei passaggi `aws:runDocument` non va a buon fine durante l'operazione, tali passaggi vengono segnalati come non andati a buon fine e l'operazione procede direttamente al Passaggio finale (Passaggio 8), che include un hook fornito. Tutti i passaggi intermedi vengono saltati. Questo passaggio viene segnalato come non andato a buon fine, l'ultimo passaggio riporta lo stato del risultato dell'operazione e tutti i passaggi intermedi vengono segnalati come esito positivo.

Parametri di **AWS-RunPatchBaselineWithHooks**

`AWS-RunPatchBaselineWithHooks` supporta sei parametri.

Il parametro `Operation` è obbligatorio.

I parametri `RebootOption`, `PreInstallHookDocName`, `PostInstallHookDocName` e `OnExitHookDocName` sono facoltativi.

`Snapshot-ID` è tecnicamente facoltativo, ma è consigliabile fornire un valore personalizzato per esso quando si esegue `AWS-RunPatchBaselineWithHooks` al di fuori di una finestra di manutenzione. Consenti a Patch Manager di fornire il valore automaticamente quando il documento viene eseguito nell'ambito di un'operazione di manutenzione.

Parameters

- [Nome del parametro: Operazione](#)
- [Nome del parametro: Snapshot ID](#)
- [Nome parametro: RebootOption](#)
- [Nome parametro: PreInstallHookDocName](#)
- [Nome parametro: PostInstallHookDocName](#)
- [Nome parametro: OnExitHookDocName](#)

Nome del parametro: Operazione

Utilizzo: obbligatorio.

Opzioni: Scan | Install.

Scan

Quando si sceglie l'opzione Scan, il sistema utilizza il documento AWS-RunPatchBaseline per determinare lo stato di conformità delle patch dell'istanza e riferisce queste informazioni a Patch Manager. Scan non richiede l'installazione degli aggiornamenti o il riavvio dei nodi gestiti. L'operazione identifica dove gli aggiornamenti approvati e applicabili al nodo risultano mancanti.

Installa

Quando si sceglie l'opzione Install, AWS-RunPatchBaselineWithHooks tenta di installare gli aggiornamenti applicabili e approvati che risultano mancanti nel nodo gestito. Le informazioni sulla conformità delle patch generate in un'operazione Install non visualizzano gli aggiornamenti mancanti, ma sono in grado di specificare lo stato di errore degli aggiornamenti se per qualsiasi motivo l'installazione non è andata a buon fine. Ogni volta che viene installato un aggiornamento su un nodo gestito, il nodo viene riavviato per assicurarsi che l'aggiornamento sia installato e attivo. (Eccezione: se il parametro RebootOption è impostato su NoReboot nel documento AWS-RunPatchBaselineWithHooks, il nodo non viene riavviato dopo l'esecuzione di Patch Manager. Per ulteriori informazioni, consulta [Nome parametro: RebootOption](#).)

Note

Se una patch specificata dalle regole di baseline viene installata prima che Patch Manager aggiorni il nodo gestito, è possibile che il sistema non venga riavviato come previsto. Ciò si verifica quando una patch viene installata manualmente da un utente o installata automaticamente da un altro programma, ad esempio il pacchetto unattended-upgrades su Ubuntu Server.

Nome del parametro: Snapshot ID

Utilizzo: facoltativo.

Snapshot ID è un ID univoco (GUID) utilizzato da Patch Manager per assicurare che una serie di nodi gestiti a cui vengono applicate le patch in un'unica operazione abbiano la stessa serie di patch approvate. Sebbene il parametro sia definito facoltativo, le nostre best practice consigliate

dipendono dal fatto che tu stia eseguendo `AWS-RunPatchBaselineWithHooks` o meno una finestra di manutenzione, come descritto nella tabella seguente.

Best practice di `AWS-RunPatchBaselineWithHooks`

Modalità	Best practice	Informazioni
In esecuzione <code>AWS-RunPatchBaselineWithHooks</code> all'interno di una finestra di manutenzione	Non fornire un ID della snapshot. Patch Manager la fornirà automaticamente.	<p>Quando utilizzi una finestra di manutenzione per eseguire <code>AWS-RunPatchBaselineWithHooks</code>, non devi fornire l'ID della snapshot generata. In questo scenario, Systems Manager fornisce un valore GUID in base all'ID di esecuzione della finestra di manutenzione. In questo modo, si garantisce che venga utilizzato un ID corretto per tutte le invocazioni di <code>AWS-RunPatchBaselineWithHooks</code> in tale finestra di manutenzione.</p> <p>Si noti che se si specifica un valore in questo scenario, la snapshot della baseline delle patch potrebbe non durare per più di 3 giorni. In seguito, verrà generata una nuova snapshot anche se hai specificato lo stesso ID dopo la scadenza della snapshot.</p>
In esecuzione <code>AWS-RunPatchBaselineWithHooks</code> al di fuori di una finestra di manutenzione	Generare e specificare un valore GUID personalizzato per l'ID della snapshot.	Se non utilizzi una finestra di manutenzione per eseguire <code>AWS-RunPatchBaselineWithHooks</code> , ti consiglia

Modalità	Best practice	Informazioni
		<p>mo di generare e specificare un ID snapshot univoco per ogni baseline delle patch, soprattutto se stai eseguendo il documento <code>AWS-RunPatchBaselineWithHooks</code> su più nodi gestiti nella stessa operazione. Se specifichi un ID in questo scenario, Systems Manager genera un altro ID snapshot per ciascun nodo gestito a cui viene inviato il comando. Di conseguenza, potrebbero venire specificate varie serie di patch fra i nodi.</p> <p>Ad esempio, potresti eseguire il documento <code>AWS-RunPatchBaselineWithHooks</code> direttamente tramite Run Command, uno strumento di AWS Systems Manager e destinarlo a un gruppo di 50 nodi gestiti. Specificando un ID snapshot personalizzato verrà creata una singola snapshot di baseline utilizzata per valutare le patch e tutti i nodi gestiti, per garantire che il relativo stato finale sia coerente.</p>

Modalità	Best practice	Informazioni
----------	---------------	--------------

¹ È possibile utilizzare qualsiasi strumento in grado di generare un GUID per ottenere il valore del parametro ID snapshot. Ad esempio, in PowerShell, è possibile utilizzare il `New-Guid` cmdlet per generare un GUID nel formato di. 12345699-9405-4f69-bc5e-9315aEXAMPLE

Nome parametro: **RebootOption**

Utilizzo: facoltativo.

Opzioni: `RebootIfNeeded` | `NoReboot`

Default: `RebootIfNeeded`

Warning

L'opzione predefinita è `RebootIfNeeded`. Assicurarsi di selezionare l'opzione corretta per il caso d'uso. Ad esempio, quando è necessario che i nodi gestiti vengano riavviati immediatamente per completare un processo di configurazione, scegli `RebootIfNeeded`. Oppure, quando è necessario mantenere la disponibilità dei nodi gestiti fino a un orario di riavvio pianificato, scegli `NoReboot`.

Important

Non è consigliabile utilizzarlo Patch Manager per applicare patch alle istanze di cluster in Amazon EMR (precedentemente chiamato Amazon Elastic). MapReduce In particolare, non selezionare l'opzione `RebootIfNeeded` per il parametro `RebootOption`. (Questa opzione è disponibile nei documenti del comando SSM per l'applicazione di patch `AWS-RunPatchBaseline`, `AWS-RunPatchBaselineAssociation` e `AWS-RunPatchBaselineWithHooks`).

I comandi sottostanti per applicare le patch tramite Patch Manager utilizzano i comandi `yum` e `dnf`. Pertanto, le operazioni generano incompatibilità a causa del modo in cui i pacchetti vengono installati. Per informazioni sui metodi preferiti per l'aggiornamento del software sui cluster Amazon EMR, consulta [Utilizzo dell'AMI predefinita per Amazon EMR](#) nella Guida per la gestione di Amazon EMR.

RebootIfNeeded

Quando si sceglie l'opzione `RebootIfNeeded`, il nodo gestito viene riavviato in uno dei seguenti casi:

- Patch Manager installato uno o più patch.

Patch Manager non valuta se un riavvio è obbligatorio per la patch. Il sistema viene riavviato anche se la patch non richiede il riavvio.

- Patch Manager rileva una o più patch con lo stato di `INSTALLED_PENDING_REBOOT` durante l'operazione `Install`.

Lo stato `INSTALLED_PENDING_REBOOT` indica che l'opzione `NoReboot` è stata selezionata l'ultima volta che l'operazione `Install` è stata eseguita, o che una patch è stata installata all'esterno di Patch Manager dall'ultimo riavvio del nodo gestito.

Il riavvio dei nodi gestiti in questi due casi garantisce che i pacchetti aggiornati vengano svuotati dalla memoria e mantengano coerenti il comportamento di patch e di riavvio in tutti i sistemi operativi.

NoReboot

Quando scegli l'opzione `NoReboot`, Patch Manager non riavvia il nodo gestito anche se ha installato patch durante l'operazione di `Install`. Questa opzione è utile se i nodi gestiti non richiedono il riavvio dopo l'applicazione di patch, oppure nel caso di applicazioni o processi in esecuzione su un nodo che non dovrebbero essere interrotti da un riavvio a seguito di un'operazione di applicazione di patch. È utile anche quando si necessita di un maggiore controllo sui tempi dei riavvii del nodo gestito, ad esempio utilizzando una finestra di manutenzione.

Note

Quando si sceglie l'opzione `NoReboot` e viene installata una patch, alla patch viene assegnato lo stato `InstalledPendingReboot`. Il nodo gestito stesso, tuttavia, viene contrassegnato come `Non-Compliant`. Dopo che si verifica un riavvio e viene eseguita un'operazione `Scan`, lo stato del nodo diventa `Compliant`.

File di monitoraggio dell'installazione delle patch: per tenere traccia dell'installazione delle patch, in particolare delle patch installate dopo l'ultimo riavvio del sistema, Systems Manager mantiene un file nel nodo gestito.

⚠ Important

Non eliminare o modificare il file di monitoraggio. Se questo file viene eliminato o danneggiato, il rapporto di conformità della patch per il nodo gestito non è accurato. In questo caso, riavvia il nodo ed esegui un'operazione di scansione della patch per ripristinare il file.

Questo file di monitoraggio viene archiviato nei seguenti percorsi nei nodi gestiti:

- Sistemi operativi Linux:
 - `/var/log/amazon/ssm/patch-configuration/patch-states-configuration.json`
 - `/var/log/amazon/ssm/patch-configuration/patch-inventory-from-last-operation.json`
- Windows Server sistema operativo:
 - `C:\ProgramData\Amazon\PatchBaselineOperations\State\PatchStatesConfiguration.json`
 - `C:\ProgramData\Amazon\PatchBaselineOperations\State\PatchInventoryFromLastOperation.json`

Nome parametro: **PreInstallHookDocName**

Utilizzo: facoltativo.

Default: AWS-Noop

Il valore da fornire per il parametro `PreInstallHookDocName` è il nome o l'Amazon Resource Name (ARN) di un documento SSM di tua scelta. Puoi fornire il nome di un documento AWS gestito o il nome o l'ARN di un documento SSM personalizzato che hai creato o che è stato condiviso con te. (Per un documento SSM che è stato condiviso con te da un altro Account AWS, devi specificare l'ARN completo della risorsa, ad esempio.) `arn:aws:ssm:us-east-2:123456789012:document/MySharedDocument`

Il documento SSM specificato viene eseguito prima dell'operazione `Install` esegue tutte le operazioni supportate da SSM Agent, ad esempio uno script di shell per controllare il controllo dell'integrità dell'applicazione prima che venga eseguita l'applicazione di patch sul nodo gestito. Per un elenco di operazioni, consulta [Documentazione di riferimento del plugin per i documenti di](#)

[comando](#)). Il nome di default del documento SSM è AWS-Noop, che non esegue alcuna operazione sul nodo gestito.

Per informazioni sulla creazione di un documento SSM personalizzato, consulta [Creazione del contenuto del documento SSM](#).

Nome parametro: **PostInstallHookDocName**

Utilizzo: facoltativo.

Default: AWS-Noop

Il valore da fornire per il parametro `PostInstallHookDocName` è il nome o l'Amazon Resource Name (ARN) di un documento SSM di tua scelta. Puoi fornire il nome di un documento AWS gestito o il nome o l'ARN di un documento SSM personalizzato che hai creato o che è stato condiviso con te. (Per un documento SSM che è stato condiviso con te da un altro Account AWS, devi specificare l'ARN completo della risorsa, ad esempio.) `arn:aws:ssm:us-east-2:123456789012:document/MySharedDocument`

Il documento SSM specificato viene eseguito dopo l'operazione `Install with NoReboot` ed esegue tutte le azioni supportate da SSM Agent, ad esempio uno script di shell per l'installazione di aggiornamenti di terze parti prima del riavvio. Per un elenco di operazioni, consulta [Documentazione di riferimento del plugin per i documenti di comando](#)). Il nome di default del documento SSM è AWS-Noop, che non esegue alcuna operazione sul nodo gestito.

Per informazioni sulla creazione di un documento SSM personalizzato, consulta [Creazione del contenuto del documento SSM](#).

Nome parametro: **OnExitHookDocName**

Utilizzo: facoltativo.

Default: AWS-Noop

Il valore da fornire per il parametro `OnExitHookDocName` è il nome o l'Amazon Resource Name (ARN) di un documento SSM di tua scelta. Puoi fornire il nome di un documento AWS gestito o il nome o l'ARN di un documento SSM personalizzato che hai creato o che è stato condiviso con te. (Per un documento SSM che è stato condiviso con te da un Account AWS diverso, è necessario specificare l'ARN della risorsa completa, ad esempio `arn:aws:ssm:us-east-2:123456789012:document/MySharedDocument`).

Il documento SSM specificato viene eseguito dopo l'operazione di riavvio del nodo gestito ed esegue tutte le operazioni supportate da SSM Agent, ad esempio uno script di shell per verificare l'integrità del nodo dopo il completamento dell'operazione di applicazione di patch. Per un elenco di operazioni, consulta [Documentazione di riferimento del plugin per i documenti di comando](#)). Il nome di default del documento SSM è AWS-Noop, che non esegue alcuna operazione sul nodo gestito.

Per informazioni sulla creazione di un documento SSM personalizzato, consulta [Creazione del contenuto del documento SSM](#).

Scenario di esempio per l'utilizzo del InstallOverrideList parametro in **AWS-RunPatchBaseline** o **AWS-RunPatchBaselineAssociation**

Usa il parametro `InstallOverrideList`, quando vuoi sovrascrivere le patch specificate dalla baseline delle patch corrente della patch predefinita, in Patch Manager, uno strumento di AWS Systems Manager. In questo argomento vengono forniti esempi che illustrano come utilizzare questo parametro per effettuare le seguenti operazioni:

- Applicare diversi set di patch a un gruppo target di nodi gestiti.
- Applicare questi set di patch a frequenze diverse.
- Utilizzare la stessa baseline delle patch per entrambe le operazioni.

Supponiamo che vuoi installare due diverse categorie di patch nei nodi Amazon Linux 2. Vuoi installare queste patch su pianificazioni diverse utilizzando le finestre di manutenzione. Vuoi eseguire una finestra di manutenzione ogni settimana e installare tutte le patch `Security`. Vuoi eseguire un'altra finestra di manutenzione una volta al mese e installare tutte le patch disponibili o le categorie di patch diverse da `Security`.

Tuttavia, solo una baseline delle patch alla volta può essere specificata come predefinita nel sistema operativo. Questo requisito consente di evitare situazioni in cui una baseline delle patch approva una patch mentre un'altra la blocca, il che può causare problemi tra versioni in conflitto.

Con la seguente strategia, è possibile utilizzare il parametro `InstallOverrideList` per applicare diversi tipi di patch a un gruppo di destinazione in pianificazioni diverse, pur utilizzando la stessa baseline delle patch:

1. Nella baseline della patch predefinita, assicurati che siano specificati solo `Security` gli aggiornamenti.

2. Crea una prima finestra di manutenzione che esegue `AWS-RunPatchBaseline` o `AWS-RunPatchBaselineAssociation` ogni settimana. Non specificare un elenco di sostituzioni.
3. Crea un elenco di sostituzioni delle patch di tutti i tipi che vuoi applicare su base mensile e archivalo in un bucket Amazon Simple Storage Service (Amazon S3).
4. Crea una seconda finestra di manutenzione che viene eseguita una volta al mese. Tuttavia, per l'attività Run Command che vuoi registrare per questa finestra di manutenzione, specifica la posizione dell'elenco di sostituzioni.

Il esito: ogni settimana vengono installate solo le patch Security, come definito nella baseline delle patch predefinita. Tutte le patch disponibili, o qualsiasi sottoinsieme di patch che definisci, vengono installate ogni mese.

Note

Quando applichi una patch a un nodo che utilizza solo IPv6, assicurati che l'URL fornito sia raggiungibile dal nodo. Se l'opzione di SSM Agent configurazione `UseDualStackEndpoint` è impostata su `true`, quando viene fornito un URL S3 viene utilizzato un client S3 dualstack. [the section called “Tutorial: applicare patch a un server in un ambiente solo IPv6”](#) Per ulteriori informazioni sulla configurazione dell'agente per l'utilizzo del dualstack, vedere.

Per maggiori informazioni ed esempi, consulta [Nome parametro: `InstallOverrideList`](#).

Utilizzo del `BaselineOverride` parametro

È possibile definire le preferenze di patching in fase di esecuzione utilizzando la funzionalità di sostituzione della linea di base in. Patch Manager Per farlo, specificare un bucket Amazon Simple Storage Service (Amazon S3) contenente un oggetto JSON con un elenco delle baseline delle patch. L'operazione di applicazione di patch utilizza le baseline fornite nell'oggetto JSON che corrispondono al sistema operativo host anziché applicare le regole dalla baseline delle patch predefinita.

Important

Il nome del file `BaselineOverride` non consente la presenza dei seguenti caratteri: backtick (`), virgolette singole ('), virgolette doppie (") e simbolo del dollaro (\$).

Tranne quando un'operazione di patch utilizza una policy di patch, l'utilizzo del parametro `BaselineOverride` non sovrascrive la conformità della patch della baseline fornita nel parametro. I risultati di output vengono registrati nei log di Stdout da. Run Command I risultati stampano solo i pacchetti contrassegnati come `NON_COMPLIANT`. Ciò significa che il pacchetto è contrassegnato come `Missing`, `Failed`, `InstalledRejected`, oppure `InstalledPendingReboot`.

Tuttavia, quando un'operazione di patch utilizza una policy di patch, il sistema passa il parametro di sostituzione dal bucket S3 associato e il valore di conformità viene aggiornato per il nodo gestito. Per ulteriori informazioni sul comportamento delle policy di patch, consulta [Configurazioni delle policy sulle patch in Configurazione rapida](#).

Note

Quando applichi una patch a un nodo che utilizza solo IPv6, assicurati che l'URL fornito sia raggiungibile dal nodo. Se l'opzione di SSM Agent configurazione `UseDualStackEndpoint` è impostata su `true`, quando viene fornito un URL S3 viene utilizzato un client S3 dualstack. [the section called “Tutorial: applicare patch a un server in un ambiente solo IPv6”](#) Per ulteriori informazioni sulla configurazione dell'agente per l'utilizzo del dualstack, vedere.

Utilizzo della sostituzione della baseline delle patch con i parametri ID Snapshot o dell'installazione Install Override List

Esistono due casi in cui la sostituzione della baseline delle patch ha un comportamento degno di nota.

Utilizzo simultaneo della sostituzione della baseline e dell'ID snapshot

Gli snapshot ID assicurano che tutti i nodi gestiti in un particolare comando di patching applichino tutti la stessa cosa. Ad esempio, quando si esegue la patch di 1.000 nodi contemporaneamente, le patch saranno le stesse.

Quando si utilizzano sia un ID snapshot che una sostituzione della baseline delle patch, l'ID snapshot ha la precedenza sulla sostituzione della baseline della patch. Le regole di sostituzione della baseline verranno comunque utilizzate, ma verranno valutate una sola volta. Nell'esempio precedente, le patch tra i 1.000 nodi gestiti saranno sempre le stesse. Se, a metà dell'operazione di applicazione di patch, è stato modificato il file JSON nel bucket S3 di riferimento per essere diverso, le patch applicate saranno comunque le stesse. Questo perché è stato fornito l'ID snapshot.

Utilizzo simultaneo della sostituzione della baseline e Install Override List

Non è possibile utilizzare questi due parametri nello stesso momento. Il documento di applicazione di patch non va a buon fine se vengono forniti entrambi i parametri e non esegue alcuna scansione o installazione nel nodo gestito.

Esempi di codice

Il seguente esempio di codice per Python mostra come generare la sostituzione della baseline delle patch.

```
import boto3
import json

ssm = boto3.client('ssm')
s3 = boto3.resource('s3')
s3_bucket_name = 'my-baseline-override-bucket'
s3_file_name = 'MyBaselineOverride.json'
baseline_ids_to_export = ['pb-0000000000000000', 'pb-0000000000000001']

baseline_overrides = []
for baseline_id in baseline_ids_to_export:
    baseline_overrides.append(ssm.get_patch_baseline(
        BaselineId=baseline_id
    ))

json_content = json.dumps(baseline_overrides, indent=4, sort_keys=True, default=str)
s3.Object(bucket_name=s3_bucket_name, key=s3_file_name).put(Body=json_content)
```

Ciò produce una sostituzione della baseline delle patch simile alla seguente.

```
[
  {
    "ApprovalRules": {
      "PatchRules": [
        {
          "ApproveAfterDays": 0,
          "ComplianceLevel": "UNSPECIFIED",
          "EnableNonSecurity": false,
          "PatchFilterGroup": {
            "PatchFilters": [
              {
                "Key": "PRODUCT",
                "Values": [
                  "*"
                ]
              }
            ]
          }
        }
      ]
    }
  }
]
```



```

        ]
      },
      {
        "Key": "CLASSIFICATION",
        "Values": [
          "*"
        ]
      },
      {
        "Key": "SEVERITY",
        "Values": [
          "*"
        ]
      }
    ]
  }
}
],
{
  "ApprovedPatches": [],
  "ApprovedPatchesComplianceLevel": "UNSPECIFIED",
  "ApprovedPatchesEnableNonSecurity": false,
  "GlobalFilters": {
    "PatchFilters": []
  },
  "OperatingSystem": "AMAZON_LINUX_2",
  "RejectedPatches": [],
  "RejectedPatchesAction": "ALLOW_AS_DEPENDENCY",
  "Sources": []
},
{
  "ApprovalRules": {
    "PatchRules": [
      {
        "ApproveUntilDate": "2021-01-06",
        "ComplianceLevel": "UNSPECIFIED",
        "EnableNonSecurity": true,
        "PatchFilterGroup": {
          "PatchFilters": [
            {
              "Key": "PRODUCT",
              "Values": [
                "*"
              ]
            }
          ]
        }
      }
    ]
  }
}

```

```

    },
    {
      "Key": "CLASSIFICATION",
      "Values": [
        "*"
      ]
    },
    {
      "Key": "SEVERITY",
      "Values": [
        "*"
      ]
    }
  ]
}
]
},
"ApprovedPatches": [
  "open-ssl*"
],
"ApprovedPatchesComplianceLevel": "UNSPECIFIED",
"ApprovedPatchesEnableNonSecurity": false,
"GlobalFilters": {
  "PatchFilters": []
},
"OperatingSystem": "SUSE",
"RejectedPatches": [
  "python*"
],
"RejectedPatchesAction": "ALLOW_AS_DEPENDENCY",
"Sources": []
}
]

```

Baseline delle patch

Gli argomenti di questa sezione forniscono informazioni su come funzionano le baseline delle patch in Patch Manager, quando si esegue un'installazione o si esegue un'operazione Scan sui nodi gestiti.

Baseline delle patch predefinite e personalizzate

Patch Manager fornisce linee di base delle patch predefinite per ciascuno dei sistemi operativi supportati da Patch Manager. È possibile utilizzare queste basi così come sono configurate (non è possibile personalizzarle) oppure è possibile creare baseline delle patch personalizzate. Le baseline delle patch personalizzate ti consentono di ottenere un maggiore controllo sulle patch approvate o rifiutate per l'ambiente. Inoltre, le baseline predefinite assegnano un livello di conformità Unspecified a tutte le patch installate queste basi. Per assegnare i valori di conformità, è possibile creare una copia di una baseline predefinita e specificare i valori di conformità che vuoi assegnare alle patch. Per ulteriori informazioni, consulta [Baseline personalizzate](#) e [Utilizzo delle baseline delle patch personalizzate](#).

Note

Le informazioni contenute in questo argomento si applicano indipendentemente dal metodo o dal tipo di configurazione utilizzato per le operazioni di applicazione di patch:

- Una policy di patch configurata in Quick Setup
- Un'opzione di gestione host configurata in Quick Setup
- Una finestra di manutenzione per eseguire un'attività Scan o Install di patch
- Un'operazione Applica subito una patch on demand

Baseline predefinite

Nella seguente tabella sono riportate le baseline delle patch predefinite fornite con Patch Manager.

Per informazioni sulle versioni di ciascun sistema operativo supportato da Patch Manager, consulta [Patch Manager prerequisiti](#).

Nome	Sistema operativo supportato	Informazioni
AWS-AlmaLinuxDefaultPatchBaseline	AlmaLinux	Approva tutte le patch del sistema operativo classificate come "Sicurezza" e con un livello di gravità pari a "Critico" o "Importante". Approva inoltre tutte le patch classificate come

Nome	Sistema operativo supportato	Informazioni
		"Bugfix". Le patch vengono approvate automaticamente 7 giorni dopo il rilascio o l'aggiornamento. ¹
AWS-AmazonLinux2DefaultPatchBaseline	Amazon Linux 2	Approva tutte le patch del sistema operativo classificate come "Sicurezza" e con un livello di gravità pari a "Critico" o "Importante". Inoltre approva tutte le patch classificate come "Bugfix". Le patch vengono approvate automaticamente 7 giorni dopo il rilascio. ¹
AWS-AmazonLinux2023DefaultPatchBaseline	Amazon Linux 2023	Approva tutte le patch del sistema operativo classificate come "Sicurezza" e con un livello di gravità pari a "Critico" o "Importante". Le patch vengono approvate automaticamente sette giorni dopo il rilascio. Inoltre approva tutte le patch classificate come "Bugfix" sette giorni dopo il rilascio.
AWS-CentOSDefaultPatchBaseline	CentOS Stream	Approva tutti gli aggiornamenti sette giorni dopo il rilascio, inclusi quelli non correlati alla sicurezza.

Nome	Sistema operativo supportato	Informazioni
AWS-DebianDefaultPatchBaseline	Debian Server	Approva immediatamente tutte le patch del sistema operativo correlate alla sicurezza con la priorità "Obbligatorio", "Importante", "Standard", "Facoltativo" oppure "Extra". Non vi è alcun tempo di attesa prima dell'approvazione perché le date di rilascio affidabili non sono disponibili nei repository.
AWS-MacOSDefaultPatchBaseline	macOS	Approva tutte le patch del sistema operativo classificate come "Security". Approva anche tutti i pacchetti con un aggiornamento corrente.
AWS-OracleLinuxDefaultPatchBaseline	Oracle Linux	Approva tutte le patch del sistema operativo classificate come "Sicurezza" e con un livello di gravità pari a "Importante" o "Moderato". Approva inoltre tutte le patch classificate come "Bugfix" 7 giorni dopo il rilascio. Le patch vengono approvate automaticamente 7 giorni dopo il rilascio o l'aggiornamento. ¹

Nome	Sistema operativo supportato	Informazioni
AWS-RedHatDefaultPatchBaseline	Red Hat Enterprise Linux (RHEL)	Approva tutte le patch del sistema operativo classificate come "Sicurezza" e con un livello di gravità pari a "Critico" o "Importante". Approva inoltre tutte le patch classificate come "Bugfix". Le patch vengono approvate automaticamente 7 giorni dopo il rilascio o l'aggiornamento. ¹
AWS-RockyLinuxDefaultPatchBaseline	Rocky Linux	Approva tutte le patch del sistema operativo classificate come "Sicurezza" e con un livello di gravità pari a "Critico" o "Importante". Approva inoltre tutte le patch classificate come "Bugfix". Le patch vengono approvate automaticamente 7 giorni dopo il rilascio o l'aggiornamento. ¹
AWS-SuseDefaultPatchBaseline	SUSE Linux Enterprise Server (SLES)	Approva tutte le patch del sistema operativo classificate come "Sicurezza" e con una gravità pari a "Critica" o "Importante". Le patch vengono approvate automaticamente 7 giorni dopo il rilascio o l'aggiornamento. ¹

Nome	Sistema operativo supportato	Informazioni
AWS-UbuntuDefaultPatchBaseline	Ubuntu Server	Approva immediatamente tutte le patch del sistema operativo correlate alla sicurezza con la priorità "Obbligatorio", "Importante", "Standard", "Facoltativo" oppure "Extra". Non vi è alcun tempo di attesa prima dell'approvazione perché le date di rilascio affidabili non sono disponibili nei repository.
AWS-DefaultPatchBaseline	Windows Server	Approva tutte le patch del sistema Windows Server operativo classificate come "" o "CriticalUpdatesSecurityUpdates" e la cui severità MSRC è «Critica» o «Importante». Le patch vengono approvate automaticamente 7 giorni dopo il rilascio o l'aggiornamento. ²
AWS-WindowsPredefinedPatchBaseline-OS	Windows Server	Approva tutte le patch del sistema Windows Server operativo classificate come "" o "CriticalUpdatesSecurityUpdates" e la cui severità MSRC è «Critica» o «Importante». Le patch vengono approvate automaticamente 7 giorni dopo il rilascio o l'aggiornamento. ²

Nome	Sistema operativo supportato	Informazioni
AWS-WindowsPredefinedPatchBaseline-0S-Applications	Windows Server	Per il sistema Windows Server operativo, approva tutte le patch classificate come "" o "CriticalUpdatesSecurityUpdates" e la cui severità MSRC è «Critica» o «Importante». Per le applicazioni rilasciate da Microsoft, approva tutte le patch. Sia le patch del sistema operativo sia quelle delle applicazioni vengono approvate automaticamente 7 giorni dopo il rilascio o l'aggiornamento. ²

¹ Per Amazon Linux 2, l'attesa di sette giorni prima dell'approvazione automatica delle patch viene calcolata in base al valore `Updated Date` in `updateinfo.xml`, non al valore `Release Date`. Vari fattori possono influire sul valore `Updated Date`. Altri sistemi operativi gestiscono le date di rilascio e aggiornamento in modo diverso. Per informazioni su come evitare risultati imprevisti dovuti a ritardi nell'approvazione automatica, consulta [Il modo in cui vengono calcolate le date di rilascio e di aggiornamento dei pacchetti](#).

² Per Windows Server, le baseline predefinite includono un ritardo di approvazione automatica di 7 giorni. Per installare una patch entro 7 giorni dal rilascio, è necessario creare una baseline personalizzata.

Baseline personalizzate

Consulta le seguenti informazioni utili per creare baseline delle patch personalizzate per raggiungere gli obiettivi di patch.

Utilizzo delle approvazioni automatiche nelle baseline personalizzate

Se crei la tua baseline delle patch, potrai scegliere le patch da approvare automaticamente utilizzando le seguenti categorie.

- Sistema operativo: versioni supportate di Windows Server, Amazon Linux, Ubuntu Server e così via.
- Nome del prodotto (per i sistemi operativi): ad esempio, RHEL 7.5, Amazon Linux 2023 2023.8.20250808, 2012, 2012 R2 e così via. Windows Server Windows Server
- Nome del prodotto (Windows Serversolo per le applicazioni rilasciate da Microsoft): ad esempio, Word 2016, Server e così via. BizTalk
- Classificazione: ad esempio aggiornamenti critici, aggiornamenti di sicurezza e così via.
- Gravità: ad esempio critica, importante e così via.

Per ogni regola di approvazione creata, è possibile scegliere di specificare un ritardo di approvazione automatica o specificare una data limite di approvazione patch.

Note

Poiché non è possibile determinare in modo affidabile le date di rilascio dei pacchetti di aggiornamento per Ubuntu Server, le opzioni di approvazione automatica non sono supportate per questo sistema operativo.

Il ritardo è il numero di giorni di attesa dopo il rilascio o l'ultimo aggiornamento della patch, prima che questa venga automaticamente approvata per l'applicazione. Ad esempio, se crei una regola con la classificazione `CriticalUpdates` e la configuri con un ritardo dell'approvazione automatica di 7 giorni, la nuova patch critica rilasciata il 7 gennaio verrà automaticamente approvata il 14 gennaio.

Se un repository Linux non fornisce informazioni sulla data di rilascio per pacchetti, Patch Manager utilizza il tempo di compilazione del pacchetto come la data dell'approvazione automatica per Amazon Linux 2, Amazon Linux 2023 e Red Hat Enterprise Linux (RHEL). Se non è possibile determinare il tempo di compilazione del pacchetto, Patch Manager utilizza una data predefinita del 1° gennaio 1970. Ciò comporta l'aggiornamento di qualsiasi specifica della data di approvazione automatica nelle baseline delle patch configurate per approvare le patch per qualsiasi data successiva al 1° gennaio 1970.

Quando si specifica una data limite di approvazione automatica, Patch Manager applica automaticamente tutte le patch rilasciate o aggiornate in data o precedente. Ad esempio, se si specifica il 7 luglio 2023 come data limite, nessuna patch rilasciata o aggiornata a partire dall'8 luglio 2023 verrà installata automaticamente.

Quando si crea una baseline delle patch personalizzata, è possibile specificare un livello di gravità di conformità per le patch approvate da quella baseline delle patch, ad esempio `Critical` o `High`. Se lo stato delle patch approvate viene riportato come `Missing`, la gravità di conformità complessiva riportata dalla baseline delle patch corrisponde al livello di gravità specificato.

Informazioni aggiuntive per la creazione di baseline delle patch

Quando crei una baseline delle patch, tieni presente quanto segue:

- Patch Manager fornisce una baseline delle patch predefinita per ogni sistema operativo supportato. Queste vengono utilizzate come baseline delle patch predefinite per ciascun tipo di sistema operativo, a meno che non si crei la propria baseline delle patch designandola come predefinita per il tipo di sistema operativo corrispondente.

Note

Per Windows Server, vengono fornite tre baseline delle patch predefinite. Le baseline delle patch `AWS-DefaultPatchBaseline` e `AWS-WindowsPredefinedPatchBaseline-OS` supportano solo gli aggiornamenti del sistema operativo Windows stesso. `AWS-DefaultPatchBaseline` viene utilizzato come baseline delle patch di default per nodi gestiti Windows Server a meno che non si specifichi una baseline delle patch diversa. Le impostazioni di configurazione in queste due baseline delle patch sono le stesse. Il più recente dei due, `AWS-WindowsPredefinedPatchBaseline-OS`, è stato creato per distinguerlo dalla terza baseline delle patch predefinita per Windows Server. Quella baseline delle patch, `AWS-WindowsPredefinedPatchBaseline-OS-Applications`, può essere utilizzata per applicare patch sia nel sistema operativo Windows Server che nelle applicazioni supportate rilasciate da Microsoft.

- Per impostazione predefinita, Windows Server 2019 e Windows Server 2022 rimuovono gli aggiornamenti che vengono sostituiti da quelli successivi. Di conseguenza, quando si utilizza il parametro `ApproveUntilDate` in una baseline delle patch di Windows Server, ma la data selezionata nel parametro `ApproveUntilDate` è precedente alla data dell'ultima patch, allora la nuova patch non viene installata durante l'operazione di applicazione. Per ulteriori informazioni sulle regole dell'applicazione di patch di Windows Server, consulta la scheda Windows Server su [Come vengono selezionate le patch di sicurezza](#).

Ciò significa che il nodo gestito è conforme in termini di operazioni di Systems Manager, anche nel caso in cui una patch critica del mese precedente non sia installata. Lo stesso scenario potrebbe

verificarsi quando si utilizza il parametro `ApproveAfterDays`. A causa del comportamento delle patch sostituite da Microsoft, è possibile impostare un numero (in genere superiore a 30 giorni) in modo che le patch per Windows Server non vengano mai installate quando l'ultima patch disponibile di Microsoft viene rilasciata prima che sia trascorso il numero di giorni su `ApproveAfterDays`.

- Solo per Windows Server, una patch di aggiornamento di sicurezza disponibile non approvata dalla baseline delle patch può avere un valore di conformità pari a `Compliant` o `Non-Compliant`, come definito in una baseline della patch personalizzata.

Quando si crea o si aggiorna una baseline delle patch, si sceglie lo stato da assegnare alle patch di sicurezza disponibili ma non approvate, perché non soddisfano i criteri di installazione specificati nella baseline delle patch. Ad esempio, le patch di sicurezza che si desidera installare possono essere ignorate se è stato specificato un lungo periodo di attesa dopo il rilascio di una patch prima dell'installazione. Se un aggiornamento della patch viene rilasciato durante il periodo di attesa specificato, il periodo di attesa per l'installazione della patch ricomincia da capo. Se il periodo di attesa è troppo lungo, è possibile che più versioni della patch vengano rilasciate e mai installate.

Utilizzando la console per creare o aggiornare una baseline delle patch, si specifica questa opzione nel campo Stato di conformità degli aggiornamenti di sicurezza disponibili. Utilizzando il [update-patch-baseline](#) comando AWS CLI to run the [create-patch-baseline](#) or, si specifica questa opzione nel `available-security-updates-compliance-status` parametro.

- Per server e macchine virtuali on-premises, Patch Manager tenta di utilizzare la baseline delle patch predefinita personalizzata. Se non è disponibile alcuna baseline delle patch predefinita personalizzata, il sistema utilizza quella predefinita per il sistema operativo corrispondente.
- Se una patch è specificata come approvata e rifiutata nella stessa baseline delle patch, viene rifiutata.
- Un nodo gestito può avere solo una baseline delle patch definita.
- I formati dei nomi dei pacchetti che possono essere aggiunti agli elenchi delle patch approvate e di quelle rifiutate per una baseline delle patch dipendono dal tipo di sistema operativo a cui si applicano le patch.

Per informazioni sui formati accettati per gli elenchi delle patch approvate e di quelle rifiutate, consulta [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#).

- Se utilizzi una [configurazione della policy di patch](#) in Quick Setup, gli aggiornamenti apportati alle baseline delle patch personalizzate vengono sincronizzati con Quick Setup una volta ogni ora.

Quando si elimina una baseline delle patch personalizzata a cui si fa riferimento in una policy di patch, viene visualizzato un banner nella pagina Dettagli di configurazione di Quick Setup relativa alla policy di patch. Il banner informa che la policy di patch fa riferimento a una baseline delle patch che non esiste più, di conseguenza le successive operazioni di applicazione di patch avranno esito negativo. In questo caso, torna alla pagina Configurazioni di Quick Setup, seleziona la configurazione Patch Manager e scegli Operazioni, Modifica configurazione. Il nome della baseline delle patch eliminata viene evidenziato ed è necessario selezionare una nuova baseline delle patch per il sistema operativo interessato.

- Quando si crea una regola di approvazione con valori `Classification` e `Severity` multipli, le patch vengono approvate in base agli attributi disponibili. I pacchetti con entrambi gli attributi `Classification` e `Severity` corrisponderanno ai valori della baseline selezionati per entrambi i campi. I pacchetti dotati solo di attributi `Classification` vengono confrontati solo con i valori `Classification` della baseline selezionati. I requisiti di gravità indicati nella stessa regola vengono ignorati per i pacchetti che non dispongono di attributi `Severity`.

Per informazioni sulla creazione di una baseline delle patch, consulta [Utilizzo delle baseline delle patch personalizzate](#) e [Tutorial: applicare patch a un ambiente server utilizzando AWS CLI](#).

Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate

I formati dei nomi dei pacchetti che è possibile aggiungere agli elenchi delle patch approvate e di quelle rifiutate dipendono dal tipo di sistema operativo a cui stai applicando le patch.

Formati dei nomi dei pacchetti per sistemi operativi Linux

I formati che è possibile specificare per le patch approvate e rifiutate della baseline delle patch variano in base al tipo di sistema operativo Linux. Più precisamente, i formati supportati dipendono dal programma di gestione dei pacchetti utilizzati dal tipo di sistema operativo Linux.

Amazon Linux 2, Amazon Linux 2023, Oracle Linux e Red Hat Enterprise Linux (RHEL)

Gestore dei pacchetti: YUM, ad eccezione di Amazon Linux 2023 e RHEL 8, che utilizzano DNF come gestore di pacchetti.

Patch approvate: per le patch approvate, è possibile specificare uno qualsiasi dei seguenti:

- ID Bugzilla, nel formato 1234567 (come ID Bugzilla, il sistema elabora stringhe numeriche).
- ID CVE, nel formato CVE-2018-1234567

- ID consultivi, in formati quali `RHSA-2017:0864`, `ALAS-2018-123`, `ALAS2023-2025-123`, e `ELSA-2025-123`
- Nomi di pacchetto creati utilizzando uno o più componenti disponibili per la denominazione dei pacchetti. A titolo illustrativo, per il pacchetto denominato `dbus.x86_64:1:1.12.28-1.amzn2023.0.1`, i componenti sono i seguenti:
 - `name: dbus`
 - `architecture: x86_64`
 - `epoch: 1`
 - `version: 1.12.28`
 - `release: 1.amzn2023.0.1`

Sono supportati i nomi di pacchetto con le seguenti costruzioni:

- `name`
- `name.arch`
- `name-version`
- `name-version-release`
- `name-version-release.arch`
- `version`
- `version-release`
- `epoch:version-release`
- `name-epoch:version-release`
- `name-epoch:version-release.arch`
- `epoch:name-version-release.arch`
- `name.arch:epoch:version-release`

Alcuni esempi:

- `dbus.x86_64`
- `dbus-1.12.28`
- `dbus-1.12.28-1.amzn2023.0.1`
- `dbus-1:1.12.28-1.amzn2023.0.1.x86_64`

- ~~Supportiamo anche i componenti dei nomi dei pacchetti con una singola wild card nei formati precedenti, come i seguenti:~~

- `dbus*`
- `dbus-1.12.2*`
- `dbus-*:1.12.28-1.amzn2023.0.1.x86_64`

Patch rifiutate: per le patch rifiutate, è possibile specificare uno qualsiasi dei seguenti:

- Nomi di pacchetto creati utilizzando uno o più componenti disponibili per la denominazione dei pacchetti. A titolo illustrativo, per il pacchetto denominato `dbus.x86_64:1:1.12.28-1.amzn2023.0.1`, i componenti sono i seguenti:
 - `name: dbus`
 - `architecture: x86_64`
 - `epoch: 1`
 - `version: 1.12.28`
 - `release: 1.amzn2023.0.1`

Sono supportati i nomi di pacchetto con le seguenti costruzioni:

- `name`
- `name.arch`
- `name-version`
- `name-version-release`
- `name-version-release.arch`
- `version`
- `version-release`
- `epoch:version-release`
- `name-epoch:version-release`
- `name-epoch:version-release.arch`
- `epoch:name-version-release.arch`
- `name.arch:epoch:version-release`

Alcuni esempi:

- `dbus.x86_64`
- `dbus-1.12.28`

- `dbus-1.12.28-1.amzn2023.0.1`
- `dbus-1:1.12.28-1.amzn2023.0.1.x86_64`
- Supportiamo anche i componenti dei nomi dei pacchetti con una sola jolly nei formati precedenti, come i seguenti:
 - `dbus*`
 - `dbus-1.12.2*`
 - `dbus-*:1.12.28-1.amzn2023.0.1.x86_64`

Debian Server and Ubuntu Server

Programma di gestione dei pacchetti: APT

Patch approvate e patch rifiutate: per le patch approvate e rifiutate, specifica quanto segue:

- Nomi dei pacchetti, nel formato `ExamplePkg33`

Note

Per gli elenchi di Debian Server e Ubuntu Server, non includere elementi come architettura o versioni. Ad esempio, è possibile specificare il nome del pacchetto `ExamplePkg33` per includere quanto riportato di seguito in un elenco delle patch:

- `ExamplePkg33.x86.1`
- `ExamplePkg33.x86.2`
- `ExamplePkg33.x64.1`
- `ExamplePkg33.3.2.5-364.noarch`

SUSE Linux Enterprise Server (SLES)

Programma di gestione dei pacchetti: Zypper

Patch approvate e patch rifiutate: per gli elenchi delle patch approvate e rifiutate, è possibile specificare uno qualsiasi dei seguenti:

- Nomi completi dei pacchetti, in formati quali:
 - `SUSE-SLE-Example-Package-15-2023-123`

- `example-pkg-2023.15.4-46.17.1.x86_64.rpm`
- Nomi dei pacchetti con un singolo carattere jolly, come:
 - `SUSE-SLE-Example-Package-15-2023-*`
 - `example-pkg-2023.15.4-46.17.1.*.rpm`

Formati dei nomi dei pacchetti per macOS

Gestori di pacchetti supportati: aggiornamento software, installatore, Brew, Brew Cask

Patch approvate e patch rifiutate: per gli elenchi delle patch approvate e rifiutate, è possibile specificare i nomi completi dei pacchetti, in formati come:

- `XProtectPlistConfigData`
- `MRTConfigData`

I caratteri jolly non sono supportati dagli elenchi delle patch approvate e rifiutate per macOS.

Formati dei nomi dei pacchetti per sistemi operativi Windows

Per i sistemi operativi Windows, specifica le patch utilizzando gli ID di Microsoft Knowledge Base e gli ID di Microsoft Security Bulletin. Ad esempio:

`KB2032276, KB2124261, MS10-048`

Gruppi di patch

Note

I gruppi di patch non vengono utilizzati nelle operazioni di applicazione di patch basate su policy di patch. Per informazioni sull'utilizzo delle policy di patch, consulta [Configurazioni delle policy sulle patch in Configurazione rapida](#).

La funzionalità dei gruppi di patch non è supportata nella console per le coppie account-Regione, che non utilizzavano già i gruppi di patch prima del rilascio del supporto per le policy di patch il 22 dicembre 2022. La funzionalità dei gruppi di patch è ancora disponibile nelle coppie account-Regione, che hanno iniziato a utilizzare i gruppi di patch prima di questa data.

È possibile utilizzare un gruppo di patch per associare i nodi gestiti a una specifica baseline di patch in Patch Manager. I gruppi di patch aiutano a garantire la distribuzione delle patch appropriate, in base alle regole di base delle patch associate, nel set di nodi corretto. Inoltre aiutano a non distribuire le patch non adeguatamente verificate. Ad esempio, è possibile creare gruppi di patch per ambienti diversi (di sviluppo, di test e di produzione) e registrare ciascun gruppo con una baseline delle patch appropriata.

Quando si esegue `AWS-RunPatchBaseline` o altri documenti del comando SSM per l'applicazione di patch è possibile definire come target i nodi gestiti tramite il relativo ID nodo o i tag. SSM Agent e Patch Manager quindi valutano quale baseline delle patch utilizzare in base al valore del gruppo di patch aggiunto al nodo gestito.

Utilizzo dei tag per definire i gruppi di patch

Crea un gruppo di patch utilizzando tag applicati sia alle tue istanze Amazon Elastic Compute Cloud (Amazon EC2) sia ai nodi non EC2 in un ambiente [ibrido e multi-cloud](#). Notare i seguenti dettagli relativi all'utilizzo dei tag per i gruppi di patch:

- Un gruppo di patch deve essere definito utilizzando la chiave tag `Patch Group` o `PatchGroup` applicati ai nodi gestiti. Quando si registra un gruppo di patch per una baseline delle patch, tutti i valori identici specificati per queste due chiavi vengono interpretati come parte dello stesso gruppo. Ad esempio, supponiamo di aver taggato cinque nodi con la prima delle seguenti coppie chiave-valore e cinque con la seconda:
 - `key=PatchGroup,value=DEV`
 - `key=Patch Group,value=DEV`

Il comando Patch Manager per creare una baseline combina questi 10 nodi gestiti in un unico gruppo in base al valore DEV. La AWS CLI equivalente del comando per creare una baseline delle patch per i gruppi di patch è la seguente:

```
aws ssm register-patch-baseline-for-patch-group \
  --baseline-id pb-0c10e65780EXAMPLE \
  --patch-group DEV
```

La combinazione di valori di chiavi diverse in un'unica destinazione è esclusiva di questo comando Patch Manager per la creazione di un nuovo gruppo di patch e non è supportata da altre operazioni API. Ad esempio, se esegui operazioni [send-command](#) utilizzando chiavi `PatchGroup` e `Patch Group` con gli stessi valori, stai definendo come target due set di nodi completamente diversi:

```
aws ssm send-command \  
  --document-name AWS-RunPatchBaseline \  
  --targets "Key=tag:PatchGroup,Values=DEV"
```

```
aws ssm send-command \  
  --document-name AWS-RunPatchBaseline \  
  --targets "Key=tag:Patch Group,Values=DEV"
```

- Esistono dei limiti alla definizione di target basata su tag. Ogni array di destinazioni per SendCommand può contenere un massimo di cinque coppie chiave-valore.
- Ti consigliamo di scegliere solo una di queste convenzioni relative alle chiavi dei tag, PatchGroup (senza spazio) o Patch Group (con uno spazio). Tuttavia, se sono presenti [tag consentiti nei metadati dell'istanza EC2](#), è necessario utilizzare PatchGroup (senza spazio).
- La chiave prevede la distinzione fra lettere maiuscole e minuscole. Puoi specificare qualsiasi valore per aiutarti a identificare e indirizzare le risorse di quel gruppo, ad esempio «server web» o "US-EAST-PROD«, ma la chiave deve essere o. Patch Group PatchGroup

Dopo avere creato un gruppo di patch e i nodi gestiti dei tag, è possibile registrare il gruppo di patch in una baseline delle patch. La registrazione del gruppo di patch con una baseline delle patch garantisce che i nodi all'interno del gruppo di patch utilizzino le regole definite nella baseline delle patch associata.

Per ulteriori informazioni su come creare un gruppo di patch e associarlo a una baseline delle patch, consulta [Creazione e gestione di gruppi di patch](#) e [Aggiungere un gruppo di patch a una baseline delle patch](#).

Per visualizzare un esempio di creazione di una baseline delle patch e di gruppi di patch con AWS Command Line Interface (AWS CLI), consulta [Tutorial: applicare patch a un ambiente server utilizzando AWS CLI](#). Per ulteriori informazioni sui tag Amazon EC2, consulta la sezione [Assegnazione di tag alle risorse Amazon EC2](#) nella Guida per l'utente di Amazon EC2.

Come funziona

Quando il sistema esegue l'attività di applicazione di una baseline delle patch a un nodo gestito, SSM Agent verifica che per il nodo sia definito un valore del gruppo di patch. Se il nodo è assegnato a un gruppo di patch, Patch Manager verifica quale baseline delle patch è stata registrata per il gruppo. Se per il gruppo viene rilevata una baseline delle patch, Patch Manager notifica a SSM

Agent di utilizzare la baseline delle patch associata. Se un nodo non è configurato per un gruppo di patch, Patch Manager comunica automaticamente a SSM Agent di utilizzare la baseline delle patch predefinita attualmente configurata.

⚠ Important

Un nodo gestito può trovarsi solo in un singolo gruppo di patch.

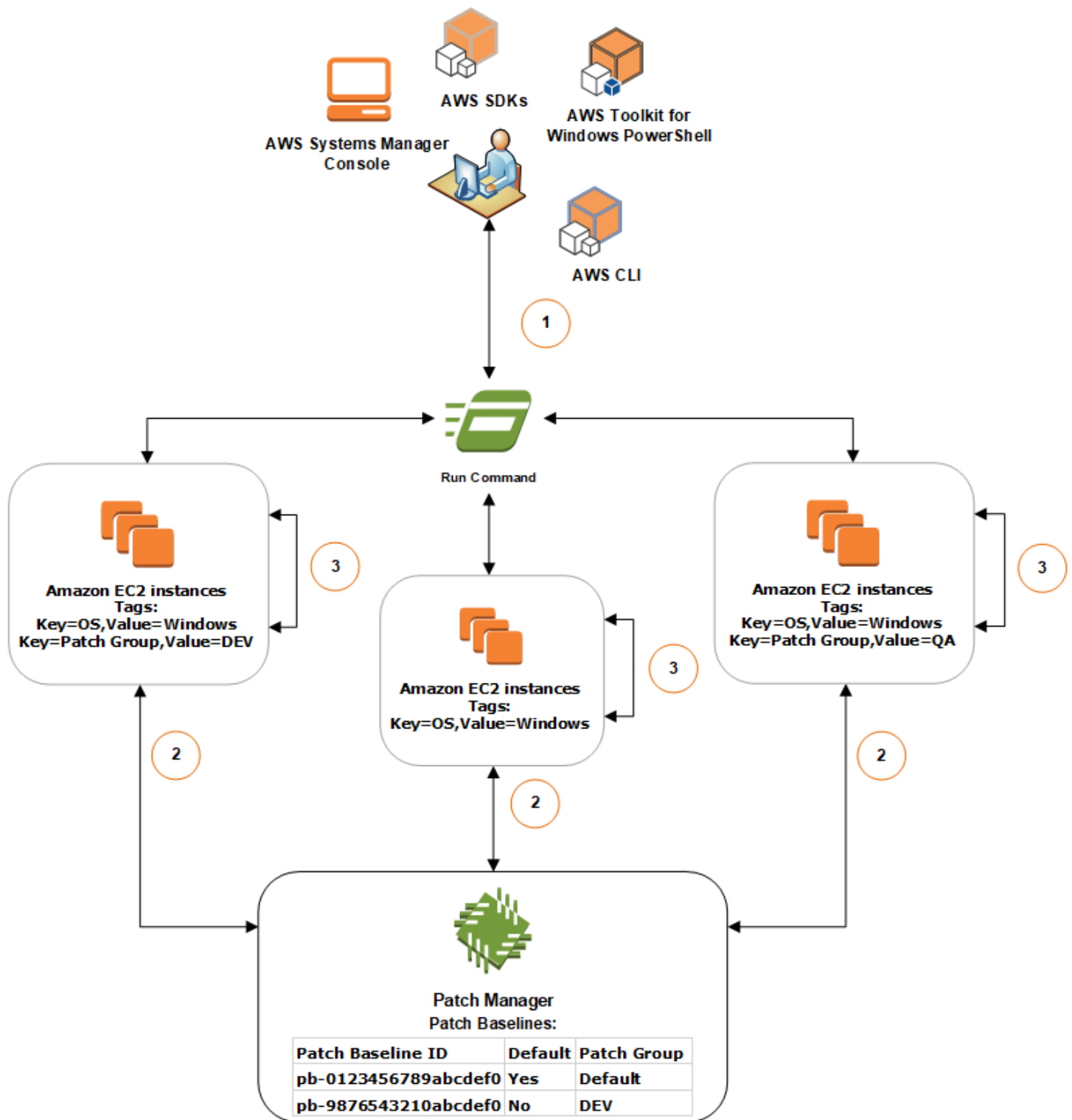
Un gruppo di patch può essere registrato con una sola baseline delle patch per ciascun tipo di sistema operativo.

Per applicare il tag Patch Group (con uno spazio) a un'istanza di Amazon EC2, l'opzione Consenti i tag nei metadati dell'istanza non deve essere abilitata sull'istanza. Consenti i tag nei metadati di istanza impedisce ai nomi delle chiavi dei tag di contenere spazi. Se hai [tag consentiti nei metadati dell'istanza EC2](#), è necessario utilizzare la chiave di tag PatchGroup (senza spazio).

Diagramma 1: esempio generale del flusso di elaborazione delle operazioni di applicazione di patch

L'immagine seguente mostra un esempio generale dei processi eseguiti da Systems Manager quando invia un'attività Run Command al parco di server per applicare le patch utilizzando Patch Manager. Questi processi determinano quali baseline delle patch utilizzare nelle operazioni di patch. (Un processo analogo viene utilizzato quando una finestra di manutenzione viene configurata per l'invio di un comando di applicazione patch utilizzando Patch Manager.)

L'intero processo è spiegato sotto l'illustrazione.



In questo esempio abbiamo tre gruppi di istanze EC2 di Windows Server con i seguenti tag applicati:

Gruppo di istanze EC2	Tag
Gruppo 1	key=OS,value=Windows
	key=PatchGroup,value=DEV
Gruppo 2	key=OS,value=Windows
Gruppo 3	key=OS,value=Windows
	key=PatchGroup,value=QA

Per questo esempio abbiamo anche le due baseline delle patch Windows Server seguenti:

ID della base di confronto delle patch	Predefinita	Gruppo di patch associate
pb-0123456789abcdef0	Sì	Default
pb-9876543210abcdef0	No	DEV

Il processo generale per la scansione o l'installazione di patch con Run Command, uno strumento di AWS Systems Manager, e Patch Manager è il seguente:

1. Invia un comando alla patch: utilizza la console di Systems Manager, SDK, AWS Command Line Interface (AWS CLI) o AWS Tools for Windows PowerShell per inviare un'Run Commandattività utilizzando il documentoAWS-RunPatchBaseline. Il diagramma mostra un'attività Run Command per l'applicazione di patch alle istanze gestite specificando come target il tag `key=OS,value=Windows`.
2. Determinazione della baseline delle patch: SSM Agent verifica i tag del gruppo di patch applicati all'istanza di EC2 e interroga Patch Manager per la baseline delle patch corrispondente.
 - Valore del gruppo di patch corrispondente associato alla baseline delle patch:
 1. SSM Agent, installato nelle istanze EC2 nel gruppo 1, riceve il comando eseguito nella Fase 1 di avviare un'operazione di applicazione di patch. SSM Agent verifica che alle istanze EC2 sia applicato il valore di tag del gruppo di patch DEV e interroga Patch Manager per ottenere una baseline delle patch associata.

2. Patch Manager verifica che alla baseline delle patch `pb-9876543210abcdef0` sia associato il gruppo di patch DEV e invia una notifica a SSM Agent.
 3. SSM Agent recupera uno snapshot della baseline delle patch da Patch Manager in base alle regole di approvazione e alle eccezioni configurate in `pb-9876543210abcdef0` e procede con la fase successiva.
- Nessun tag del gruppo di patch aggiunto all'istanza:
 1. SSM Agent, installato nelle istanze EC2 nel gruppo 2, riceve il comando eseguito nella Fase 1 di avviare un'operazione di applicazione di patch. SSM Agent verifica che alle istanze EC2 non sia applicato il tag Patch Group e PatchGroup, di conseguenza, SSM Agent interroga Patch Manager per ottenere la baseline delle patch Windows predefinita.
 2. Patch Manager verifica che la baseline delle patch predefinita Windows Server sia `pb-0123456789abcdef0` e notifica SSM Agent.
 3. SSM Agent recupera uno snapshot della baseline delle patch da Patch Manager in base alle regole di approvazione e alle eccezioni configurate nella baseline delle patch predefinita `pb-0123456789abcdef0` e procede con la fase successiva.
 - Nessun valore del gruppo di patch corrispondente associato a una baseline delle patch:
 1. SSM Agent, installato nelle istanze EC2 nel gruppo 3, riceve il comando eseguito nella Fase 1 di avviare un'operazione di applicazione di patch. SSM Agent verifica che alle istanze EC2 sia applicato il valore di tag QA del gruppo di patch e interroga Patch Manager per ottenere una baseline delle patch associata.
 2. Patch Manager non trova una baseline delle patch a cui sia associato il gruppo di patch QA.
 3. Patch Manager comunica a SSM Agent di utilizzare la baseline delle patch predefinita di Windows `pb-0123456789abcdef0`.
 4. SSM Agent recupera uno snapshot della baseline delle patch da Patch Manager in base alle regole di approvazione e alle eccezioni configurate nella baseline delle patch predefinita `pb-0123456789abcdef0` e procede con la fase successiva.
3. Scansione o installazione di patch: dopo aver stabilito la baseline delle patch appropriata da utilizzare, SSM Agent inizia a eseguire la scansione o l'installazione delle patch in base al valore dell'operazione specificato nella Fase 1. Per stabilire quali patch devono essere sottoposte a scansione o installate, vengono seguite le regole di approvazione e le eccezioni delle patch definite nella snapshot della baseline delle patch fornita da Patch Manager.

Ulteriori informazioni

- [Valori dello stato di conformità delle patch](#)

Applicazioni di patch rilasciate da Microsoft il Windows Server

Usa le informazioni contenute in questo argomento per prepararti a applicare patch alle applicazioni in fase di Windows Server utilizzo Patch Manager.

Applicazione di patch alle applicazioni Microsoft

Il supporto per l'applicazione di patch per le applicazioni sui nodi gestiti da Windows Server è limitato alle applicazioni rilasciate da Microsoft.

Note

In alcuni casi, Microsoft rilascia patch per applicazioni che non specificano una data e un'ora aggiornate. In questi casi, una data e un'ora aggiornate di 01/01/1970 viene fornito per impostazione predefinita.

Baseline delle patch per applicare patch alle applicazioni rilasciate da Microsoft

Per Windows Server, vengono fornite tre baseline delle patch predefinite. Le baseline delle patch AWS-DefaultPatchBaseline e AWS-WindowsPredefinedPatchBaseline-OS supportano solo gli aggiornamenti del sistema operativo Windows stesso. AWS-DefaultPatchBaselineViene utilizzato come baseline delle patch di default per nodi gestiti Windows Server a meno che non si specifichi una baseline delle patch diversa. Le impostazioni di configurazione in queste due baseline delle patch sono le stesse. Il più recente dei due, AWS-WindowsPredefinedPatchBaseline-OS, è stato creato per distinguerlo dalla terza baseline delle patch predefinita per Windows Server. Quella baseline delle patch, AWS-WindowsPredefinedPatchBaseline-OS-Applications, può essere utilizzata per applicare patch sia nel sistema operativo Windows Server che nelle applicazioni supportate rilasciate da Microsoft.

È anche possibile creare una baseline delle patch personalizzata per aggiornare le applicazioni Microsoft su macchine Windows Server

Supporto per le applicazioni di patch rilasciate da Microsoft nei server on-premises, nei dispositivi edge, nelle macchine virtuali e in altri nodi non EC2

È possibile applicare patch alle applicazioni rilasciate da Microsoft su macchine virtuali (VM) e altri nodi gestiti non EC2. Patch Manager utilizza prezzi con pagamento in base al consumo se utilizzato su nodi gestiti ibridi. Per ulteriori informazioni sui prezzi, consulta [Prezzi di AWS Systems Manager](#).

Opzione di aggiornamento di Windows per “altri prodotti Microsoft”

Per Patch Manager poter applicare patch alle applicazioni rilasciate da Microsoft sui nodi Windows Server gestiti, l'opzione di Windows Update Dammi aggiornamenti per altri prodotti Microsoft quando aggiorno Windows deve essere attivata sul nodo gestito.

Per informazioni sull'abilitazione di questa opzione su un singolo nodo gestito, vedere [Aggiornare Office con Microsoft Update](#) nel sito Web del Support Microsoft.

Per un parco istanze di nodi gestiti che esegue Windows Server 2016 e versioni successive, è possibile utilizzare un oggetto Policy di gruppo (GPO) per attivare l'impostazione. Nell'Editor Gestione Policy di gruppo, accedere a Configurazione computer, Modelli amministrativi, Componenti di Windows, Aggiornamenti di Windows e scegliere Installare gli aggiornamenti per altri prodotti Microsoft. Si consiglia inoltre di configurare il GPO con parametri aggiuntivi che impediscano aggiornamenti automatici non pianificati e riavvii al di fuori di Patch Manager. Per ulteriori informazioni, vedi [Configurazione degli aggiornamenti automatici in un ambiente](#) di Non-Active directory nel sito Web della documentazione tecnica Microsoft.

Per un parco di nodi gestiti che eseguono Windows Server 2012 o 2012 R2, è possibile attivare l'opzione utilizzando uno script, come descritto in [Abilitazione e disattivazione di Microsoft Update in Windows 7 tramite Script nel](#) sito Web Microsoft Docs Blog. Ad esempio, è possibile eseguire le operazioni seguenti:

1. Salvare lo script dal post del blog in un file.
2. Caricare il file in un bucket Amazon Simple Storage Service (Amazon S3) o in un'altra posizione accessibile.
3. Run CommandConsente di eseguire lo script sui nodi gestiti utilizzando il documento Systems Manager (documento SSM) AWS-RunPowerShellScript con un comando simile al seguente.

```
Invoke-WebRequest `
  -Uri "https://s3.aws-api-domain/amzn-s3-demo-bucket/script.vbs" `
  -Outfile "C:\script.vbs" cscript c:\script.vbs
```

Requisiti minimi dei parametri

Per includere le applicazioni rilasciate da Microsoft nella baseline delle patch personalizzata, è necessario almeno specificare il prodotto a cui si desidera applicare le patch. Il comando seguente AWS Command Line Interface (AWS CLI) illustra i requisiti minimi per applicare le patch a un prodotto, come Microsoft Office 2016.

Linux & macOS

```
aws ssm create-patch-baseline \  
  --name "My-Windows-App-Baseline" \  
  --approval-rules  
  "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=PRODUCT,Values='Office 2016'},  
{Key=PATCH_SET,Values='APPLICATION'}}],ApproveAfterDays=5}]"
```

Windows Server

```
aws ssm create-patch-baseline ^  
  --name "My-Windows-App-Baseline" ^  
  --approval-rules  
  "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=PRODUCT,Values='Office 2016'},  
{Key=PATCH_SET,Values='APPLICATION'}}],ApproveAfterDays=5}]"
```

Se si specifica la famiglia di prodotti applicativi Microsoft, ogni prodotto specificato deve essere un membro supportato della famiglia di prodotti selezionata. Ad esempio, per l'applicazione di patch al prodotto "Active Directory Rights Management Services Client 2.0", è necessario specificare la famiglia di prodotti come "Active Directory" e non, ad esempio "Office" o "SQL Server". Il AWS CLI comando seguente dimostra una combinazione abbinata di famiglia di prodotti e prodotto.

Linux & macOS

```
aws ssm create-patch-baseline \  
  --name "My-Windows-App-Baseline" \  
  --approval-rules  
  "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=PRODUCT_FAMILY,Values='Active  
Directory'},{Key=PRODUCT,Values='Active Directory Rights Management Services Client  
2.0'},{Key=PATCH_SET,Values='APPLICATION'}}],ApproveAfterDays=5}]"
```

Windows Server

```
aws ssm create-patch-baseline ^  
  --name "My-Windows-App-Baseline" ^
```

```
--approval-rules
"PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=PRODUCT_FAMILY,Values='Active
Directory'},{Key=PRODUCT,Values='Active Directory Rights Management Services Client
2.0'},{Key=PATCH_SET,Values='APPLICATION'}]}],ApproveAfterDays=5}]"
```

Note

Se viene visualizzato un messaggio di errore relativo a un prodotto e una famiglia non corrispondenti, consulta [Problema: coppie di prodotti family/product non corrispondenti](#) per assistenza nella risoluzione del problema.

Utilizzo Applicazione di patch live del kernel su nodi gestiti Amazon Linux 2

Kernel Live Patching per Amazon Linux 2 ti consente di applicare vulnerabilità di sicurezza e patch di bug critici a un kernel Linux in esecuzione senza riavvii o interruzioni delle applicazioni in esecuzione. Ciò ti consente di beneficiare di una migliore disponibilità di servizi e applicazioni, mantenendo al contempo la tua infrastruttura sicura e aggiornata. Kernel Live Patching è supportato su istanze Amazon EC2, dispositivi AWS IoT Greengrass principali e macchine virtuali [locali che](#) eseguono Amazon Linux 2.

Per informazioni generali su Kernel Live Patching, consulta [Kernel Live Patching su AL2](#) nella Guida per l'utente di Amazon Linux 2.

Dopo aver Kernel Live Patching attivato un nodo gestito di Amazon Linux 2, puoi utilizzarlo Patch Manager per applicare le patch live del kernel al nodo gestito. L'utilizzo di Patch Manager per applicare gli aggiornamenti è un'alternativa ai flussi di lavoro yum nel nodo.

Prima di iniziare

Patch Manager Per applicare le patch live del kernel ai nodi gestiti di Amazon Linux 2, assicurati che i nodi siano basati sull'architettura e sulla versione del kernel corrette. Per informazioni, consulta [Configurazioni e prerequisiti supportati](#) nelle istanze Guida per l'utente di Amazon EC2.

Applicazione di patch live del kernel utilizzo di Patch Manager

Aggiornamento della versione del kernel

Non è necessario riavviare un nodo gestito dopo aver applicato un aggiornamento della patch live del kernel. Tuttavia, AWS fornisce patch live del kernel per una versione del kernel di Amazon

Linux 2 per un massimo di tre mesi dopo il suo rilascio. Dopo il periodo di tre mesi, è necessario eseguire l'aggiornamento a una versione del kernel successiva per continuare a ricevere patch live del kernel. Ti consigliamo di utilizzare una finestra di manutenzione per pianificare un riavvio del nodo almeno una volta ogni tre mesi per richiedere l'aggiornamento della versione del kernel.

Disinstallazione delle patch live del kernel

Le patch live del kernel non possono essere disinstallate utilizzando Patch Manager. È possibile invece disabilitare Kernel Live Patching, che rimuove i pacchetti RPM per le patch live del kernel applicate. Per ulteriori informazioni, consulta [Spegnimento Applicazione di patch live del kernel utilizzo di Run Command](#).

Conformità del kernel

In alcuni casi, l'installazione di tutte le correzioni CVE dalle patch live per la versione corrente del kernel può far sì che il kernel sia stesso stato di conformità di una versione più recente. Quando ciò accade, la versione più recente viene segnalata come `Installed` e il nodo gestito restituito come `Compliant`. Tuttavia, non viene restituita l'ora di installazione per la versione più recente del kernel.

Una patch live del kernel, più CVE

Se una patch live del kernel risolve più CVE e queste CVE hanno diversi valori di classificazione e gravità, per la patch viene restituita solo la classificazione e la gravità più elevate tra le CVE.

Nella parte restante di questa sezione viene descritto come utilizzare Patch Manager per applicare patch live del kernel ai nodi gestiti che soddisfano questi requisiti.

In che modo Applicazione di patch live del kernel utilizzo di Patch Manager funzionamento

AWS rilascia due tipi di patch live del kernel per Amazon Linux 2: aggiornamenti di sicurezza e correzioni di bug. Per applicare questi tipi di patch, utilizzare un documento della baseline delle patch destinato solo alle classificazioni e alle severità elencate nella tabella seguente.

Classificazione	Gravità
Security	Critical, Important
Bugfix	All

È possibile creare una baseline delle patch personalizzata destinata solo a queste patch oppure utilizzare la baseline delle patch `AWS-AmazonLinux2DefaultPatchBaseline` predefinita. In altre parole, è possibile utilizzare `AWS-AmazonLinux2DefaultPatchBaseline` con i nodi gestiti Amazon Linux 2 in cui è abilitato Kernel Live Patching per applicare gli aggiornamenti live del kernel.

Note

La configurazione `AWS-AmazonLinux2DefaultPatchBaseline` specifica un periodo di attesa di 7 giorni dopo il rilascio o l'ultimo aggiornamento di una patch prima dell'installazione automatica. Se non si desidera attendere 7 giorni per l'approvazione automatica delle patch live del kernel, è possibile creare e utilizzare una baseline delle patch personalizzata. Nella baseline delle patch, è possibile specificare nessun periodo di attesa per l'approvazione automatica o specificarne uno più breve o più lungo. Per ulteriori informazioni, consulta [Utilizzo delle baseline delle patch personalizzate](#).

Ti consigliamo la seguente strategia per applicare patch ai nodi gestiti con aggiornamenti live del kernel:

1. Attiva Kernel Live Patching sui nodi gestiti Amazon Linux 2.
2. Run CommandDa utilizzare per eseguire un'operazione Scan sui nodi gestiti utilizzando una baseline di patch predefinita `AWS-AmazonLinux2DefaultPatchBaseline` o personalizzata che riguardi anche solo gli Security aggiornamenti con gravità classificata come `Critical` e `Important` gravità di `Bugfix All`.
3. Usa Compliance per verificare se la non conformità per l'applicazione delle patch viene segnalata per uno qualsiasi dei nodi gestiti che sono stati scansionati. In caso affermativo, visualizza i dettagli della conformità del nodo per determinare se alcune patch live del kernel mancano dal nodo gestito.
4. Per installare patch live del kernel mancanti, utilizza Run Command con la stessa baseline delle patch specificata in precedenza, ma questa volta esegui un'operazione `Install` invece di un'operazione `Scan`.

Poiché le patch live del kernel vengono installate senza la necessità di riavviare, è possibile scegliere l'opzione di riavvio `NoReboot` per questa operazione.

 Note

È comunque possibile riavviare il nodo gestito se necessario per altri tipi di patch installati nel nodo o se vuoi eseguire l'aggiornamento a un kernel più recente. In questi casi, scegli invece l'opzione di riavvio `RebootIfNeeded`.

5. Torna a Conformità per verificare che le patch live del kernel siano state installate.

Accensione Applicazione di patch live del kernel utilizzo di Run Command

Per attivare Kernel Live Patching, è possibile eseguire `yum` sui tuoi nodi gestiti o usare Run Command e un documento di Systems Manager personalizzato (documento SSM) creato dall'utente.

Per informazioni sull'attivazione di Kernel Live Patching eseguendo i comandi `yum` direttamente sul nodo gestito, vedi [Abilitazione Kernel Live Patching](#) nelle istanze Guida per l'utente di Amazon EC2.

 Note

Quando si attiva Kernel Live Patching, se il kernel già in esecuzione sul nodo gestito è precedente rispetto a `kernel-4.14.165-131.185.amzn2.x86_64` (la versione minima supportata), il processo installa l'ultima versione disponibile del kernel e riavvia il nodo gestito. Se il nodo sta già eseguendo `kernel-4.14.165-131.185.amzn2.x86_64` o versione successiva, il processo non installa una versione più recente e non riavvia il nodo.

Attivare Applicazione di patch live del kernel utilizzo di Run Command (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Run Command.
3. Seleziona Esegui comando.
4. Nell'elenco Documento di comando, scegliere il documento SSM personalizzato `AWS-ConfigureKernelLivePatching`.
5. Nella sezione Parametri di comando specifica se vuoi che i nodi gestiti vengano riavviati come parte di questa operazione.

6. Per informazioni sull'utilizzo dei controlli rimanenti in questa pagina, consulta [Esecuzione di comandi dalla console](#).
7. Scegli Esegui.

Per accendere Applicazione di patch live del kernel (AWS CLI)

- Esegui il comando seguente sul computer locale.

Linux & macOS

```
aws ssm send-command \  
  --document-name "AWS-ConfigureKernelLivePatching" \  
  --parameters "EnableOrDisable=Enable" \  
  --targets "Key=instanceids,Values=instance-id"
```

Windows Server

```
aws ssm send-command ^  
  --document-name "AWS-ConfigureKernelLivePatching" ^  
  --parameters "EnableOrDisable=Enable" ^  
  --targets "Key=instanceids,Values=instance-id"
```

Sostituiscilo *instance-id* con l'ID del nodo gestito di Amazon Linux 2 su cui desideri attivare la funzionalità, ad esempio I-02573CAFCFEXAMPLE. Per disabilitare la funzionalità su più nodi gestiti puoi utilizzare uno dei seguenti formati.

- --targets "Key=instanceids,Values=*instance-id1,instance-id2*"
- --targets "Key=tag:*tag-key*,Values=*tag-value*"

Per informazioni sulle altre opzioni che puoi utilizzare con il comando, consulta [send-command](#) in Riferimento ai comandi della AWS CLI .

Applicazione di patch live del kernel tramite Run Command

Per applicare patch live del kernel puoi eseguire comandi yum sui nodi gestiti o utilizzare Run Command e il documento SSMAWS-RunPatchBaseline.

Per informazioni sull'applicazione delle patch live del kernel eseguendo comandi yum direttamente sul nodo gestito, consulta [Applicazione delle patch live del kernel](#) nella Guida per l'utente di Amazon EC2.

Per applicare patch live del kernel utilizzando Run Command (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Run Command.
3. Seleziona Esegui comando.
4. Nell'elenco Documento comando, scegli il documento SSM AWS-RunPatchBaseline.
5. Nella sezione Parametri di comando esegui una delle operazioni seguenti:
 - Se devi verificare se sono disponibili nuove patch live del kernel, per Operazione scegli Scan. Per Opzione di riavvio, se non vuoi che i nodi gestiti vengano riavviati dopo questa operazione, scegli NoReboot. Al termine dell'operazione, puoi verificare la presenza di nuove patch e lo stato di conformità in Conformità.
 - Se hai già verificato la conformità delle patch e vuoi applicare le patch live del kernel disponibili, per Operazione scegli Install. Per Opzione di riavvio, se non desideri che i nodi gestiti vengano riavviati dopo questa operazione, scegli NoReboot.
6. Per informazioni sull'utilizzo dei controlli rimanenti in questa pagina, consulta [Esecuzione di comandi dalla console](#).
7. Scegli Esegui.

Per applicare patch live del kernel tramite Run Command (AWS CLI)

1. Per eseguire un'operazione Scan prima di controllare i risultati in Conformità , esegui il comando seguente dal computer locale.

Linux & macOS

```
aws ssm send-command \  
  --document-name "AWS-RunPatchBaseline" \  
  --targets "Key=InstanceIds,Values=instance-id" \  
  --parameters '{"Operation":["Scan"],"RebootOption":["RebootIfNeeded"]}'
```

Windows Server

```
aws ssm send-command ^
  --document-name "AWS-RunPatchBaseline" ^
  --targets "Key=InstanceIds,Values=instance-id" ^
  --parameters {"Operation":["Scan"],"RebootOption":["RebootIfNeeded"]} }
```

Per informazioni sulle altre opzioni che puoi utilizzare con il comando, consulta [send-command](#) in Riferimento ai comandi della AWS CLI .

2. Per eseguire un'operazione Install dopo aver verificato i risultati in Conformità , esegui il comando seguente dal computer locale.

Linux & macOS

```
aws ssm send-command \
  --document-name "AWS-RunPatchBaseline" \
  --targets "Key=InstanceIds,Values=instance-id" \
  --parameters '{"Operation":["Install"],"RebootOption":["NoReboot"]}'
```

Windows Server

```
aws ssm send-command ^
  --document-name "AWS-RunPatchBaseline" ^
  --targets "Key=InstanceIds,Values=instance-id" ^
  --parameters {"Operation":["Install"],"RebootOption":["NoReboot"]} }
```

In entrambi i comandi precedenti, sostituiscilo *instance-id* con l'ID del nodo gestito di Amazon Linux 2 su cui desideri applicare le patch live del kernel, come I-02573CAFCFExample. Per disabilitare la funzionalità su più nodi gestiti puoi utilizzare uno dei seguenti formati.

- --targets "Key=instanceids,Values=*instance-id1,instance-id2*"
- --targets "Key=tag:*tag-key*,Values=*tag-value*"

Per informazioni sulle altre opzioni che puoi utilizzare con questi comandi, consulta [send-command](#) in Riferimento ai comandi della AWS CLI .

Spegnimento Applicazione di patch live del kernel utilizzo di Run Command

Per abilitare Kernel Live Patching puoi eseguire comandi yum sui nodi gestiti o utilizzare Run Command e un documento SSM personalizzato AWS-ConfigureKernelLivePatching.

Note

Se non è più necessario utilizzare Kernel Live Patching, puoi disabilitarla in qualsiasi momento. Di solito, non è necessario disattivare la funzionalità.

Per informazioni sulla disattivazione di Kernel Live Patching eseguendo yum direttamente sul nodo gestito, consulta [AbilitazioneKernel Live Patching](#) nella Guida per l'utente di Amazon EC2.

Note

Quando si disattiva Kernel Live Patching, il processo disinstalla il plugin Kernel Live Patching e quindi riavvia il nodo gestito.

Per disattivare Applicazione di patch live del kernel utilizzo di Run Command (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Run Command.
3. Seleziona Esegui comando.
4. Nell'elenco Documento comando, scegli il documento SSM AWS-ConfigureKernelLivePatching.
5. Nella sezione Parametri di comando, specifica i valori per i parametri necessari.
6. Per informazioni sull'utilizzo dei controlli rimanenti in questa pagina, consulta [Esecuzione di comandi dalla console](#).
7. Scegli Esegui.

Per disattivare Applicazione di patch live del kernel (AWS CLI)

- Esegui un comando simile al seguente.

Linux & macOS

```
aws ssm send-command \  
  --document-name "AWS-ConfigureKernelLivePatching" \  
  --targets "Key=instanceIds,Values=instance-id" \  
  --parameters "EnableOrDisable=Disable"
```

Windows Server

```
aws ssm send-command ^  
  --document-name "AWS-ConfigureKernelLivePatching" ^  
  --targets "Key=instanceIds,Values=instance-id" ^  
  --parameters "EnableOrDisable=Disable"
```

Sostituiscilo *instance-id* con l'ID del nodo gestito di Amazon Linux 2 su cui desideri disattivare la funzionalità, ad esempio I-02573CAFCFEXAMPLE. Per disabilitare la funzionalità su più nodi gestiti puoi utilizzare uno dei seguenti formati.

- `--targets "Key=instanceids,Values=instance-id1,instance-id2"`
- `--targets "Key=tag:tag-key,Values=tag-value"`

Per informazioni sulle altre opzioni che puoi utilizzare con il comando, consulta [send-command](#) in Riferimento ai comandi della AWS CLI .

Lavorare con Patch Manager risorse e conformità utilizzando la console

Per utilizzarlo Patch Manager, completa le seguenti attività. Tali attività sono descritte in maggiore dettaglio più avanti in questa sezione.

1. Verifica che la patch di base AWS predefinita per ogni tipo di sistema operativo utilizzato soddisfi le tue esigenze. In caso contrario, creare una baseline delle patch che definisca un set di patch standard per quel tipo di nodo gestito e impostarla come di default.
2. Organizzare i nodi gestiti in gruppi di patch utilizzando i tag Amazon Elastic Compute Cloud (Amazon EC2) (facoltativo, ma consigliato).
3. Esegui una delle seguenti operazioni:

- (Consigliato) Configura una policy sulle patch in Quick Setup, che ti consenta di installare le patch mancanti in base a una pianificazione per un'intera organizzazione, un sottoinsieme di unità organizzative o una singola. Account AWS Per ulteriori informazioni, consulta [Configurare l'applicazione di patch per le istanze in un'organizzazione utilizzando un Configurazione rapida politica sulle patch](#).
 - Crea una finestra di manutenzione che utilizza il documento di Systems Manager (documento SSM) AWS-RunPatchBaseline in un tipo di attività Run Command. Per ulteriori informazioni, consulta [Tutorial: creazione di una finestra di manutenzione per l'applicazione di patch tramite console](#).
 - Esegui manualmente AWS-RunPatchBaseline in un'operazione Run Command. Per ulteriori informazioni, consulta [Esecuzione di comandi dalla console](#).
 - Applicare manualmente le patch ai nodi utilizzando la funzionalità on demand Applica subito una patch. Per ulteriori informazioni, consulta [Patching dei nodi gestiti on demand](#).
4. Monitorare l'applicazione di patch per verificare la conformità e analizzare gli errori.

Creazione di una policy di patch

Una policy sulle patch è una configurazione che puoi configurare utilizzando Quick Setup. Le policy di patch offrono un controllo più ampio e centralizzato sulle operazioni di applicazione di patch rispetto ad altri metodi precedenti. Una policy di patch definisce la pianificazione e la linea di base da utilizzare quando si applicano automaticamente le patch ai nodi e alle applicazioni.

Per ulteriori informazioni, consulta i seguenti argomenti:

- [Configurazioni delle policy sulle patch in Configurazione rapida](#)
- [Configurare l'applicazione di patch per le istanze in un'organizzazione utilizzando un Configurazione rapida politica sulle patch](#)

Visualizzazione dei riepiloghi del pannello di controllo delle patch

La scheda Dashboard Patch Manager offre una visualizzazione riassuntiva nella console che è possibile utilizzare per monitorare le operazioni di applicazione delle patch in una vista consolidata. Patch Manager è uno strumento in AWS Systems Manager. Sulla scheda Dashboard (Pannello di controllo) è possibile visualizzare le informazioni seguenti:

- Uno snapshot del numero di nodi gestiti conformi e non conformi alle regole di applicazione di patch.

- Uno snapshot dell'età dei risultati della conformità delle patch per i tuoi nodi gestiti.
- Conteggio collegato del numero di nodi gestiti non conformi presenti per ciascuno dei motivi più comuni di non conformità.
- Elenco collegato delle operazioni di applicazione di patch più recenti.
- Elenco collegato delle attività ricorrenti di applicazione patch impostate.

Visualizzazione dei riepiloghi del pannello di controllo delle patch

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Patch Manager.
3. Seleziona la scheda Pannello di controllo.
4. Scorrere fino alla sezione contenente i dati di riepilogo da visualizzare:
 - Amazon EC2 instance management (Gestione delle istanze Amazon EC2)
 - Compliance summary (Riepilogo della conformità)
 - Noncompliance counts (Conteggi delle non conformità)
 - Compliance reports (Report di conformità)
 - Non-patch operazioni basate su policy
 - Non-patch attività ricorrenti basate su politiche

Utilizzo dei report sulla conformità delle patch

Utilizza le informazioni contenute nei seguenti argomenti per generare e utilizzare i report di conformità delle patch in Patch Manager.

Le informazioni contenute negli argomenti seguenti sono valide indipendentemente dal metodo o dal tipo di configurazione utilizzato per le operazioni di applicazione di patch:

- Una policy di patch configurata in Quick Setup
- Un'opzione di gestione host configurata in Quick Setup
- Una finestra di manutenzione per eseguire un'attività Scan o Install di patch
- Un'operazione Applica subito una patch on demand

 Important

I report di conformità delle patch sono istantanee temporali generate solo da operazioni di patch riuscite. Ogni report contiene un orario di acquisizione che identifica quando è stato calcolato lo stato di conformità.

Se disponi di più tipi di operazioni per la scansione delle istanze al fine di verificarne la conformità delle patch, tieni presente che ogni scansione sovrascrive i dati di conformità delle patch delle scansioni precedenti. Di conseguenza, potresti ottenere risultati imprevisti nei dati di conformità delle patch. Per ulteriori informazioni, consulta [Identificazione dell'esecuzione che ha creato i dati di conformità delle patch](#).

Per verificare la baseline delle patch utilizzata per generare le informazioni di conformità più recenti, accedi alla scheda Report di conformità in Patch Manager, individua la riga relativa al nodo gestito per il quale desideri ottenere informazioni, quindi scegli l'ID di base nella colonna ID di base utilizzato.

Visualizzazione dei risultati di conformità delle patch

Utilizza queste procedure per visualizzare le informazioni sulla conformità delle patch relative ai nodi gestiti.

Questa procedura si applica alle operazioni delle patch che utilizzano il documento AWS-RunPatchBaseline. Per informazioni sulla visualizzazione delle informazioni di conformità di patch per le relative operazioni che utilizzano il documento AWS-RunPatchBaselineAssociation, consulta [Identificazione di nodi gestiti non conformi](#).

 Note

Le operazioni di scansione delle patch per Quick Setup e Explorer utilizzo del AWS-RunPatchBaselineAssociation documento. Quick Setup Explorer sono entrambi gli strumenti in AWS Systems Manager.

Identificare la soluzione di patch per un problema CVE specifico (Linux)

Per molti sistemi Linux-based operativi, i risultati della conformità delle patch indicano quali problemi del bollettino CVE (Common Vulnerabilities and Exposure) vengono risolti con quali patch. Queste informazioni consentono di determinare con quale urgenza è necessario installare una patch mancante o non riuscita.

I dettagli di CVE sono inclusi per le versioni supportate dei seguenti tipi di sistema operativo:

- AlmaLinux
- Amazon Linux 2
- Amazon Linux 2023
- Oracle Linux
- Red Hat Enterprise Linux (RHEL)
- Rocky Linux

 Note

Per impostazione predefinita, CentOS Stream non fornisce informazioni CVE sugli aggiornamenti. È possibile, tuttavia, consentire questo supporto utilizzando repository di terze parti, come il repository Extra Packages for Enterprise Linux (EPEL) pubblicato da Fedora. Per informazioni, consulta [EPEL](#) sul Wiki di Fedora. Attualmente, i valori dell'ID CVE vengono riportati solo per le patch con stato Missing o Failed.

È inoltre possibile aggiungere ID CVE agli elenchi di patch approvate o rifiutate nelle baseline delle patch, a condizione che la situazione e gli obiettivi di applicazione di patch lo richiedano.

Per informazioni sull'utilizzo di elenchi di patch approvate e rifiutate, consulta i seguenti argomenti:

- [Utilizzo delle baseline delle patch personalizzate](#)
- [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#)
- [Come funzionano le regole di base delle patch sui sistemi Linux-based](#)
- [Come vengono installate le patch](#)

 Note

In alcuni casi, Microsoft rilascia patch per applicazioni che non specificano una data e un'ora aggiornate. In questi casi, una data e un'ora aggiornate di 01/01/1970 viene fornito per impostazione predefinita.

Visualizzazione dei risultati della conformità delle patch

Utilizza le seguenti procedure per visualizzare i risultati di conformità delle patch nella console AWS Systems Manager .

Note

Per informazioni sulla generazione dei report di conformità alle patch che vengono scaricati in un bucket Amazon Simple Storage Service (Amazon S3), consulta [Generazione di report sulla conformità delle patch csv](#).

Visualizzazione dei risultati della conformità delle patch

1. Scegli una delle seguenti operazioni.

Opzione 1 (consigliata): naviga da Patch Manager, uno strumento di AWS Systems Manager:

- Nel pannello di navigazione, scegli Patch Manager.
- Seleziona la scheda Report di conformità.
- Nell'area Dettagli sull'applicazione di patch, scegli l'ID del nodo gestito per il quale desideri esaminare i risultati di conformità delle patch. Nodi che vengono visualizzati stopped o non terminated verranno visualizzati qui.
- Vai nell'area Dettagli e, nell'elenco Proprietà, scegli Patch.

Opzione 2: naviga da Conformità, uno strumento di AWS Systems Manager:

- Nel riquadro di navigazione, seleziona Conformità.
- Per il riepilogo delle risorse sulla conformità, scegli un numero nella colonna per i tipi di risorse sulle patch che desideri esaminare, ad esempio Non-Compliant le risorse.
- Sotto, nell'elenco Risorsa, scegli l'ID del nodo gestito per il quale desideri esaminare i risultati di conformità delle patch.
- Vai nell'area Dettagli e, nell'elenco Proprietà, scegli Patch.

Opzione 3: naviga da Fleet Manager.

- Nel pannello di navigazione, scegli Fleet Manager.

- Nell'area Istanze gestite, scegli l'ID del nodo gestito per il quale desideri esaminare i risultati di conformità delle patch.
 - Vai nell'area Dettagli e, nell'elenco Proprietà, scegli Patch.
2. (Facoltativo) Nella casella di ricerca , scegli tra i filtri disponibili.

Ad esempio, per Red Hat Enterprise Linux(RHEL), scegli tra le seguenti opzioni:

- Nome
- Classificazione
- Stato
- Gravità

Per Windows Server, scegli tra le seguenti opzioni:

- KB
- Classificazione
- Stato
- Gravità

3. Scegli uno dei valori disponibili per il tipo di filtro scelto. Ad esempio, se hai scelto Stato, ora scegli uno stato di conformità come `InstalledPendingReboot` `Fallito` o `Mancante`.

 Note

Attualmente, i valori dell'ID CVE vengono riportati solo per le patch con stato `Missing` o `Failed`.

4. A seconda dello stato di conformità del nodo gestito, è possibile scegliere l'azione da intraprendere per porre rimedio a eventuali nodi non conformi.

Ad esempio, è possibile scegliere di applicare immediatamente patch ai nodi gestiti non conformi. Per informazioni su come applicare patch su nodi gestiti on demand, consulta [Patching dei nodi gestiti on demand](#).

Per informazioni sui dati di conformità delle patch, consulta [Valori dello stato di conformità delle patch](#).

Generazione di report sulla conformità delle patch csv

Puoi utilizzare la AWS Systems Manager console per generare report di conformità delle patch che vengono salvati come file .csv in un bucket Amazon Simple Storage Service (Amazon S3) a tua scelta. È possibile generare un singolo report su richiesta o specificare una pianificazione per la generazione automatica dei report.

I report possono essere generati per un singolo nodo gestito o per tutti i nodi gestiti nell'account selezionato. Account AWS Regione AWS Per un singolo nodo, un report contiene dettagli completi, inclusi gli ID delle patch relative a un nodo non conforme. Per un report su tutti i nodi gestiti, vengono fornite solo le informazioni di riepilogo e i conteggi delle patch dei nodi non conformi.

Dopo aver generato un report, puoi utilizzare uno strumento come Amazon Quick per importare e analizzare i dati. Quick è un servizio di business intelligence (BI) che puoi utilizzare per esplorare e interpretare le informazioni in un ambiente visivo interattivo. Per ulteriori informazioni, consulta la [Amazon Quick User Guide](#).

Note

Quando si crea una baseline delle patch personalizzata, è possibile specificare un livello di gravità di conformità per le patch approvate da quella baseline delle patch, ad esempio `Critical` o `High`. Se lo stato delle patch approvate viene riportato come `Missing`, la gravità di conformità complessiva riportata dalla baseline delle patch corrisponde al livello di gravità specificato.

È possibile anche specificare un argomento Amazon Simple Notification Service (Amazon SNS) da utilizzare per l'invio delle notifiche quando viene generato un report.

Ruoli del servizio per la generazione di report sulla conformità delle patch

La prima volta che generi un report, Systems Manager crea un ruolo di Automation denominato `AWS-SystemsManager-PatchSummaryExportRole` da utilizzare per il processo di esportazione a S3.

 Note

Se stai esportando dati di conformità in un bucket S3 crittografato, devi aggiornare la politica delle AWS KMS chiavi associata per fornire le autorizzazioni necessarie per. `AWS-SystemsManager-PatchSummaryExportRole` Ad esempio, aggiungi un'autorizzazione simile a questa alla politica del tuo bucket S3: AWS KMS

```
{
  "Effect": "Allow",
  "Action": [
    "kms:GenerateDataKey"
  ],
  "Resource": "role-arn"
}
```

Sostituiscilo *role-arn* con l'Amazon Resource Name (ARN) del nome creato nel tuo account, nel formato. `arn:aws:iam::111222333444:role/service-role/AWS-SystemsManager-PatchSummaryExportRole`

Per ulteriori informazioni, consulta [Policy delle chiavi in AWS KMS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

La prima volta che generi un report su una pianificazione, Systems Manager crea un altro ruolo di servizio denominato `AWS-EventBridge-Start-SSMAutomationRole`, insieme al ruolo di servizio `AWS-SystemsManager-PatchSummaryExportRole` (se non è già stato creato) da utilizzare per il processo di esportazione. `AWS-EventBridge-Start-SSMAutomationRole` consente EventBridge ad Amazon di avviare un'automazione utilizzando il runbook [AWS- ExportPatchReportToS3](#).

Si consiglia di non tentare di modificare questi criteri e ruoli. In questo modo, la generazione del report sulla conformità delle patch potrebbe non riuscire. Per ulteriori informazioni, consulta [Risoluzione dei problemi relativi alla generazione del report sulla conformità delle patch](#).

Cosa c'è in un report sulla conformità delle patch generato?

In questo argomento vengono fornite informazioni sui tipi di contenuto inclusi nei report di conformità delle patch generati e scaricati in un bucket S3 specificato.

Formato report per un singolo nodo gestito

Un report generato per un singolo nodo gestito fornisce informazioni di riepilogo e dettagliate.

[Scaricare un report di esempio \(singolo nodo\)](#)

Le informazioni di riepilogo per un singolo nodo gestito includono quanto segue:

- Indice
- ID istanza
- Instance name (Nome dell'istanza)
- IP istanza
- Nome piattaforma
- Versione della piattaforma
- Versione SSM Agent
- baseline delle patch
- Gruppo di patch
- Compliance status (Stato di conformità)
- Gravità di conformità
- Conteggio delle patch di gravità critica non conforme
- Conteggio delle patch a gravità elevata non conforme
- Conteggio delle patch di gravità media non conforme
- Conteggio delle patch a bassa gravità non conforme
- Conteggio delle patch di gravità delle informazioni non conforme
- Conteggio delle patch di gravità non conforme non specificato

Le informazioni dettagliate per un singolo nodo gestito includono quanto segue:

- Indice
- ID istanza
- Instance name (Nome dell'istanza)
- Nome patch
- ID KB ID/Patch
- Stato della patch
- Ora dell'ultimo report
- Livelli di conformità

- Gravità della patch
- Classificazione di patch
- ID CVE
- baseline delle patch
- URL di log
- IP istanza
- Nome piattaforma
- Versione della piattaforma
- Versione SSM Agent

Note

Quando si crea una baseline delle patch personalizzata, è possibile specificare un livello di gravità di conformità per le patch approvate da quella baseline delle patch, ad esempio `Critical` o `High`. Se lo stato delle patch approvate viene riportato come `Missing`, la gravità di conformità complessiva riportata dalla baseline delle patch corrisponde al livello di gravità specificato.

Formato report per tutti i nodi gestiti

Un report generato per tutti i nodi gestiti fornisce solo informazioni di riepilogo.

[Scarica un report di esempio \(tutti i nodi gestiti\)](#)

Le informazioni di riepilogo per tutti i nodi gestiti includono:

- Indice
- ID istanza
- Instance name (Nome dell'istanza)
- IP istanza
- Nome piattaforma
- Versione della piattaforma
- Versione SSM Agent
- baseline delle patch

- Gruppo di patch
- Compliance status (Stato di conformità)
- Gravità di conformità
- Conteggio delle patch di gravità critica non conforme
- Conteggio delle patch a gravità elevata non conforme
- Conteggio delle patch di gravità media non conforme
- Conteggio delle patch a bassa gravità non conforme
- Conteggio delle patch di gravità delle informazioni non conforme
- Conteggio delle patch di gravità non conforme non specificato

Generazione di report sulla conformità delle patch per un singolo nodo

Utilizzare la procedura seguente per generare un report di riepilogo delle patch per un singolo nodo nel tuo Account AWS. Il report per un singolo nodo gestito fornisce dettagli su ogni patch non conforme, inclusi i nomi e gli ID delle patch.

Per generare report sulla conformità delle patch per un singolo nodo gestito

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Patch Manager.
3. Seleziona la scheda Report di conformità.
4. Scegli il pulsante relativo alla riga del nodo gestito per il quale generare un report e quindi fai clic su Visualizza i dettagli.
5. Sulla sezione Pagina di riepilogo patch, scegli Esporta in S3.
6. Per Nome del report, immetti un nome per semplificare l'identificazione del report in un secondo momento.
7. Per Frequenza di report, scegli una delle opzioni seguenti:
 - Su richiesta: consente di creare un report una tantum. Passa alla fase 9.
 - In una programmazione: specifica una pianificazione ricorrente per la generazione automatica dei report. Prosegui alla fase 8.
8. Per Tipo di pianificazione, specifica un'espressione della frequenza, ad esempio ogni 3 giorni, o fornire un'espressione cron per impostare la frequenza del report.

Per informazioni sulle espressioni Cron, consulta [Riferimento: espressioni Cron e della frequenza per Systems Manager](#).

9. Per Nome bucket, seleziona il nome di un bucket S3 in cui memorizzare i file di report CSV.

 Important

Se lavori in un Regione AWS bucket lanciato dopo il 20 marzo 2019, devi selezionare un bucket S3 nella stessa regione. Le regioni lanciate dopo tale data sono state disattivate per impostazione predefinita. Per ulteriori informazioni e un elenco di queste regioni, consulta [Abilitazione di una regione](#) in nella Riferimenti generali di Amazon Web Services.

10. (Facoltativo) Per inviare notifiche quando viene generato il report, espandi la sezione Argomenti SNS e scegli un Argomento Amazon SNS esistente da SNS topic Amazon Resource Name (ARN).
11. Seleziona Invia.

Per informazioni sulla visualizzazione di una cronologia dei report generati, consulta [Visualizzazione della cronologia dei rapporti sulla conformità delle patch](#).

Per informazioni sulla visualizzazione dei dettagli delle pianificazioni di report create, consulta [Visualizzazione delle pianificazioni di report sulla conformità delle patch](#).

Generazione di report sulla conformità delle patch per tutti i nodi gestiti

Utilizza la procedura seguente per generare un report di riepilogo delle patch per tutti i nodi gestiti in Account AWS. Il report per tutti i nodi gestiti indica quali nodi non sono conformi e il numero di patch non conformi. Non fornisce i nomi o altri identificatori delle patch. Per questi dettagli aggiuntivi, è possibile generare un report sulla conformità delle patch per un singolo nodo gestito. Per ulteriori informazioni, consulta la sezione [Generazione di report sulla conformità delle patch per un singolo nodo](#) riportata in precedenza in questo argomento.

Per generare report sulla conformità delle patch per tutti i nodi gestiti

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Patch Manager.

3. Seleziona la scheda Report di conformità.
4. Scegli Esportazione in S3. (Non selezionare prima un ID nodo.)
5. Per Nome del report, immetti un nome per semplificare l'identificazione del report in un secondo momento.
6. Per Frequenza di report, scegli una delle opzioni seguenti:
 - On demand - Consente di creare un report una tantum. Passare alla fase 8.
 - In un programma - Specifica una pianificazione ricorrente per la generazione automatica dei report. Continuare con la fase 7.
7. Per Tipo di pianificazione, specifica un'espressione di frequenza, ad esempio ogni 3 giorni, o fornire un'espressione cron per impostare la frequenza del report.

Per informazioni sulle espressioni Cron, consulta [Riferimento: espressioni Cron e della frequenza per Systems Manager](#).

8. Per Nome bucket, seleziona il nome di un bucket S3 in cui memorizzare i file di report CSV.

 Important

Se lavori in un Regione AWS bucket lanciato dopo il 20 marzo 2019, devi selezionare un bucket S3 nella stessa regione. Le regioni lanciate dopo tale data sono state disattivate per impostazione predefinita. Per ulteriori informazioni e un elenco di queste regioni, consulta [Abilitazione di una regione](#) in nella Riferimenti generali di Amazon Web Services.

9. (Facoltativo) Per inviare notifiche quando viene generato il report, espandi la sezione Argomenti SNS e scegli un Argomento Amazon SNS esistente da SNS topic Amazon Resource Name (ARN).
10. Seleziona Invia.

Per informazioni sulla visualizzazione di una cronologia dei report generati, consulta [Visualizzazione della cronologia dei rapporti sulla conformità delle patch](#).

Per informazioni sulla visualizzazione dei dettagli delle pianificazioni di report create, consulta [Visualizzazione delle pianificazioni di report sulla conformità delle patch](#).

Visualizzazione della cronologia dei rapporti sulla conformità delle patch

Utilizza le informazioni contenute in questo argomento per visualizzare i dettagli sui report di conformità delle patch generati nel tuo Account AWS

Visualizzazione della cronologia dei rapporti sulla conformità delle patch

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Patch Manager.
3. Seleziona la scheda Report di conformità.
4. Scegliere Visualizza tutte le esportazioni di S3 e quindi selezionare la scheda Cronologia dell'esportazione.

Visualizzazione delle pianificazioni di report sulla conformità delle patch

Utilizza le informazioni contenute in questo argomento per visualizzare i dettagli sulle pianificazioni di reporting sulla conformità delle patch create nel tuo Account AWS.

Visualizzazione della cronologia dei rapporti sulla conformità delle patch

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Patch Manager.
3. Seleziona la scheda Report di conformità.
4. Sceglie Visualizza tutte le esportazioni di S3 e quindi selezionare la casella Regole di report pianificati.

Risoluzione dei problemi relativi alla generazione del report sulla conformità delle patch

Utilizza le informazioni seguenti per risolvere i problemi relativi alla generazione del report di conformità patch in Patch Manager, uno strumento di AWS Systems Manager.

Un messaggio segnala che la policy **AWS-SystemsManager-PatchManagerExportRolePolicy** è danneggiata

Problema: viene visualizzato un messaggio di errore simile al seguente, indicando che AWS-SystemsManager-PatchManagerExportRolePolicy è danneggiato:

An error occurred while updating the AWS-SystemsManager-PatchManagerExportRolePolicy policy. If you have edited the policy, you might need to delete the policy, and any role that uses it, then try again. Systems Manager recreates the roles and policies you have deleted.

- Soluzione: utilizza la Patch Manager console o elimina AWS CLI i ruoli e le policy interessati prima di generare un nuovo rapporto sulla conformità delle patch.

Per eliminare la policy danneggiata utilizzando la console

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Esegui una delle seguenti operazioni:

On-demand report: se il problema si è verificato durante la generazione di un report una tantum su richiesta, nella barra di navigazione a sinistra, scegli Policy, cerca AWS-SystemsManager-PatchManagerExportRolePolicy, quindi elimina la policy. Quindi, selezionare Ruoli, cercare AWS-SystemsManager-PatchSummaryExportRole ed eliminare il ruolo.

Report pianificati - Se il problema si è verificato durante la generazione di un report in base a una pianificazione, nella navigazione a sinistra seleziona Policy, cerca uno alla volta per AWS-EventBridge-Start-SSMAutomationRolePolicy e AWS-SystemsManager-PatchManagerExportRolePolicy ed elimina ogni policy. Quindi, selezionare Ruoli, cerca uno alla volta per AWS-EventBridge-Start-SSMAutomationRole e AWS-SystemsManager-PatchSummaryExportRole ed eliminare ogni ruolo.

Per eliminare la policy danneggiata utilizzando il AWS CLI

Sostituiscila *placeholder values* con l'ID del tuo account.

- Se il problema si è verificato durante la generazione di un report monouso su richiesta, esegui i seguenti comandi:

```
aws iam delete-policy --policy-arn arn:aws:iam::account-id:policy/AWS-SystemsManager-PatchManagerExportRolePolicy
```

```
aws iam delete-role --role-name AWS-SystemsManager-PatchSummaryExportRole
```

Se il problema si è verificato durante la generazione di un report monouso su richiesta, esegui i seguenti comandi:

```
aws iam delete-policy --policy-arn arn:aws:iam::account-id:policy/AWS-EventBridge-Start-SSMAutomationRolePolicy
```

```
aws iam delete-policy --policy-arn arn:aws:iam::account-id:policy/AWS-SystemsManager-PatchManagerExportRolePolicy
```

```
aws iam delete-role --role-name AWS-EventBridge-Start-SSMAutomationRole
```

```
aws iam delete-role --role-name AWS-SystemsManager-PatchSummaryExportRole
```

Dopo aver completato una delle due procedure, segui i passaggi per generare o pianificare un nuovo report sulla conformità delle patch.

Dopo aver eliminato i ruoli o i criteri di conformità delle patch, i report pianificati non vengono generati correttamente

Problema: la prima volta che si genera un report, Systems Manager crea un ruolo di servizio e una policy da utilizzare per il processo di esportazione (AWS-SystemsManager-PatchSummaryExportRole e AWS-SystemsManager-PatchManagerExportRolePolicy). La prima volta che si genera un report in base a una pianificazione, Systems Manager crea un altro ruolo di servizio e una policy (AWS-EventBridge-Start-SSMAutomationRole e AWS-EventBridge-Start-SSMAutomationRolePolicy). Questi consentono EventBridge ad Amazon di avviare un'automazione utilizzando il runbook [AWS- ExportPatchReportToS3](#).

Se elimini una di queste policy o di questi ruoli, le connessioni tra la pianificazione e il bucket S3 specificato e l'argomento Amazon SNS potrebbero andare perdute.

- Soluzione: per risolvere questo problema, si consiglia di eliminare la pianificazione precedente e di creare una nuova pianificazione per sostituire quella che si verificava problemi.

Correzione dei nodi gestiti non conformi con Patch Manager

Gli argomenti di questa sezione forniscono una panoramica su come identificare i nodi gestiti che non sono conformi alle patch. Descrivono inoltre come rendere i nodi conformi.

Identificazione di nodi gestiti non conformi

Out-of-compliance i nodi gestiti vengono identificati quando viene eseguito uno dei due AWS Systems Manager documenti (documenti SSM). Questi documenti SSM fanno riferimento alla baseline delle patch idonea per ogni nodo gestito in Patch Manager, uno strumento di AWS Systems Manager. Essi valutano quindi lo stato della patch del nodo gestito e quindi rendono disponibili i risultati di conformità.

Esistono due documenti SSM utilizzati per identificare o aggiornare nodi gestiti non conformi: `AWS-RunPatchBaseline` e `AWS-RunPatchBaselineAssociation`. Ognuno di essi è utilizzato da processi diversi e i risultati di conformità sono disponibili attraverso diversi canali. La tabella seguente illustra le differenze tra questi documenti.

Note

I dati di conformità delle patch da Patch Manager possono essere inviati a AWS Security Hub CSPM. Security Hub CSPM offre una visione completa degli avvisi di sicurezza ad alta priorità e dello stato di conformità. Monitora anche lo stato di applicazione di patch del parco istanze. Per ulteriori informazioni, consulta [Integrazione Patch Manager con AWS Security Hub CSPM](#).

	AWS-RunPatchBaseline	AWS-RunPatchBaselineAssociation
Processi che utilizzano il documento	Patch on demand - È possibile eseguire la scansione o applicare patch sui nodi gestiti su richiesta utilizzando l'opzione Applica patch ora. Per informazioni, consulta Patching dei nodi gestiti on demand .	Gestione host per Quick Setup di Systems Manager: è possibile abilitare un'opzione di configurazione della gestione host in Quick Setup per eseguire ogni giorno la scansione delle istanze gestite e verificare la conformità

	AWS-RunPatchBaseline	AWS-RunPatchBaselineAssociation
	<p>Policy sulle Quick Setup patch di Systems Manager: è possibile creare una configurazione di patch in Quick Setup, in grado di scansionare o installare le patch mancanti in pianificazioni separate per un'intera organizzazione, un sottoinsieme di unità organizzative o una singola. Account AWS Per informazioni, consulta Configurare l'applicazione di patch per le istanze in un'organizzazione utilizzando un Configurazione rapida politica sulle patch.</p> <p>Esegui un comando: è possibile eseguire manualmente un'operazione AWS-RunPatchBaseline in Run Command Per informazioni, consulta Esecuzione di comandi dalla console.</p> <p>Maintenance window (Finestra di manutenzione) - È possibile creare una finestra di manutenzione che utilizza il documento SSM AWS-RunPatchBaseline in un tipo di attività Run Command. Per informazioni, consulta Tutorial: creazione di una finestra di</p>	<p>delle patch. Per informazioni, consulta Configura la gestione degli host di Amazon EC2 utilizzando Configurazione rapida.</p> <p>Systems Manager Explorer: quando lo consenti Explorer, analizza regolarmente le istanze gestite per verificarle e la conformità alle patch e riporta i risultati nella Explorer dashboard.</p>

	AWS-RunPatchBaseline	AWS-RunPatchBaselineAssociation
	manutenzione per l'applicazione di patch tramite console.	
Formato dei dati dei risultati della scansione delle patch	Dopo le AWS-RunPatchBaseline esecuzioni, Patch Manager invia un <code>AWS:PatchSummary</code> oggetto a Inventory. Questo report viene generato solo dopo aver eseguito correttamente le operazioni di applicazione delle patch e include un orario di acquisizione che identifica quando è stato calcolato lo stato di conformità.	Dopo l'esecuzione di <code>AWS-RunPatchBaselineAssociation</code> , Patch Manager invia un oggetto <code>AWS:ComplianceItem</code> a Systems Manager Inventory.

	AWS-RunPatchBaseline	AWS-RunPatchBaselineAssociation
Visualizzazione di report di conformità delle patch nella console	<p>È possibile visualizzare le informazioni sulla conformità delle patch per i processi che utilizzano AWS-RunPatchBaseline in Conformità della configurazione di Systems Manager e Utilizzo dei nodi gestiti. Per ulteriori informazioni, consulta Visualizzazione dei risultati di conformità delle patch.</p>	<p>Quando si utilizza Quick Setup per eseguire la scansione delle istanze gestite per verificare la conformità delle patch, è possibile visualizzare il report di conformità in Systems Manager Fleet Manager. Nella console Fleet Manager, scegli l'ID del nodo gestito. Nel menu Generale, scegli Conformità alla configurazione.</p> <p>Quando si utilizza Explorer per eseguire la scansione delle istanze gestite per verificare la conformità delle patch, è possibile visualizzare il report di conformità sia in Explorer che Systems Manager OpsCenter.</p>

	AWS-RunPatchBaseline	AWS-RunPatchBaselineAssociation
AWS CLI comandi per visualizzare i risultati di conformità delle patch	<p>Per i processi che utilizzano <code>AWS-RunPatchBaseline</code>, è possibile utilizzare i seguenti AWS CLI comandi per visualizzare informazioni di riepilogo sulle patch su un nodo gestito.</p> <ul style="list-style-type: none"> • describe-instance-patch-states • describe-instance-patch-states-for-patch-group • describe-patch-group-state 	<p>Per i processi che utilizzano <code>AWS-RunPatchBaselineAssociation</code>, è possibile utilizzare il AWS CLI comando seguente per visualizzare informazioni di riepilogo sulle patch su un'istanza.</p> <ul style="list-style-type: none"> • list-compliance-items
Informazioni sull'applicazione di patch	<p>Per i processi che utilizzano <code>AWS-RunPatchBaseline</code>, si specifica se si desidera che l'operazione esegua solo un'operazione <code>Scan</code> o un'operazione <code>Scan and install</code>.</p> <p>Se il tuo obiettivo è identificare i nodi gestiti non conformi e non correggerli, esegui solo un'operazione <code>Scan</code>.</p>	<p>I processi Quick Setup e Explorer, che utilizzano <code>AWS-RunPatchBaselineAssociation</code>, eseguono solo un'operazione <code>Scan</code>.</p>
Ulteriori informazioni	Documento di comando SSM per l'applicazione di patch: AWS-RunPatchBaseline	Documento di comando SSM per l'applicazione di patch: AWS-RunPatchBaselineAssociation

Per informazioni sui vari stati di conformità delle patch che potrebbero essere riportati, consulta [Valori dello stato di conformità delle patch](#)

Per informazioni sulla correzione dei nodi gestiti che non rispettano la conformità delle patch, consulta [Applicazione di patch a nodi gestiti non conformi](#).

Valori dello stato di conformità delle patch

Le informazioni sulle patch per un nodo gestito includono un rapporto sullo stato di ogni singola patch.

Tip

Se desideri assegnare uno stato di conformità delle patch specifico a un nodo gestito, puoi utilizzare il comando [put-compliance-items](#) AWS Command Line Interface (AWS CLI) o l'operazione [PutComplianceItems](#) API. L'assegnazione dello stato di conformità non è supportata nella console.

Utilizza le informazioni riportate nelle tabelle seguenti per riuscire a identificare i motivi per cui un nodo gestito potrebbe non essere conforme alle patch.

Valori di conformità delle patch per Debian Server and Ubuntu Server

Per Debian Server e Ubuntu Server, le regole per la classificazione dei pacchetti nei vari stati di conformità sono descritte nella seguente tabella.

Note

Tieni presente quanto segue, quando valuti i valori dello stato INSTALLED, INSTALLED_OTHER e MISSING: se non selezioni la casella di controllo Includi aggiornamenti non di sicurezza durante la creazione o l'aggiornamento di una baseline delle patch, le versioni patch candidate sono limitate alle patch nei seguenti repository:

- `bionic-security`(Ubuntu Server18.04 LTS)
- `focal-security`(Ubuntu Server20.04 LTS)
- `jammy-security`(Ubuntu Server22.04 LTS)
- `noble-security`(Ubuntu Server24.04 LTS)
- `plucky-security`(25.04) Ubuntu Server
- `debian-security` (Debian Server)

Quando si seleziona l'opzione Includi aggiornamenti non correlati alla sicurezza, vengono considerate anche le patch di altri repository.

Stato della patch	Description	Compliance status (Stato di conformità)
INSTALLED	La patch non è inclusa nella baseline delle patch, ma è installata nel nodo gestito. Potrebbe essere stato installato manualmente da un individuo o automaticamente da Patch Manager quando il documento AWS-RunPatchBaseline è stato eseguito sul nodo gestito.	Conforme
INSTALLED_OTHER	La patch non è inclusa nella baseline, o non è approvata da essa ma è installata nel nodo gestito. La patch potrebbe essere stata installata manualmente, il pacchetto potrebbe essere una dipendenza obbligatoria di un'altra patch approvata o la patch potrebbe essere stata inclusa in un' InstallOverrideList operazione. Se non indichi Block come azione Patch rifiutate, INSTALLED_OTHER include anche patch installate ma rifiutate.	Conforme

Stato della patch	Description	Compliance status (Stato di conformità)
INSTALLED_PENDING_REBOOT	<p>INSTALLED_PENDING_REBOOT significa una delle due cose:</p> <ul style="list-style-type: none">• L'operazione Patch Manager Install ha applicato la patch al nodo gestito, ma il nodo non è stato riavviato dopo l'applicazione della patch. Ciò significa in genere che l'opzione NoReboot è stata selezionata per il parametro RebootOption quando il documento AWS-RunPatchBaseline è stato eseguito l'ultima volta sul nodo gestito. <p>Per ulteriori informazioni, consulta Nome parametro: RebootOption.</p> <ul style="list-style-type: none">• Una patch è stata installata all'esterno di Patch Manager dall'ultima volta che il nodo gestito è stato riavviato. <p>In nessun caso ciò significa che una patch con questo stato richieda un riavvio, ma solo che il nodo non è stato riavviato dopo l'installazione della patch.</p>	Non-Compliant

Stato della patch	Description	Compliance status (Stato di conformità)
INSTALLED_REJECTED	La patch è installata nel nodo gestito, ma è specificata in un elenco di Patch rifiutate . Questo in genere significa che la patch è stata installata prima di essere aggiunta a un elenco di patch rifiutate.	Non-Compliant
MISSING	La patch è approvata nella baseline, ma non è installata nel nodo gestito. Se configuri l'attività del documento AWS-RunPatchBaseline per l'analisi anziché per l'installazione, il sistema riporta questo stato per le patch individuate durante l'analisi ma non installate.	Non-Compliant
FAILED	La patch è approvata nella baseline, ma non è stato possibile installarla. Per risolvere questa situazione, esamina l'output del comando per ottenere informazioni utili per comprendere il problema.	Non-Compliant

Valori di conformità delle patch per altri sistemi operativi

Per tutti i sistemi operativi oltre a Debian Server e Ubuntu Server, le regole per la classificazione dei pacchetti nei vari stati di conformità sono descritte nella tabella seguente.

Stato della patch	Description	Valore di conformità
INSTALLED	La patch non è inclusa nella baseline delle patch, ma è installata nel nodo gestito. Potrebbe essere stato installato manualmente da un individuo o automaticamente da Patch Manager quando il documento AWS-RunPatchBaseline è stato eseguito sul nodo.	Conforme
INSTALLED_OTHER ¹	<p>La patch non è inclusa nella baseline, ma è installata nel nodo. I possibili motivi sono due:</p> <ol style="list-style-type: none"> 1. C'è la possibilità che la patch non sia stata installata manualmente. 2. Solo Linux: c'è la possibilità che il pacchetto sia stato installato come dipendenza richiesta di una patch diversa e approvata. Quando si specifica <code>Allow as dependency</code> come azione di Patch rifiutate, alle patch installate e come dipendenze viene assegnato lo stato di segnalazione INSTALLED_OTHER. <p>Nota che Windows Server non supporta il concetto</p>	Conforme

Stato della patch	Description	Valore di conformità
	di dipendenza dalle patch. Per informazioni su come Patch Manager gestisce le patch nell'elenco delle patch rifiutate su Windows Server, consulta le opzioni dell'elenco delle patch rifiutate nelle baseline delle patch personalizzate .	
INSTALLED_REJECTED	La patch è installata nel nodo gestito, ma è specificata in un elenco di Patch rifiutate . Questo in genere significa che la patch è stata installata prima di essere aggiunta a un elenco di patch rifiutate.	Non-Compliant

Stato della patch	Description	Valore di conformità
INSTALLED_PENDING_REBOOT	<p>INSTALLED_PENDING_REBOOT significa una delle due cose:</p> <ul style="list-style-type: none">• L'operazione Patch Manager Install ha applicato la patch al nodo gestito, ma il nodo non è stato riavviato dopo l'applicazione della patch. Ciò significa in genere che l'opzione NoReboot è stata selezionata per il parametro RebootOption quando il documento AWS-RunPatchBaseline è stato eseguito l'ultima volta sul nodo gestito. <p>Per ulteriori informazioni, consulta Nome parametro: RebootOption.</p> <ul style="list-style-type: none">• Una patch è stata installata all'esterno di Patch Manager dall'ultima volta che il nodo gestito è stato riavviato. <p>In nessun caso ciò significa che una patch con questo stato richieda un riavvio, ma solo che il nodo non è stato riavviato dopo l'installazione della patch.</p>	Non-Compliant

Stato della patch	Description	Valore di conformità
MISSING	La patch è approvata nella baseline, ma non è installata nel nodo gestito. Se configuri l'attività del documento AWS-RunPatchBaseline per l'analisi anziché per l'installazione, il sistema riporta questo stato per le patch individuate durante l'analisi ma non installate.	Non-Compliant
FAILED	La patch è approvata nella baseline, ma non è stato possibile installarla. Per risolvere questa situazione, esamina l'output del comando per ottenere informazioni utili per comprendere il problema.	Non-Compliant

Stato della patch	Description	Valore di conformità
NOT_APPLICABLE ¹	<p>Questo stato di conformità viene segnalato solo per i sistemi operativi Windows Server.</p> <p>La patch è approvata nella baseline, ma la funzionalità o il servizio da cui viene utilizzata non è installato nel nodo gestito. Ad esempio, una patch per un servizio server Web, come Internet Information Services (IIS), mostrerà NOT_APPLICABLE se è stata approvata nella baseline, ma il servizio Web non è installato nel nodo gestito. Una patch ha anche la possibilità di essere contrassegnata con NOT_APPLICABLE se è stata sostituita da un aggiornamento successivo. Ciò significa che è installato l'aggiornamento più recente e che l'aggiornamento NOT_APPLICABLE non è più richiesto.</p>	Non applicabile

Stato della patch	Description	Valore di conformità
AVAILABLE_SECURITY_UPDATES	<p>Questo stato di conformità viene segnalato solo per i sistemi operativi Windows Server.</p> <p>Una patch di aggiornamento di sicurezza disponibile, non approvata dalla baseline delle patch, può avere un valore di conformità di Compliant o Non-Compliant, come definito in una baseline di patch personalizzata.</p> <p>Quando si crea o si aggiorna una baseline delle patch, si sceglie lo stato da assegnare alle patch di sicurezza, disponibili ma non approvate, perché non soddisfano i criteri di installazione specifici nella baseline delle patch. Ad esempio, le patch di sicurezza che si desidera installare possono essere ignorate se è stato specificato un lungo periodo di attesa dopo il rilascio di una patch prima dell'installazione. Se un aggiornamento della patch viene rilasciato durante il periodo di attesa specificato, il periodo di attesa per l'installazione della patch ricomincia da capo. Se il periodo</p>	<p>Conforme o Non-Compliant, a seconda dell'opzione selezionata per gli aggiornamenti di sicurezza disponibili.</p> <div> <p> Note</p> <p>Utilizzando la console per creare o aggiornare una baseline delle patch, si specifica questa opzione nel campo Stato di conformità degli aggiornamenti di sicurezza disponibili. Utilizzando il update-patch-baseline comando AWS CLI to run the create-patch-baseline or, si specifica questa opzione nel available-security-updates-compliance-status parametro.</p> </div>

Stato della patch	Description	Valore di conformità
	<p>di attesa è troppo lungo, è possibile che più versioni della patch vengano rilasciate e mai installate.</p> <p>Per quanto riguarda il conteggio riepilogativo delle patch, quando una patch viene segnalata come <code>AvailableSecurityUpdate</code>, verrà sempre inclusa in <code>AvailableSecurityUpdateCount</code>. Se la baseline è configurata per riportare queste patch come <code>NonCompliant</code>, viene inclusa anche in <code>SecurityNonCompliantCount</code>. Se la baseline è configurata per riportare queste patch come <code>Compliant</code>, viene inclusa anche in <code>SecurityNonCompliantCount</code>. Queste patch vengono sempre segnalate con una gravità non specificata e non sono mai incluse nel <code>CriticalNonCompliantCount</code>.</p>	

¹ Per le patch con lo stato `INSTALLED_OTHER` e `NOT_APPLICABLE`, Patch Manager omette alcuni dati dai risultati delle query in base al comando [describe-instance-patches](#), ad esempio i valori per `Classification` e `Severity`. Questo viene fatto per evitare il superamento del limite di dati per i singoli nodi in Inventory. Per visualizzare tutti i dettagli della patch, è possibile utilizzare il comando [describe-available-patches](#).

Applicazione di patch a nodi gestiti non conformi

Molti degli stessi AWS Systems Manager strumenti e processi che puoi utilizzare per verificare la conformità alle patch dei nodi gestiti possono essere utilizzati per rendere i nodi conformi alle regole di patch attualmente applicabili a loro. Per rendere i nodi gestiti conformi alle patch, Patch Manager è necessario eseguire un'operazione `Scan and install`. (Se il tuo obiettivo è solo identificare i nodi gestiti non conformi ma non correggerli, esegui piuttosto un'operazione di `Scan`. Per ulteriori informazioni, consulta [Identificazione di nodi gestiti non conformi](#)).

Installa le patch utilizzando Systems Manager

È possibile scegliere tra diversi strumenti per eseguire un'operazione `Scan and install`:

- (Consigliato) Configura una policy di patch in Quick Setup, uno strumento di Systems Manager, che consente di installare le patch mancanti in base alla pianificazione di un'intera organizzazione, un sottoinsieme di unità organizzative o di un singolo Account AWS. Per ulteriori informazioni, consulta [Configurare l'applicazione di patch per le istanze in un'organizzazione utilizzando un Configurazione rapida politica sulle patch](#).
- Crea una finestra di manutenzione che utilizza il documento di Systems Manager (documento SSM) `AWS-RunPatchBaseline` in un tipo di attività `Run Command`. Per informazioni, consulta [Tutorial: creazione di una finestra di manutenzione per l'applicazione di patch tramite console](#).
- Esegui manualmente `AWS-RunPatchBaseline` in un'operazione `Run Command`. Per informazioni, consulta [Esecuzione di comandi dalla console](#).
- Installa le patch su richiesta utilizzando l'opzione `Applica patch ora`. Per informazioni, consulta [Patching dei nodi gestiti on demand](#).

Identificazione dell'esecuzione che ha creato i dati di conformità delle patch

I dati sulla conformità delle patch rappresentano un'istantanea temporizzata dell'ultima operazione di patching riuscita. Ogni rapporto di conformità include sia un ID di esecuzione che un orario di acquisizione che consentono di identificare l'operazione che ha creato i dati di conformità e quando sono stati generati.

Quando si dispone di più tipi di operazioni per la scansione delle istanze al fine di verificarne la conformità alle patch, ogni analisi sovrascrive i dati di conformità delle patch delle scansioni precedenti. Di conseguenza, potresti ottenere risultati imprevisti nei dati di conformità delle patch.

Supponiamo ad esempio di creare una policy di patch che analizzi la conformità delle patch ogni giorno alle 2 del mattino ora locale. Tale policy di patch utilizza una baseline delle patch destinata alle patch con gravità `Critical`, `Important` e `Moderate`. Tale baseline delle patch indica inoltre alcune patch specificamente rifiutate.

Supponiamo inoltre che tu abbia già configurato una finestra di manutenzione, che non è possibile eliminare o disattivare per analizzare lo stesso set di nodi gestiti ogni giorno alle 16:00 ora locale. L'attività di quella finestra di manutenzione utilizza una baseline delle patch diversa, che si rivolge solo alle patch con severità `Critical` e non esclude alcuna patch specifica.

Quando la finestra di manutenzione esegue la seconda scansione, i dati di conformità delle patch della prima scansione vengono eliminati e sostituiti con quelli della seconda scansione.

Pertanto, consigliamo di utilizzare un solo metodo automatizzato per la scansione e l'installazione nelle operazioni di applicazione di patch. Se stai configurando le policy di patch, dovresti eliminare o disattivare altri metodi di scansione per verificarne la conformità. Per ulteriori informazioni, consulta i seguenti argomenti:

- Per annullare un'attività di applicazione di patch da una finestra di manutenzione, consulta [Aggiornamento o annullamento della registrazione delle attività di una finestra di manutenzione utilizzando la console](#)
- Per eliminare un'associazione State Manager, consulta [Eliminazione di associazioni](#).

Per disattivare le scansioni giornaliere di conformità delle patch in una configurazione di gestione host, segui questi passaggi in Quick Setup:

1. Nel pannello di navigazione, scegli Quick Setup.
2. Seleziona la configurazione di gestione host da aggiornare.
3. Scegli Actions, Edit configuration (Operazioni, Modifica configurazione).
4. Deseleziona la casella di controllo Scan instances for missing patches daily (Scansiona le istanze per le patch mancanti ogni giorno).
5. Scegliere Aggiorna.

 Note

L'utilizzo dell'opzione Patch now (Applica subito una patch) per verificare la conformità di un nodo gestito comporta anche una sovrascrittura dei dati di conformità delle patch.

Patching dei nodi gestiti on demand

Utilizzando l'opzione Patch now in Patch Manager, è possibile eseguire operazioni di patching su richiesta dalla console di Systems Manager. Ciò significa che non è necessario creare una pianificazione per aggiornare lo stato di conformità dei nodi gestiti o per installare patch sui nodi non conformi. Inoltre, non è necessario passare dalla console di Systems Manager a Patch Manager e viceversa Maintenance Windows, per impostare o modificare una finestra di patching pianificata.

Applica patch ora è particolarmente utile quando è necessario applicare aggiornamenti zero-day o installare altre patch fondamentali nei nodi gestiti il prima possibile.

 Note

L'applicazione di patch su richiesta è supportata per una singola Account AWS Regione AWS coppia alla volta. Non può essere utilizzata per l'applicazione di patch basate su policy di patch. Ti consigliamo di mantenere la conformità tra tutti i nodi gestiti tramite le policy di patch. Per ulteriori informazioni sull'utilizzo delle policy di patch, consulta [Configurazioni delle policy sulle patch in Configurazione rapida](#).

Come funziona “Applica patch ora”

Per eseguire Applica patch ora, si specificano solo due impostazioni richieste:

- Se eseguire la scansione solo per le patch mancanti o per eseguire la scansione di e, installare patch sui nodi gestiti
- Su quali nodi gestiti eseguire l'operazione

Quando viene eseguita l'operazione Patch now, determina quale base patch utilizzare nello stesso modo in cui viene selezionata per altre operazioni di patch. Se un nodo gestito è associato a un gruppo di patch, viene utilizzata la baseline delle patch specificata per quel gruppo. Se il nodo gestito non è associato a un gruppo di patch, l'operazione utilizza la baseline delle patch attualmente

impostata come di default per il tipo di sistema operativo del nodo gestito. Può trattarsi di una baseline predefinita o di una baseline personalizzata impostata come predefinita. Per ulteriori informazioni sulla selezione della baseline delle patch, consulta [Gruppi di patch](#).

Le opzioni che è possibile specificare per **Applica subito patch** includono la scelta di quando o se riavviare i nodi gestiti dopo l'applicazione di patch, la specificazione di un bucket Amazon Simple Storage Service (Amazon S3) per memorizzare i dati di log relativi a operazione di applicazione di patch ed esecuzione dei documenti di Systems Manager (documenti SSM) come hook del ciclo di vita durante l'applicazione di patch.

Soglie di concorrenza e di errore per “Applica patch ora”

Per **Applica patch ora**, le opzioni di concorrenza e soglia di errore sono gestite da Patch Manager. Non è necessario specificare su quanti nodi gestiti applicare la patch contemporaneamente, né quanti errori sono consentiti prima che l'operazione abbia esito negativo. Patch Manager applica le impostazioni di soglia di concorrenza e di errore descritte nelle tabelle seguenti quando si esegue la patch su richiesta.

Important

Le seguenti soglie si applicano solo a operazioni `Scan` and `install`. Per le operazioni `Scan`, Patch Manager tenta di scansionare contemporaneamente fino a 1.000 nodi e continuare la scansione fino a quando non ha riscontrato fino a 1.000 errori.

Concurrency: operazioni di installazione

Numero totale di nodi gestiti nell'operazione Patch now	Numero di nodi gestiti sottoposti a scansione o a cui vengono applicate patch contemporaneamente
Meno di 25	1
25-100	5%
da 101 a 1.000	8%
Oltre 1.000	10%

Soglia di errore: operazioni di installazione

Numero totale di nodi gestiti nell'operazione Patch now	Numero di errori consentiti prima che l'operazione non vada a buon fine
Meno di 25	1
25-100	5
Da 101 a 1.000	10
Oltre 1.000	10

Utilizzo degli hook del ciclo di vita “Applica patch ora”

Patch ora offre la possibilità di eseguire i documenti SSM Command come hook del ciclo di vita durante un'operazione di patching. Install È possibile utilizzare questi hook per attività quali l'arresto delle applicazioni prima dell'applicazione di patch o dell'esecuzione dei controlli di integrità delle applicazioni dopo l'applicazione di patch o in seguito a un riavvio.

Per ulteriori informazioni sull'utilizzo di Hook del ciclo di vita, consulta [Documento di comando SSM per l'applicazione di patch: AWS-RunPatchBaselineWithHooks](#).

La tabella seguente elenca gli hook del ciclo di vita disponibili per ciascuna delle tre opzioni di riavvio di Patch now, oltre a esempi di utilizzo per ciascun hook.

Hook del ciclo di vita e usi di esempio

Opzione di riavvio	Hook: prima dell'installazione	Hook: dopo l'installazione	Hook: in uscita	Hook: dopo il riavvio pianificato
Riavvia se necessario	Eseguire un documento di SSM prima di iniziare l'applicazione di patch. Esempio di utilizzo: arrestare le applicazioni	Eseguire un documento SSM al termine dell'operazione di applicazione di patch e prima del riavvio nodo gestito.	Esegui un documento SSM dopo il completamento dell'operazione di applicazione di patch e il riavvio delle istanze.	Non disponibile

Opzione di riavvio	Hook: prima dell'installazione	Hook: dopo l'installazione	Hook: in uscita	Hook: dopo il riavvio pianificato
	in modo sicuro prima dell'inizio del processo di applicazione di patch.	Esempio di utilizzo: eseguire operazioni come l'installazione di applicazioni di terze parti prima di un potenziale riavvio.	Esempio di utilizzo: assicurati che le applicazioni funzionino come previsto dopo l'applicazione delle patch.	
Non riavviare le istanze	Come sopra.	Eseguire un documento SSM al termine dell'operazione di applicazione di patch. Esempio di utilizzo: assicurati che le applicazioni funzionino come previsto dopo l'applicazione delle patch.	Non disponibile	Non disponibile

Opzione di riavvio	Hook: prima dell'installazione	Hook: dopo l'installazione	Hook: in uscita	Hook: dopo il riavvio pianificato
Pianificare un tempo di riavvio	Come sopra.	Stessa cosa per Non riavviare le istanze.	Non disponibile	<p>Esegui un documento SSM immediatamente dopo il completamento di un riavvio pianificato.</p> <p>Esempio di utilizzo: assicurati che le applicazioni funzionino come previsto dopo il riavvio.</p>

Esecuzione di “Applica patch ora”

Utilizza la procedura seguente per applicare patch ai tuoi nodi gestiti on demand.

Per eseguire “Applica patch ora”

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Patch Manager.
3. Scegli Applica patch ora.
4. Per Operazione di applicazione di patch, scegli una delle opzioni seguenti:
 - Scan: Patch Manager trova quali patch mancano dai tuoi nodi gestiti ma non le installa. È possibile visualizzare i risultati nel pannello di controllo Conformità o in altri strumenti utilizzati per la visualizzazione della conformità delle patch.
 - Scansione e installazione: Patch Manager trova quali patch mancano ai tuoi nodi gestiti e le installa.
5. Utilizza questa fase solo se è stato scelto Scansione e installazione nella fase precedente. Per Regions (Regioni), scegli una delle seguenti opzioni:

- **Riavvia se necessario:** Dopo l'installazione, Patch Manager riavvia i nodi gestiti solo se necessario per completare un'installazione di patch.
- **Non riavviare le mie istanze:** Dopo l'installazione, Patch Manager non riavvia i nodi gestiti. È possibile riavviare manualmente i nodi gestiti quando si sceglie o si gestiscono i riavvii al di fuori di Patch Manager.
- **Pianificare un tempo di riavvio:** specificare la data, l'ora e il fuso orario UTC per Patch Manager per riavviare i nodi gestiti. Dopo aver eseguito l'operazione **Applica patch ora**, il riavvio pianificato viene elencato come associazione in State Manager con il nome **AWS-PatchRebootAssociation**.

 Important

Se si annulla l'operazione principale di patching dopo che è stata avviata, l'**AWS-PatchRebootAssociation** associazione NON State Manager viene annullata automaticamente. Per evitare riavvii imprevisti, è necessario eliminare manualmente **AWS-PatchRebootAssociation** da State Manager se non si desidera più che si verifichi il riavvio pianificato. In caso contrario, potrebbero verificarsi riavvii non pianificati del sistema che potrebbero influire sui carichi di lavoro di produzione. È possibile trovare questa associazione nella console di Systems Manager in **State Manager > Associazioni**.

6. Per **Instances to patch** (Istanze a cui applicare le patch), scegliere una delle seguenti opzioni:
 - **Correggi tutte le istanze:** Patch Manager esegue l'operazione specificata su tutti i nodi gestiti Account AWS nel tuo sistema operativo corrente Regione AWS.
 - **Applica patch solo alle istanze di destinazione specificate:** è possibile specificare i nodi gestiti da assegnare nel passaggio successivo.
7. Utilizzare questa fase solo se è stato scelto **Applica patch solo alle istanze di destinazione specificate** nella fase precedente. Nella sezione **Selezione target**, identificare i nodi gestiti in cui si desidera eseguire questa operazione specificando i tag, selezionando i nodi gestiti manualmente o specificando un gruppo di risorse.

 Note

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

Se scegli come target un gruppo di risorse, tieni presente che i gruppi di risorse basati su uno AWS CloudFormation stack devono comunque essere contrassegnati con il `aws:cloudformation:stack-id` tag predefinito. Se è stato rimosso, Patch Manager potrebbe non essere in grado di determinare quali nodi gestiti appartengono al gruppo di risorse.

8. (Facoltativo) Per Archiviazione di log di applicazione di patch, se si desidera creare e salvare i log da questa operazione di applicazione di patch, selezionare il bucket S3 per la memorizzazione dei log.

 Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud](#). Inoltre, se il bucket S3 specificato si trova in un altro Account AWS, assicurati che il profilo di istanza o il ruolo del servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere in quel bucket.

9. (Facoltativo) Se si desidera eseguire documenti SSM come hook del ciclo di vita durante punti specifici dell'operazione di applicazione di patch, eseguire le operazioni seguenti:
 - Scegliere Usa hook del ciclo di vita.
 - Per ogni hook disponibile, selezionare il documento SSM da eseguire nel punto specificato dell'operazione:
 - Prima dell'installazione
 - Dopo l'installazione
 - All'uscita

- Dopo il riavvio pianificato

 Note

Il documento predefinito, AWS-Noop, non esegue alcuna operazione.

10. Scegli Applica patch ora.

Viene aperta la pagina Resoconto di esecuzione dell'associazione. (Patch ora utilizza le associazioni inState Manager, per le sue operazioni.) Nell'area Riepilogo dell'operazione è possibile monitorare lo stato della scansione o dell'applicazione di patch nei nodi gestiti specificati.

Apertura con le baseline delle patch

Una baseline delle patch in Patch Manager definisce quali patch sono approvate per l'installazione sui nodi gestiti. È possibile specificare singolarmente le patch approvate o rifiutate. È possibile anche creare regole di approvazione automatica per specificare che determinati tipi di aggiornamenti (ad esempio, quelli critici) devono essere approvati automaticamente. L'elenco dei rifiutati ha la priorità sulle regole e sull'elenco di quelli approvati. Per utilizzare un elenco di patch approvate per installare pacchetti specifici, è necessario, innanzitutto, rimuovere tutte le regole di approvazione automatica. Quando identifichi esplicitamente una patch come rifiutata, non verrà approvata né installata, anche se corrisponde a tutti i criteri specificati in una regola di approvazione automatica. Inoltre, verrà installata una patch in un nodo gestito solo se è valida per il software del nodo, anche se tale patch è stata comunque approvata per il nodo gestito.

Ulteriori informazioni

- [Baseline delle patch](#)

Visualizzazione AWS linee di base predefinite delle patch

Patch Manager include una baseline di patch predefinita per ogni sistema operativo supportato da Patch Manager. È possibile utilizzare queste baseline delle patch predefinite, che non possono essere personalizzate, oppure crearne una personale. La procedura seguente descrive come visualizzare una baseline delle patch predefinita per vedere se soddisfa le proprie esigenze. Per ulteriori informazioni sulle baseline delle patch, consulta [Baseline delle patch predefinite e personalizzate](#).

Per visualizzare AWS linee di base predefinite delle patch

1. Aprire la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Patch Manager.
3. Nell'elenco delle baseline delle patch scegliere l'ID di una delle baseline delle patch predefinite.

oppure

Se è la prima volta che accedi a Patch Manager nella Regione AWS corrente, scegli Inizia con una panoramica, scegli la scheda Baseline delle patch, quindi scegli l'ID di baseline delle patch predefinite.

Note

Per Windows Server, vengono fornite tre baseline delle patch predefinite. Le baseline delle patch AWS-DefaultPatchBaseline e AWS-WindowsPredefinedPatchBaseline-OS supportano solo gli aggiornamenti del sistema operativo Windows stesso. AWS-DefaultPatchBaselineViene utilizzato come baseline delle patch di default per nodi gestiti Windows Server a meno che non si specifichi una baseline delle patch diversa. Le impostazioni di configurazione in queste due baseline delle patch sono le stesse. Il più recente dei due, AWS-WindowsPredefinedPatchBaseline-OS, è stato creato per distinguerlo dalla terza baseline delle patch predefinita per Windows Server. Quella baseline delle patch, AWS-WindowsPredefinedPatchBaseline-OS-Applications, può essere utilizzata per applicare patch sia nel sistema operativo Windows Server che nelle applicazioni supportate rilasciate da Microsoft.

Per ulteriori informazioni, consulta [Impostare una baseline delle patch esistente come predefinita](#).

4. Nella sezione Regole di approvazione, rivedi la configurazione della baseline delle patch.
5. Se la configurazione è accettabile per i tuoi nodi gestiti, è possibile passare direttamente alla procedura [Creazione e gestione di gruppi di patch](#).

oppure

Per creare una baseline delle patch predefinita personale, proseguire con l'argomento [Utilizzo delle baseline delle patch personalizzate](#).

Utilizzo delle baseline delle patch personalizzate

Patch Manager include una baseline di patch predefinita per ogni sistema operativo supportato da Patch Manager. È possibile utilizzare queste baseline delle patch predefinite, che non possono essere personalizzate, oppure crearne una personale.

Le seguenti procedure descrivono come creare, aggiornare e cancellare le proprie baseline delle patch personalizzate. Per ulteriori informazioni sulle baseline delle patch, consulta [Baseline delle patch predefinite e personalizzate](#).

Creazione di una baseline delle patch personalizzata per Linux

Usa la seguente procedura per creare una baseline di patch personalizzata per i nodi gestiti da Linux in Patch Manager.

Per informazioni sulla creazione di una baseline delle patch per i nodi gestiti macOS, vedi [Creazione di una baseline di patch personalizzata per macOS](#). Per informazioni sulla creazione di una baseline delle patch per i nodi gestiti di Windows, consulta [Creazione di una baseline di patch personalizzata per Windows Server](#).

Per creare una baseline delle patch personalizzata per i nodi gestiti da Linux

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Patch Manager.
3. Scegli la scheda Baseline delle patch e quindi Crea baseline delle patch.

oppure

Se è la prima volta che accedi a Patch Manager nella Regione AWS corrente, scegli Inizia da una panoramica, scegli la scheda baseline delle patch e quindi Crea una baseline delle patch.

4. Nel campo Nome inserisci il nome della nuova baseline delle patch, ad esempio MyRHELPatchBaseline.
5. (Facoltativo) Per Descrizione, inserisci una descrizione per questa baseline delle patch.
6. Per Sistema operativo, scegli un sistema operativo, ad esempio Red Hat Enterprise Linux.
7. Se desideri iniziare a utilizzare questa baseline della patch come baseline predefinita per il sistema operativo selezionato non appena la crei, seleziona la casella accanto a Imposta questa patch baseline come baseline della patch predefinita per le istanze. **operating system name**

 Note

Questa opzione è disponibile solo se hai effettuato l'accesso per la prima volta a Patch Manager prima del rilascio delle [policy di patch](#) del 22 dicembre 2022.

Per informazioni sull'impostazione di una baseline delle patch esistente come predefinita, consulta [Impostare una baseline delle patch esistente come predefinita](#).

8. Nella sezione Regole di approvazione per sistema operativo utilizza i campi per creare una o più regole di approvazione automatica.

- **Prodotti:** la versione del sistema operativo a cui si applica la regola di approvazione, ad esempio `RedhatEnterpriseLinux7.4`. L'opzione predefinita è `All`.
- **Classificazione:** il tipo di patch a cui si applica la regola di approvazione, ad esempio `Security` o `Enhancement`. L'opzione predefinita è `All`.

 Tip

È possibile configurare una baseline delle patch per controllare se sono installati aggiornamenti di versione secondaria per Linux, ad esempio RHEL 7.8. Aggiornamenti di versione secondari possono essere installati in automatico da Patch Manager a condizione che l'aggiornamento sia disponibile nel repository appropriato.

Per i sistemi operativi Linux, gli aggiornamenti delle versioni secondari non sono classificati in modo coerente. Possono essere classificati come correzioni di bug o aggiornamenti di sicurezza, o non classificati, anche all'interno della stessa versione del kernel. Ecco alcune opzioni per controllare se una baseline delle patch ne esegue l'installazione.

- **Opzione 1:** la regola di approvazione più ampia per assicurarsi che gli aggiornamenti delle versioni minori vengano installati quando disponibili è specificare **Classificazione** come `All (*)` e scegliere l'opzione **Includi aggiornamenti non di sicurezza**.
- **Opzione 2:** per assicurarti che le patch per una versione del sistema operativo siano installate, puoi utilizzare un carattere jolly (*) per specificarne il formato del kernel nella sezione **Eccezioni delle patch** della **linea di base**. Ad esempio, il formato del kernel per RHEL 7.* è `kernel-3.10.0-*.el7.x86_64`.

Entra `kernel-3.10.0-*.el7.x86_64` nell'elenco delle patch approvate nella baseline delle patch per assicurarti che tutte le patch, inclusi gli aggiornamenti delle versioni minori, siano applicate ai nodi gestiti 7.*. RHEL (Se conosci il nome esatto del pacchetto di una patch di versione secondaria, è possibile inserirlo quello invece.)

- Opzione 3: puoi avere il massimo controllo sulle patch applicate ai nodi gestiti, inclusi gli aggiornamenti delle versioni minori, utilizzando il parametro nel documento. [InstallOverrideList](#) AWS-RunPatchBaseline Per ulteriori informazioni, consulta [Documento di comando SSM per l'applicazione di patch: AWS-RunPatchBaseline](#).

- Gravità: il valore di gravità delle patch a cui si applica la regola, ad esempio `Critical`. L'opzione predefinita è `All`.
- Auto-approval: il metodo per selezionare le patch per l'approvazione automatica.

Note

Poiché non è possibile determinare in modo affidabile le date di rilascio dei pacchetti di aggiornamento per Ubuntu Server, le opzioni di approvazione automatica non sono supportate per questo sistema operativo.

- Approva le patch dopo un determinato numero di giorni: il numero di giorni in cui Patch Manager Patch Manager deve attendere dopo il rilascio o l'ultimo aggiornamento di una patch prima che una patch venga approvata automaticamente. È possibile inserire qualsiasi numero intero da zero (0) a 360. Per la maggior parte degli scenari, consigliamo di attendere non più di 100 giorni.
- Approva le patch rilasciate fino a una data specifica: la data di rilascio delle patch per la quale Patch Manager applica automaticamente tutte le patch rilasciate o aggiornate prima di tale data (inclusa). Ad esempio, se specifichi il 7 luglio 2023, nessuna patch rilasciata o aggiornata a partire dall'8 luglio 2023 verrà installata automaticamente.
- (Facoltativo) Report di conformità: il livello di gravità da assegnare alle patch approvate dalla baseline, ad esempio `Critical` o `High`.

 Note

Se specifichi un livello di report di conformità e lo stato delle patch approvate viene riportato come Missing, la gravità di conformità complessiva riportata dalla baseline delle patch corrisponde al livello di gravità specificato.

- Includi aggiornamenti non relativi alla sicurezza: seleziona la casella per installare le patch del sistema operativo Linux non relative alla sicurezza disponibili nel repository di origine, oltre a quelle relative alla sicurezza.

Per ulteriori informazioni sulle operazioni con le regole di approvazione in una baseline delle patch personalizzata, consulta [Baseline personalizzate](#).

9. Se desideri approvare esplicitamente qualsiasi patch oltre a quelle che soddisfano le tue regole di approvazione, procedi come segue nella sezione Eccezioni delle patch:

- In Patch approvate, inserisci un elenco separato da virgole delle patch che desideri approvare.

Per informazioni sui formati accettati per gli elenchi delle patch approvate e di quelle rifiutate, consulta [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#).

- (Facoltativo) In Livello di conformità patch approvate, assegna un livello di conformità alle patch dell'elenco.
 - Se qualche patch approvata e specificata non è correlata alla sicurezza, seleziona la casella di controllo Includi aggiornamenti non critici per installare anche queste patch sul sistema operativo Linux.
10. Per rifiutare esplicitamente qualsiasi patch oltre che comunque soddisfano le regole di approvazione, procedere come segue nella sezione Eccezioni patch:

- In Patch rifiutate, inserisci un elenco separato da virgole delle patch che desideri rifiutare.

Per informazioni sui formati accettati per gli elenchi delle patch approvate e di quelle rifiutate, consulta [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#).

- In Operazione patch rifiutate, seleziona l'operazione che Patch Manager effettuerà sulle patch incluse nell'elenco Patch rifiutate.
- Consenti come dipendenza: un pacchetto dell'elenco Patch rifiutate viene installato solo se è incluso automaticamente in un altro pacchetto. È considerata conforme alla baseline della

patch e il suo stato viene riportato come. `InstalledOther` Si tratta dell'operazione predefinita se non viene specificata alcuna opzione.

- Blocca: i pacchetti dell'elenco Patch rifiutate e quelli che le includono come dipendenze non verranno installati da Patch Manager in alcun caso. Se un pacchetto è stato installato prima di essere stato aggiunto all'elenco Patch rifiutate, oppure è stato successivamente installato fuori da Patch Manager, viene considerato non conforme alla baseline delle patch e il relativo stato è `InstalledRejected`.

Note

Patch Manager cerca le dipendenze delle patch in modo ricorsivo.

11. (Facoltativo) Se desideri specificare repository di patch alternativi per diverse versioni di un sistema operativo, ad esempio `AmazonLinux2016.03` e `AmazonLinux2017.09`, procedi come segue per ogni prodotto nella sezione Sorgenti delle patch:

- In Nome, inserisci un nome per semplificare l'identificazione della configurazione di origine.
- In Prodotto, seleziona la versione dei sistemi operativi a cui è destinato il repository di origine delle patch, ad esempio `RedhatEnterpriseLinux7.4`.
- In Configurazione, immetti il valore della configurazione del repository da utilizzare nel formato appropriato:

Example for yum repositories

```
[main]
name=MyCustomRepository
baseurl=https://my-custom-repository
enabled=1
```

Tip

Per informazioni sulle altre opzioni disponibili per la configurazione del repository yum, consulta [dnf.conf\(5\)](#).

Examples for Ubuntu Server and Debian Server

```
deb http://security.ubuntu.com/ubuntu jammy main
```

```
deb https://site.example.com/debian distribution component1  
component2 component3
```

Le informazioni sui repository per quelli di Ubuntu Server devono essere specificate in un'unica riga. Per ulteriori esempi e informazioni, consulta [jammy \(5\) sources.list.5.gz](#) sul sito web dei Manuali di Ubuntu Server e [il formato sources.list](#) sulla Wiki Debian.

Sceglie Aggiungi un'altra origine per specificare un repository di origine per ciascuna versione aggiuntiva del sistema operativo, fino a un massimo di 20.

Per ulteriori informazioni sui repository di patch di origine alternativi, consulta [Come specificare un repository alternativo di origine delle patch \(Linux\)](#).

12. (Facoltativo) Per la gestione dei tag, applicate una o più name/value coppie di tag key alla baseline della patch.

I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Ad esempio, è possibile applicare tag a una baseline delle patch per identificare il livello di gravità delle patch che specifica, la famiglia del sistema operativo a cui si applica e il tipo di ambiente. In questo caso, è possibile specificare tag simili alle seguenti name/value coppie di chiavi:

- Key=PatchSeverity, Value=Critical
- Key=OS, Value=RHEL
- Key=Environment, Value=Production

13. Scegli Crea una baseline delle patch.

Creazione di una baseline di patch personalizzata per macOS

Utilizza la seguente procedura per creare una baseline di patch personalizzata per i nodi macOS gestiti in Patch Manager.

Per informazioni sulla creazione di una baseline delle patch per i nodi gestiti Windows Server, vedi [Creazione di una baseline di patch personalizzata per Windows Server](#). Per informazioni sulla creazione di una baseline delle patch per i nodi gestiti Linux, vedi [Creazione di una baseline delle patch personalizzata per Linux](#).

 Note

macOS non è supportato in tutte le Regioni AWS. Per ulteriori informazioni sul supporto di Amazon EC2 per macOS, consulta [Istanze Amazon EC2 Mac](#) nella Guida per l'utente di Amazon EC2.

Per creare una baseline di patch personalizzata per macOS nodi gestiti

1. Aprire la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Patch Manager.
3. Scegli la scheda Baseline delle patch e quindi Crea baseline delle patch.

oppure

Se è la prima volta che accedi a Patch Manager nella Regione AWS corrente, scegli Inizia da una panoramica, scegli la scheda baseline delle patch e quindi Crea una baseline delle patch.

4. Nel campo Nome inserisci il nome della nuova baseline delle patch, ad esempio MymacOSPatchBaseline.
5. (Facoltativo) Per Descrizione, inserisci una descrizione per questa baseline delle patch.
6. Per Sistema operativo, seleziona macOS.
7. Se desideri cominciare a utilizzare subito la baseline delle patch appena creata come impostazione predefinita per macOS, seleziona la casella vicino a Rendi predefinita questa baseline delle patch per le istanze di macOS.

 Note

Questa opzione è disponibile solo se hai effettuato l'accesso per la prima volta a Patch Manager prima del rilascio delle [policy di patch](#) del 22 dicembre 2022.
Per informazioni sull'impostazione di una baseline delle patch esistente come predefinita, consulta [Impostare una baseline delle patch esistente come predefinita](#).

8. Nella sezione Regole di approvazione per sistema operativo utilizza i campi per creare una o più regole di approvazione automatica.

- **Prodotti:** la versione del sistema operativo a cui si applica la regola di approvazione, ad esempio `BigSur11.3.1` o `Ventura13.7`. L'opzione predefinita è `All`.
- **Classificazione:** Il gestore di pacchetti o i gestori di pacchetti a cui si desidera applicare i pacchetti durante il processo di applicazione delle patch. È possibile scegliere tra le seguenti opzioni:
 - `softwareupdate`
 - `Installer` (Programma di installazione)
 - `Brew`
 - `Brew cask`

L'opzione predefinita è `All`.

- (Facoltativo) **Report di conformità:** il livello di gravità da assegnare alle patch approvate dalla baseline, ad esempio `Critical` o `High`.

 Note

Quando si specifica un livello di report di conformità e lo stato delle patch approvate viene riportato come `Missing`, la gravità di conformità complessiva riportata dalla baseline delle patch corrisponde al livello di gravità specificato.

Per ulteriori informazioni sulle operazioni con le regole di approvazione in una baseline delle patch personalizzata, consulta [Baseline personalizzate](#).

9. Se desideri approvare esplicitamente qualsiasi patch oltre a quelle che soddisfano le tue regole di approvazione, procedi come segue nella sezione **Eccezioni delle patch**:
 - In **Patch approvate**, inserisci un elenco separato da virgole delle patch che desideri approvare.

Per informazioni sui formati accettati per gli elenchi delle patch approvate e di quelle rifiutate, consulta [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#).
 - (Facoltativo) In **Livello di conformità patch approvate**, assegna un livello di conformità alle patch dell'elenco.
10. Per rifiutare esplicitamente qualsiasi patch oltre che comunque soddisfano le regole di approvazione, procedere come segue nella sezione **Eccezioni patch**:
 - In **Patch rifiutate**, inserisci un elenco separato da virgole delle patch che desideri rifiutare.

Per informazioni sui formati accettati per gli elenchi delle patch approvate e di quelle rifiutate, consulta [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#).

- In Operazione patch rifiutate, seleziona l'operazione che Patch Manager effettuerà sulle patch incluse nell'elenco Patch rifiutate.
 - Consenti come dipendenza: un pacchetto dell'elenco Patch rifiutate viene installato solo se è incluso automaticamente in un altro pacchetto. È considerata conforme alla baseline della patch e il suo stato viene riportato come. `InstalledOther` Si tratta dell'operazione predefinita se non viene specificata alcuna opzione.
 - Blocca: i pacchetti dell'elenco Patch rifiutate e quelli che le includono come dipendenze non verranno installati da Patch Manager in alcun caso. Se un pacchetto è stato installato prima di essere stato aggiunto all'elenco Patch rifiutate, oppure è stato successivamente installato fuori da Patch Manager, viene considerato non conforme alla baseline delle patch e il relativo stato è `InstalledRejected`.

11. (Facoltativo) Per `Manage tags`, applicate una o più name/value coppie di tag key alla baseline della patch.

I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Ad esempio, è possibile applicare tag a una baseline delle patch per identificare il livello di gravità delle patch che specifica, il gestore di pacchetti a cui si applica e il tipo di ambiente. In questo caso, è possibile specificare tag simili alle seguenti name/value coppie di chiavi:

- `Key=PatchSeverity,Value=Critical`
- `Key=PackageManager,Value=softwareupdate`
- `Key=Environment,Value=Production`

12. Scegli Crea una baseline delle patch.

Creazione di una baseline di patch personalizzata per Windows Server

Utilizza la procedura seguente per creare una baseline di patch personalizzata per i nodi gestiti da Windows in. Patch Manager

Per informazioni sulla creazione di una baseline delle patch per i nodi gestiti Linux, vedi [Creazione di una baseline delle patch personalizzata per Linux](#). Per informazioni sulla creazione di baseline delle patch per i nodi gestiti da macOS, vedi [Creazione di una baseline di patch personalizzata per macOS](#).

Per un esempio di creazione di una baseline delle patch limitata solo all'installazione di Windows Service Pack, consulta [Tutorial: creare una baseline delle patch per l'installazione di Windows Service Pack tramite la console](#).

Creazione di una baseline delle patch personalizzata (Windows)

1. Aprire la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Patch Manager.
3. Scegli la scheda Baseline delle patch e quindi Crea baseline delle patch.

oppure

Se è la prima volta che accedi a Patch Manager nella Regione AWS corrente, scegli Inizia da una panoramica, scegli la scheda baseline delle patch e quindi Crea una baseline delle patch.

4. Nel campo Nome inserisci il nome della nuova baseline delle patch, ad esempio MyWindowsPatchBaseline.
5. (Facoltativo) Per Descrizione, inserisci una descrizione per questa baseline delle patch.
6. Per Sistema operativo, seleziona Windows.
7. Per lo stato di conformità degli aggiornamenti di sicurezza disponibili, scegli lo stato che desideri assegnare alle patch di sicurezza disponibili ma non approvate perché non soddisfano i criteri di installazione specificati nella baseline delle patch Non-Compliant o Conforme.

Scenario di esempio: le patch di sicurezza che potresti voler installare possono essere ignorate, se hai specificato un lungo periodo di attesa dopo il rilascio di una patch prima dell'installazione. Se un aggiornamento della patch viene rilasciato durante il periodo di attesa specificato, il periodo di attesa per l'installazione della patch ricomincia da capo. Se il periodo di attesa è troppo lungo, è possibile che più versioni della patch vengano rilasciate, ma non installate mai.

8. Se desideri iniziare a utilizzare subito questa baseline delle patch appena creata come impostazione predefinita per Windows, seleziona Rendi predefinita questa baseline delle patch per le istanze di Windows Server.

Note

Questa opzione è disponibile solo se hai effettuato l'accesso per la prima volta a Patch Manager prima del rilascio delle [policy di patch](#) del 22 dicembre 2022.

Per informazioni sull'impostazione di una baseline delle patch esistente come predefinita, consulta [Impostare una baseline delle patch esistente come predefinita](#).

9. Nella sezione Regole di approvazione per i sistemi operativi, utilizza i campi per creare una o più regole di approvazione automatica.

- **Prodotti:** la versione del sistema operativo a cui si applica la regola di approvazione, ad esempio `WindowsServer2012`. L'opzione predefinita è `All`.
- **Classificazione:** il tipo di patch a cui si applica la regola di approvazione, ad esempio `CriticalUpdates`, `Drivers` e `Tools`. L'opzione predefinita è `All`.

 Tip

È possibile includere le installazioni di Windows Service Pack nelle regole di approvazione includendo `ServicePacks` o scegliendo `All` nell'elenco **Classificazione**. Per vedere un esempio, consulta [Tutorial: creare una baseline delle patch per l'installazione di Windows Service Pack tramite la console](#).

- **Gravità:** il valore di gravità delle patch a cui si applica la regola, ad esempio `Critical`. L'opzione predefinita è `All`.
- **Auto-approval:** il metodo per selezionare le patch per l'approvazione automatica.
 - **Approva le patch dopo un determinato numero di giorni:** il numero di giorni in cui Patch Manager deve attendere dopo il rilascio o l'aggiornamento di una patch prima che una patch venga approvata automaticamente. È possibile inserire qualsiasi numero intero da zero (0) a 360. Per la maggior parte degli scenari, consigliamo di attendere non più di 100 giorni.
 - **Approva le patch rilasciate fino a una data specifica:** la data di rilascio delle patch per la quale Patch Manager applica automaticamente tutte le patch rilasciate o aggiornate prima di tale data (inclusa). Ad esempio, se si specifica il 7 luglio 2023, nessuna patch rilasciata o aggiornata a partire dall'8 luglio 2023 verrà installata automaticamente.
- **(Facoltativo) Report di conformità:** il livello di gravità da assegnare alle patch approvate dalla baseline, ad esempio `High`.

 Note

Se specifichi un livello di report di conformità e lo stato delle patch approvate viene riportato come `Missing`, la gravità di conformità complessiva riportata dalla baseline delle patch corrisponde al livello di gravità specificato.

10. (Facoltativo) Nella sezione Regole di approvazione per le applicazioni, utilizza i campi per creare una o più regole di approvazione automatica.

 Note

Anziché specificare le regole di approvazione, è possibile specificare elenchi di patch approvate e rifiutate come eccezioni di patch. Vedere i passaggi 10 e 11.

- **Famiglia di prodotti:** la famiglia di prodotti Microsoft generale per cui si desidera specificare una regola, ad esempio `Office` o `Exchange Server`.
- **Prodotti:** la versione dell'applicazione a cui si applica la regola di approvazione, ad esempio `Office 2016` o `Active Directory Rights Management Services Client 2.0 2016`. L'opzione predefinita è `All`.
- **Classificazione:** il tipo di patch a cui si applica la regola di approvazione, ad esempio `CriticalUpdates`. L'opzione predefinita è `All`.
- **Gravità:** il valore di gravità delle patch a cui si applica la regola, ad esempio `Critical`. L'opzione predefinita è `All`.
- **Auto-approval:** Il metodo per selezionare le patch per l'approvazione automatica.
 - **Approva le patch dopo un determinato numero di giorni:** il numero di giorni in cui Patch Manager Patch Manager deve attendere dopo il rilascio o l'aggiornamento di una patch prima che una patch venga approvata automaticamente. È possibile inserire qualsiasi numero intero da zero (0) a 360. Per la maggior parte degli scenari, consigliamo di attendere non più di 100 giorni.
 - **Approva le patch rilasciate fino a una data specifica:** la data di rilascio delle patch per la quale Patch Manager applica automaticamente tutte le patch rilasciate o aggiornate prima di tale data (inclusa). Ad esempio, se specifichi il 7 luglio 2023, nessuna patch rilasciata o aggiornata a partire dall'8 luglio 2023 verrà installata automaticamente.

- (Facoltativo) Report di conformità: il livello di gravità da assegnare alle patch approvate dalla baseline, ad esempio `Critical` o `High`.

 Note

Se si specifica un livello di report di conformità e lo stato delle patch approvate viene riportato come `Missing`, la gravità di conformità complessiva riportata dalla baseline delle patch corrisponde al livello di gravità specificato.

11. (Facoltativo) Per approvare esplicitamente qualsiasi patch anziché selezionare patch in base alle regole di approvazione, completa la procedura seguente nella sezione Eccezioni di patch:

- In Patch approvate, inserisci un elenco separato da virgole delle patch che desideri approvare.

Per informazioni sui formati accettati per gli elenchi delle patch approvate e di quelle rifiutate, consulta [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#).

- (Facoltativo) In Livello di conformità patch approvate, assegna un livello di conformità alle patch dell'elenco.
12. Per rifiutare esplicitamente qualsiasi patch oltre che comunque soddisfano le regole di approvazione, procedere come segue nella sezione Eccezioni patch:
- In Patch rifiutate, inserisci un elenco separato da virgole delle patch che desideri rifiutare.
- Per informazioni sui formati accettati per gli elenchi delle patch approvate e di quelle rifiutate, consulta [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#).
- In Operazione patch rifiutate, seleziona l'operazione che Patch Manager effettuerà sulle patch incluse nell'elenco Patch rifiutate.
 - Consenti come dipendenza: Windows Server non supporta il concetto di dipendenza dei pacchetti. Quando un pacchetto nell'elenco delle patch rifiutate è già installato sul nodo, lo stato viene riportato come `INSTALLED_OTHER`. Qualsiasi pacchetto non già installato sul nodo viene ignorato.
 - Blocco: i pacchetti nell'elenco delle Patch rifiutate non vengono installati da Patch Manager in nessun caso. Se un pacchetto è stato installato prima di essere stato aggiunto all'elenco Patch rifiutate, oppure è stato successivamente installato fuori da Patch Manager, viene considerato non conforme alla baseline delle patch e il relativo stato è `INSTALLED_REJECTED`.

Per ulteriori informazioni sulle operazioni relative ai pacchetti rifiutati, consulta le [Opzioni dell'elenco delle patch rifiutate nelle baseline delle patch personalizzate](#).

13. (Facoltativo) Per la gestione dei tag, applica una o più name/value coppie di tag key alla baseline della patch.

I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Ad esempio, è possibile applicare tag a una baseline delle patch per identificare il livello di gravità delle patch che specifica, la famiglia del sistema operativo a cui si applica e il tipo di ambiente. In questo caso, è possibile specificare tag simili alle seguenti name/value coppie di chiavi:

- Key=PatchSeverity, Value=Critical
- Key=OS, Value=RHEL
- Key=Environment, Value=Production

14. Scegli Crea una baseline delle patch.

Aggiornamento o eliminazione di una baseline delle patch personalizzata

È possibile aggiornare o eliminare una baseline di patch personalizzata in cui è stata creata. Patch Manager Quando si aggiorna una baseline delle patch, è possibile modificare il nome, la descrizione, le regole di approvazione e le eccezioni per le patch approvate e rifiutate. Si possono aggiornare anche i tag che vengono applicati alla baseline delle patch. Non è possibile modificare il tipo di sistema operativo per cui è stata creata una baseline di patch e non è possibile apportare modifiche a una baseline di patch predefinita fornita da AWS.

Aggiornamento o eliminazione di una baseline delle patch

Segui questi passaggi per aggiornare o eliminare una baseline delle patch.

Important

Presta attenzione durante l'eliminazione di una baseline delle patch personalizzata che potrebbe essere utilizzata da una configurazione delle policy di patch in Quick Setup.

Se utilizzi una [configurazione della policy di patch](#) in Quick Setup, gli aggiornamenti apportati alle baseline delle patch personalizzate vengono sincronizzati con Quick Setup una volta ogni ora.

Quando si elimina una baseline delle patch personalizzata a cui si fa riferimento in una policy di patch, viene visualizzato un banner nella pagina Dettagli di configurazione di Quick Setup relativa alla policy di patch. Il banner informa che la policy di patch fa riferimento a una baseline delle patch che non esiste più, di conseguenza le successive operazioni di applicazione di patch avranno esito negativo. In questo caso, torna alla pagina Configurazioni di Quick Setup, seleziona la configurazione Patch Manager e scegli Operazioni, Modifica configurazione. Il nome della baseline delle patch eliminata viene evidenziato ed è necessario selezionare una nuova baseline delle patch per il sistema operativo interessato.

Aggiornamento o eliminazione di una baseline delle patch

1. Apri la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Patch Manager.
3. Scegliere la baseline delle patch che si desidera aggiornare o eliminare ed eseguire una delle operazioni seguenti:
 - Per rimuovere la baseline della patch dal tuo Account AWS, scegli Elimina. Il sistema richiede di confermare le operazioni.
 - Per modificare il nome o la descrizione della baseline delle patch, le regole di approvazione o le eccezioni relative alle patch, scegliere Modifica. Nella pagina Modifica delle baseline delle patch, modifica i valori e le opzioni desiderate, quindi scegli Salva le modifiche.
 - Per aggiungere, modificare o eliminare i tag applicati alla baseline delle patch, scegli la scheda Tag, quindi scegli Modifica tag. Nella pagina Modifica tag della baseline delle patch, aggiorna i tag della baseline delle patch e scegli Salva le modifiche.

Per informazioni sulle scelte di configurazione disponibili, consulta [Utilizzo delle baseline delle patch personalizzate](#).

Impostare una baseline delle patch esistente come predefinita

Important

Qualsiasi selezione delle baseline delle patch predefinite effettuata qui non si applica alle operazioni basate su una policy di patch. Le policy di patch utilizzano le proprie specifiche per

le baseline delle patch. Per ulteriori informazioni sulle policy di patch, consulta [Configurazioni delle policy sulle patch in Configurazione rapida](#).

Quando si crea una baseline di patch personalizzata in Patch Manager, è possibile impostare la baseline come predefinita per il tipo di sistema operativo associato non appena la si crea. Per informazioni, consulta [Utilizzo delle baseline delle patch personalizzate](#).

È possibile anche impostare una baseline delle patch come predefinita per un tipo di sistema operativo.

Note

I passaggi da seguire dipendono dal fatto che tu abbia effettuato l'accesso a Patch Manager per la prima volta prima o dopo il rilascio delle policy di patch il 22 dicembre 2022. Se l'hai usato Patch Manager prima di quella data, è possibile utilizzare la procedura della console. Altrimenti, utilizzare la procedura AWS CLI. Il menu Operazioni a cui si fa riferimento nella procedura della console non viene visualizzato nelle regioni in cui Patch Manager non è stato utilizzato prima del rilascio delle policy di patch.

Per impostare una baseline delle patch come predefinita

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Patch Manager.
3. Selezionare la scheda baseline delle patch
4. Nell'elenco delle baseline delle patch scegliere il pulsante di una baseline delle patch che attualmente non è impostata come predefinita per un tipo di sistema operativo.

La colonna Baseline predefinita indica le baseline attualmente impostate come predefinite.

5. Nel menu Operazioni, scegli Imposta baseline delle patch predefinita.

 Important

Il menu Azioni non è disponibile se non hai lavorato con Patch Manager la versione attuale Account AWS e la regione prima del 22 dicembre 2022. Per ulteriori informazioni, consulta la nota riportata in precedenza in questo argomento.

6. Nella finestra di dialogo di conferma, scegli Imposta la configurazione predefinita.

Per impostare una baseline di patch come impostazione predefinita (AWS CLI)

1. Esegui il comando [describe-patch-baselines](#) per visualizzare un elenco delle baseline delle patch disponibili con i relativi ID e nomi delle risorse Amazon (ARN).

```
aws ssm describe-patch-baselines
```

2. Esegui il comando [register-default-patch-baseline](#) per impostare una baseline come predefinita per il sistema operativo a cui è associata. Sostituire *baseline-id-or-ARN* con l'ID della baseline della patch personalizzata o della baseline predefinita da utilizzare.

Linux & macOS

```
aws ssm register-default-patch-baseline \  
--baseline-id baseline-id-or-ARN
```

Di seguito è riportato un esempio di impostazione di una baseline personalizzata come impostazione predefinita.

```
aws ssm register-default-patch-baseline \  
--baseline-id pb-abc123cf9bEXAMPLE
```

Di seguito è riportato un esempio di impostazione di una baseline predefinita gestita come predefinita. AWS

```
aws ssm register-default-patch-baseline \  
--baseline-id arn:aws:ssm:us-east-2:733109147000:patchbaseline/  
pb-0574b43a65ea646e
```

Windows Server

```
aws ssm register-default-patch-baseline ^  
  --baseline-id baseline-id-or-ARN
```

Di seguito è riportato un esempio di impostazione di una baseline personalizzata come impostazione predefinita.

```
aws ssm register-default-patch-baseline ^  
  --baseline-id pb-abc123cf9bEXAMPLE
```

Di seguito è riportato un esempio di impostazione di una baseline predefinita gestita da AWS come predefinita.

```
aws ssm register-default-patch-baseline ^  
  --baseline-id arn:aws:ssm:us-east-2:733109147000:patchbaseline/  
pb-071da192df1226b63
```

Visualizzazione delle patch disponibili

Con Patch Manager, è possibile visualizzare tutte le patch disponibili per un sistema operativo specificato e, facoltativamente, una versione specifica del sistema operativo.

Tip

Per generare un elenco di patch disponibili e salvarle in un file, è possibile utilizzare il comando [describe-available-patches](#) e specificare il tuo [output](#) preferito.

Visualizzazione delle patch disponibili

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Patch Manager.
3. Seleziona la scheda Patch.

oppure

Se è la prima volta che accedi a Patch Manager nella Regione AWS corrente, scegli Inizia da una panoramica e quindi scegli la scheda Patch.

Note

Per Windows Server, la scheda Patch mostra gli aggiornamenti disponibili da Windows Server Update Service (WSUS).

4. Per Sistema operativo, seleziona il sistema operativo per il quale desideri visualizzare le patch disponibili, ad esempio Windows o Amazon Linux.
5. (Facoltativo) Per Prodotto, scegliere una versione del sistema operativo, ad esempio WindowsServer2019 o AmazonLinux2018.03.
6. (Facoltativo) Per aggiungere o rimuovere colonne di informazioni per i risultati, scegli il pulsante Configura



in alto a destra dell'elenco Patch. (Per impostazione predefinita, la scheda Patch visualizza le colonne solo per alcuni metadati delle patch disponibili.)

Per informazioni sui tipi di metadati che è possibile aggiungere alla visualizzazione, consulta [Patch](#) nella Documentazione di riferimento API di AWS Systems Manager .

Creazione e gestione di gruppi di patch

Se non utilizzi le politiche di patch, puoi organizzare l'applicazione delle patch aggiungendo nodi gestiti ai gruppi di patch utilizzando i tag.

Note

I gruppi di patch non vengono utilizzati nelle operazioni di applicazione di patch basate su policy di patch. Per informazioni sull'utilizzo delle policy di patch, consulta [Configurazioni delle policy sulle patch in Configurazione rapida](#).

La funzionalità dei gruppi di patch non è supportata nella console per le coppie account-regione che non utilizzavano gruppi di patch prima del 22 dicembre 2022. È ancora disponibile nelle coppie account-regione che utilizzavano gruppi di patch prima di questa data.

Per utilizzare i tag nelle operazioni di applicazione di patch, devi applicare la chiave dei tag Patch Group o PatchGroup ai nodi gestiti. Devi inoltre specificare il nome che desideri assegnare al gruppo di patch come valore del tag. È possibile specificare un valore tag qualsiasi, ma la chiave di tag deve essere Patch Group o PatchGroup.

PatchGroup (senza spazio) è necessario se sono presenti [tag consentiti nei metadati dell'istanza EC2](#).

Dopo aver raggruppato i nodi gestiti utilizzando i tag, aggiungere il valore del gruppo di patch a una baseline delle patch. Registrando il gruppo di patch con una baseline di patch, ci si assicura che durante l'operazione di patching vengano installate le patch corrette. Per ulteriori informazioni sui gruppi di patch, consulta [Gruppi di patch](#).

Completa le attività descritte in questo argomento per preparare i nodi gestiti all'applicazione di patch utilizzando i tag con i nodi e la baseline delle patch. L'attività 1 è richiesta solo se stai applicando patch a istanze Amazon EC2. L'attività 2 è richiesta solo se stai applicando patch a istanze non EC2 in un ambiente [ibrido e multicloud](#). L'attività 3 è richiesta per tutti i nodi gestiti.

Tip

È inoltre possibile aggiungere tag ai nodi gestiti utilizzando il AWS CLI comando [add-tags-to-resource](#) o l'operazione API di Systems Manager ssm-agent-minimum-s3-permissions-required. [AddTagsToResource](#)

Processi

- [Attività 1: aggiunta di istanze EC2 a un gruppo di patch mediante tag](#)
- [Attività 2: aggiunta di nodi gestiti a un gruppo di patch mediante i tag](#)
- [Attività 3: aggiunta di un gruppo di patch a una baseline delle patch](#)

Attività 1: aggiunta di istanze EC2 a un gruppo di patch mediante tag

È possibile aggiungere tag alle istanze EC2 utilizzando la console di Systems Manager o la console di Amazon EC2. Questa attività è richiesta solo se stai applicando patch a istanze Amazon EC2.

⚠ Important

Per applicare il tag Patch Group (con uno spazio) a un'istanza di Amazon EC2, l'opzione Consenti i tag nei metadati dell'istanza non deve essere abilitata sull'istanza. Consenti i tag nei metadati di istanza impedisce ai nomi delle chiavi dei tag di contenere spazi. Se hai [tag consentiti nei metadati dell'istanza EC2](#), è necessario utilizzare la chiave di tag PatchGroup (senza spazio).

Opzione 1: per aggiungere istanze EC2 a un gruppo di patch (console di Systems Manager)

1. <https://console.aws.amazon.com/systems-manager/>Aprire la console all'indirizzo. AWS Systems Manager
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Nell'elenco Nodi gestiti scegli l'ID dell'istanza EC2 gestita da configurare per l'applicazione di patch. Gli ID dei nodi per le istanze EC2 iniziano con i -.

📘 Note

Quando si utilizza la console Amazon EC2 AWS CLI, è possibile applicare Key = Patch Group o Key = PatchGroup contrassegnare istanze non ancora configurate per l'uso con Systems Manager.

Se un nodo che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

4. Seleziona la scheda Tag, quindi scegli Modifica.
5. Nella colonna di sinistra immettere **Patch Group** o **PatchGroup**. Se sono presenti [tag consentiti nei metadati dell'istanza EC2](#), è necessario utilizzare PatchGroup (senza spazio).
6. Nella colonna di destra inserisci un valore di tag da utilizzare come nome di questo gruppo di patch.
7. Scegli Salva.
8. Ripeti la procedura per aggiungere altre istanze EC2 allo stesso gruppo di patch.

Opzione 2: per aggiungere istanze EC2 a un gruppo di patch (console di Amazon EC2)

1. Apri la [console Amazon EC2](#) e nel pannello di navigazione scegli Istanze.
2. Nell'elenco delle istanze, scegline una da configurare per l'applicazione di patch.
3. Dal menu Operazioni, scegli Impostazioni istanza, Gestisci tag.
4. Scegli Aggiungi nuovo tag.
5. Per Chiave, immetti **Patch Group** o **PatchGroup**. Se sono presenti [tag consentiti nei metadati dell'istanza EC2](#), è necessario utilizzare PatchGroup (senza spazio).
6. Per Valore, immetti un valore da utilizzare come nome per il gruppo di patch.
7. Selezionare Salva.
8. Ripetere la procedura per aggiungere altre istanze allo stesso gruppo di patch.

Attività 2: aggiunta di nodi gestiti a un gruppo di patch mediante i tag

Segui i passaggi descritti in questo argomento per aggiungere tag ai dispositivi AWS IoT Greengrass principali e ai nodi gestiti ad attivazione ibrida non EC2 (mi-*). Questa attività è richiesta solo se stai applicando patch a istanze non EC2 in un ambiente ibrido e multicloud.

Note

Non è possibile aggiungere i tag per i nodi gestiti non EC2 utilizzando la console di Amazon EC2.

Per aggiungere nodi gestiti non EC2 a un gruppo di patch (console di Systems Manager)

1. AWS Systems Manager Apri <https://console.aws.amazon.com/systems-manager/> la console all'indirizzo.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Nell'elenco Nodi gestiti, scegli il nome del nodo gestito da configurare per l'applicazione di patch.

Note

Se un nodo che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

4. Seleziona la scheda Tag, quindi scegli Modifica.
5. Nella colonna di sinistra immettere **Patch Group** o **PatchGroup**. Se sono presenti [tag consentiti nei metadati dell'istanza EC2](#), è necessario utilizzare PatchGroup (senza spazio).
6. Nella colonna di destra inserisci un valore di tag da utilizzare come nome di questo gruppo di patch.
7. Scegli Salva.
8. Ripetere la procedura per aggiungere altri nodi gestiti allo stesso gruppo di patch.

Attività 3: aggiunta di un gruppo di patch a una baseline delle patch

Per associare una determinata baseline delle patch ai propri nodi gestiti, è necessario aggiungere il valore del gruppo di patch alla baseline delle patch. Registrando il gruppo di patch con una baseline di patch, è possibile assicurarsi che vengano installate le patch corrette durante un'operazione di patching. Questa attività è necessaria sia che si applichino patch a istanze EC2, nodi gestiti non EC2 o entrambi.

Per ulteriori informazioni sui gruppi di patch, consulta [Gruppi di patch](#).

Note

I passaggi da seguire dipendono dal fatto che tu abbia effettuato l'accesso a Patch Manager per la prima volta prima o dopo il rilascio delle [policy di patch](#) il 22 dicembre 2022.

Per aggiungere un gruppo di patch a una baseline delle patch (console di Systems Manager)

1. Aprire la console all'indirizzo. AWS Systems Manager <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Patch Manager.
3. Se accedi a Patch Manager per la prima volta nella Regione AWS corrente e si apre la pagina iniziale di Patch Manager, scegli Inizia con una panoramica.
4. Scegli la scheda baseline delle patch, quindi dall'elenco baseline delle patch scegli il nome della baseline delle patch da configurare per il gruppo di patch.

Se hai effettuato l'accesso per la prima volta a Patch Manager solo dopo il rilascio delle policy di patch, devi scegliere una baseline personalizzata che hai creato.

5. Se la pagina dei dettagli dell'ID baseline include un menu Operazioni, procedi come segue:

- Scegliere Operazioni, quindi Modifica i gruppi di patch.
- Inserisci il valore di tag aggiunto ai nodi gestiti in [Attività 2: aggiunta di nodi gestiti a un gruppo di patch mediante i tag](#), quindi scegli Aggiungi.

Se la pagina dei dettagli dell'ID baseline non include un menu Operazioni, i gruppi di patch non possono essere configurati nella console. È possibile invece procedere come descritto di seguito:

- (Consigliato) Configura una policy di patch in Quick Setup, uno strumento di AWS Systems Manager, per mappare una baseline delle patch su una o più istanze EC2.

Per ulteriori informazioni, consulta [Utilizzo delle policy di patch di Quick Setup](#) e [Automatizzazione dell'applicazione di patch a livello di organizzazione utilizzando una policy di patch di Quick Setup](#).

- Utilizzate il [register-patch-baseline-for-patch-group](#) comando in AWS Command Line Interface (AWS CLI) per configurare un gruppo di patch.

Integrazione Patch Manager con AWS Security Hub CSPM

[AWS Security Hub CSPM](#) ti offre una visione completa del tuo stato di sicurezza in. AWS Security Hub CSPM raccoglie dati di sicurezza da tutti Account AWS i prodotti di partner di terze parti supportati e supportati. Servizi AWS Con Security Hub CSPM, puoi verificare il tuo ambiente rispetto agli standard e alle best practice del settore della sicurezza. Security Hub CSPM ti aiuta ad analizzare le tendenze di sicurezza e a identificare i problemi di sicurezza con la massima priorità.

Utilizzando l'integrazione tra Security Hub CSPM Patch Manager, è possibile inviare i risultati relativi ai nodi non conformi da Security Hub CSPM. Patch Manager Un esito è la registrazione osservabile di un controllo di sicurezza o di un rilevamento correlato alla sicurezza. Security Hub CSPM può quindi includere i risultati relativi alle patch nell'analisi del tuo stato di sicurezza.

Le informazioni contenute negli argomenti seguenti si applicano indipendentemente dal metodo o dal tipo di configurazione utilizzato per le operazioni di applicazione di patch:

- Una policy di patch configurata in Quick Setup
- Un'opzione di gestione host configurata in Quick Setup
- Una finestra di manutenzione per eseguire un'attività Scan o Install di patch
- Un'operazione Applica subito una patch on demand

In che modo Patch Manager invia i risultati a Security Hub CSPM

In CSPM Security Hub, i problemi di sicurezza vengono monitorati come esiti. Alcuni risultati derivano da problemi rilevati da altri Servizi AWS o da partner terzi. Security Hub CSPM dispone anche di una serie di regole che utilizza per rilevare problemi di sicurezza e generare risultati.

Patch Manager è uno degli strumenti di Systems Manager che invia i risultati a Security Hub CSPM. Dopo aver eseguito un'operazione di patching eseguendo un documento SSM (AWS-RunPatchBaseline,, oAWS-RunPatchBaselineWithHooks)AWS-RunPatchBaselineAssociation, le informazioni sull'applicazione delle patch vengono inviate a Inventory o Compliance, tools in o entrambi. AWS Systems Manager Dopo che Inventory, Compliance o entrambi ricevono i dati, Patch Manager riceve una notifica. In seguito, Patch Manager valuta i dati per verificarne la precisione, la formattazione e la conformità. Se tutte le condizioni sono soddisfatte, Patch Manager inoltra i dati a Security Hub CSPM.

CSPM Security Hub fornisce strumenti per gestire gli esiti da tutte queste origini. È possibile visualizzare e filtrare gli elenchi di esiti e visualizzare i dettagli per un riscontro. Per ulteriori informazioni, consulta [Visualizzazione degli esiti](#) nella Guida per l'utente AWS Security Hub . È inoltre possibile monitorare lo stato di un'indagine in un esito. Per ulteriori informazioni, consulta [Operazioni sugli esiti](#) nella Guida per l'utente di AWS Security Hub .

Tutti i risultati in Security Hub CSPM utilizzano un formato JSON standard chiamato AWS Security Finding Format (ASFF). L'ASFF include dettagli sull'origine del problema, sulle risorse interessate e sullo stato corrente dell'esito. Per ulteriori informazioni, consulta [AWS Security Finding Format \(ASFF\)](#) nella Guida per l'utente di AWS Security Hub .

Tipi di risultati che Patch Manager spedisce

Patch Manager invia i risultati a Security Hub CSPM utilizzando il [AWS Security Finding Format \(ASFF\)](#). In ASFF, il Types campo fornisce il tipo di esito. Gli esiti ottenuti da Patch Manager possono avere i seguenti valori per Types:

- Gestione del software e della configurazione Checks/Patch

Patch Manager invia un esito per nodo gestito non conforme. Il risultato viene riportato con il tipo di risorsa [AwsEc2Instance](#) in modo che i risultati possano essere correlati con altre integrazioni CSPM di Security Hub che segnalano i tipi di risorse. AwsEc2Instance Patch Manager inoltra un risultato a Security Hub CSPM solo se l'operazione ha rilevato che il nodo gestito non è conforme. L'esito include i risultati di riepilogo di patch.

 Note

Dopo aver segnalato un nodo non conforme a Security Hub CSPM, Patch Manager non invia un aggiornamento a Security Hub CSPM dopo che il nodo è stato reso conforme. È possibile risolvere manualmente i risultati in Security Hub CSPM dopo che le patch richieste sono state applicate al nodo gestito.

Per ulteriori informazioni sulla definizione di conformità, consulta [Valori dello stato di conformità delle patch](#). Per ulteriori informazioni PatchSummary, consulta l'API [PatchSummary](#) Reference. AWS Security Hub

Latenza per l'invio degli esiti

Quando Patch Manager crea un nuovo risultato, di solito viene inviato a Security Hub CSPM entro pochi secondi o 2 ore. La velocità dipende dal traffico nella Regione AWS in fase di elaborazione in quel momento.

Riprova quando CSPM Security Hub non è disponibile

In caso di interruzione del servizio, viene eseguita una AWS Lambda funzione per rimettere i messaggi nella coda principale dopo la riattivazione del servizio. Dopo che i messaggi sono nella coda principale, il tentativo è automatico.

Se Security Hub CSPM non è disponibile, Patch Manager riprova a inviare i risultati finché non vengono ricevuti.

Visualizzazione dei risultati in Security Hub CSPM

Questa procedura descrive come visualizzare i risultati in Security Hub CSPM sui nodi gestiti della flotta che non sono conformi alle patch.

Per esaminare i risultati del CSPM di Security Hub per verificare la conformità delle patch

1. Accedi Console di gestione AWS e apri la AWS Security Hub CSPM console all'indirizzo. <https://console.aws.amazon.com/securityhub/>
2. Nel riquadro di navigazione, seleziona Esiti.
3. Scegli la casella Aggiungi filtri



).

4. Nel menu, sotto Filtri, scegli Nome prodotto.
5. Nella finestra di dialogo che si apre, scegli è nel primo campo e poi inserisci **Systems Manager Patch Manager** nel secondo campo.
6. Scegli Applica.
7. Aggiungi eventuali filtri aggiuntivi che desideri per restringere i risultati.
8. Nell'elenco degli esiti, scegli il titolo di un esito su cui desideri maggiori informazioni.

Sul lato destro dello schermo si apre un riquadro con ulteriori dettagli sulla risorsa, sul problema rilevato e sulla soluzione consigliata.

 Important

Attualmente, Security Hub CSPM riporta il tipo di risorsa di tutti i nodi gestiti come. EC2 Instance Sono inclusi server e macchine virtuali (VM) on-premises registrati per l'utilizzo con Systems Manager.

Classificazioni di gravità

L'elenco degli esiti di **Systems Manager Patch Manager** include un report sulla gravità dell'esito. I livelli di gravità includono i seguenti, dal meno grave al più grave:

- INFORMATIVO: non è stato riscontrato alcun problema.
- BASSO: il problema non richiede alcuna correzione.
- MEDIO: il problema va risolto, ma non con urgenza.
- ALTO: il problema deve essere risolto in via prioritaria.
- CRITICO: il problema deve essere risolto immediatamente per evitare l'escalation.

La gravità è determinata dal pacchetto non conforme più grave presente su un'istanza. Poiché è possibile disporre di più baseline delle patch con più livelli di gravità, tra tutti i pacchetti non conformi viene segnalata la gravità più elevata. Ad esempio, supponiamo di avere due pacchetti non conformi in cui la gravità del pacchetto A è "Critica" e la gravità del pacchetto B è "Bassa". "Critica" verrà riportata come gravità.

Tieni presente che il campo di gravità è direttamente correlato al campo Compliance di Patch Manager. Si tratta di un campo che è possibile assegnare alle singole patch che corrispondono alla

regola. Poiché questo campo Compliance è assegnato a singole patch, non si riflette sul livello di riepilogo delle patch.

Contenuti correlati

- [Esiti](#) nella Guida per l'utente di AWS Security Hub
- [Multi-Account conformità delle patch Patch Manager e Security Hub](#) nel AWS Management & Governance Blog

Risultato tipico di Patch Manager

Patch Manager invia i risultati a Security Hub CSPM utilizzando il [AWS Security Finding Format \(ASFF\)](#).

Ecco un esempio di un esito tipico di Patch Manager.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:patchmanager:us-east-2:111122223333:instance/i-02573cafcfEXAMPLE/
document/AWS-RunPatchBaseline/run-command/d710f5bd-04e3-47b4-82f6-df4e0EXAMPLE",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/ssm-patch-manager",
  "GeneratorId": "d710f5bd-04e3-47b4-82f6-df4e0EXAMPLE",
  "AwsAccountId": "111122223333",
  "Types": [
    "Software & Configuration Checks/Patch Management/Compliance"
  ],
  "CreatedAt": "2021-11-11T22:05:25Z",
  "UpdatedAt": "2021-11-11T22:05:25Z",
  "Severity": {
    "Label": "INFORMATIONAL",
    "Normalized": 0
  },
  "Title": "Systems Manager Patch Summary - Managed Instance Non-Compliant",
  "Description": "This AWS control checks whether each instance that is managed by AWS
Systems Manager is in compliance with the rules of the patch baseline that applies to
that instance when a compliance Scan runs.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information about bringing instances into patch compliance, see
'Remediating out-of-compliance instances (Patch Manager)'.",
      "Url": "https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-
compliance-remediation.html"
```

```

    }
  },
  "SourceUrl": "https://us-east-2.console.aws.amazon.com/systems-manager/fleet-manager/i-02573cafcfEXAMPLE/patch?region=us-east-2",
  "ProductFields": {
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/ssm-patch-manager/arn:aws:patchmanager:us-east-2:111122223333:instance/i-02573cafcfEXAMPLE/document/AWS-RunPatchBaseline/run-command/d710f5bd-04e3-47b4-82f6-df4e0EXAMPLE",
    "aws/securityhub/ProductName": "Systems Manager Patch Manager",
    "aws/securityhub/CompanyName": "AWS"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "i-02573cafcfEXAMPLE",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "PatchSummary": {
    "Id": "pb-0c10e65780EXAMPLE",
    "InstalledCount": 45,
    "MissingCount": 2,
    "FailedCount": 0,
    "InstalledOtherCount": 396,
    "InstalledRejectedCount": 0,
    "InstalledPendingReboot": 0,
    "OperationStartTime": "2021-11-11T22:05:06Z",
    "OperationEndTime": "2021-11-11T22:05:25Z",
    "RebootOption": "NoReboot",
    "Operation": "SCAN"
  }
}

```

Attivazione e configurazione dell'integrazione

Per utilizzare l'integrazione Patch Manager con Security Hub CSPM, è necessario attivare Security Hub CSPM. Per informazioni su come attivare Security Hub CSPM, consulta [Configurazione di Security Hub CSPM nella Guida per l'utente](#). AWS Security Hub

La procedura seguente descrive come integrare Patch Manager Security Hub CSPM quando Security Hub CSPM è già attivo ma l'integrazione è disattivata. Patch Manager È necessario completare questa procedura solo se l'integrazione è stata disattivata manualmente.

Per aggiungere Patch Manager all'integrazione con Security Hub CSPM

1. Nel pannello di navigazione, scegli Patch Manager.
2. Seleziona la scheda Impostazioni.

oppure

Se è la prima volta che accedi a Patch Manager nella Regione AWS corrente, scegli Inizia da una panoramica e quindi scegli la scheda Impostazioni.

3. Nella sezione Esporta in Security Hub CSPM, a destra di I risultati della conformità delle patch non vengono esportati in Security Hub, scegli Abilita.

Come interrompere l'invio degli esiti

Per interrompere l'invio degli esiti a CSPM Security Hub, è possibile utilizzare la console CSPM Security Hub o l'API.

Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente AWS Security Hub :

- [Disabilitazione e abilitazione del flusso di esiti di un'integrazione \(console\)](#)
- [Disattivazione del flusso di risultati da un'integrazione \(API Security Hub CSPM,\) AWS CLI](#)

Lavorare con Patch Manager risorse che utilizzano AWS CLI

La sezione include esempi di comandi AWS Command Line Interface (AWS CLI) che è possibile utilizzare per eseguire attività di configurazione per Patch Manager.

Per un'illustrazione dell'utilizzo di patch AWS CLI per applicare patch a un ambiente server utilizzando una baseline di patch personalizzata, vedere. [Tutorial: applicare patch a un ambiente server utilizzando AWS CLI](#)

Per ulteriori informazioni sull'utilizzo delle AWS Systems Manager attività AWS CLI for, vedere la [AWS Systems Manager sezione del AWS CLI Command Reference](#).

AWS CLI comandi per le baseline delle patch

Comandi di esempio per le baseline delle patch

- [Creazione di una baseline delle patch](#)
- [Creazione di una baseline delle patch con repository personalizzati per varie versioni dei sistemi operativi](#)
- [Aggiornamento di una baseline delle patch](#)
- [Assegnazione di un nuovo nome a una baseline delle patch](#)
- [Eliminazione di una baseline delle patch](#)
- [Elenco di tutte le baseline delle patch](#)
- [Elenca tutto AWS-linee di base delle patch fornite](#)
- [Elenco di tutte le baseline delle patch personali](#)
- [Visualizzazione di una baseline delle patch](#)
- [Ottenimento della baseline delle patch predefinita](#)
- [Impostare una linea di baseline delle patch personalizzata come impostazione predefinita](#)
- [Reimposta un AWS baseline della patch come impostazione predefinita](#)
- [Tag di una baseline delle patch](#)
- [Elenca i tag di una baseline delle patch.](#)
- [Rimozione di un tag da una baseline delle patch](#)

Creazione di una baseline delle patch

Il seguente comando crea una baseline delle patch che approva tutti gli aggiornamenti correlati alla sicurezza critici o importanti per Windows Server 2012 R2 5 giorni dopo il rilascio. Sono state specificate anche le patch per gli elenchi approvati e rifiutati. Inoltre, la baseline delle patch è stata contrassegnata per indicare che è destinata a un ambiente di produzione.

Linux & macOS

```
aws ssm create-patch-baseline \  
  --name "Windows-Server-2012R2" \  
  --
```

```
--tags "Key=Environment,Value=Production" \
--description "Windows Server 2012 R2, Important and Critical security updates"
\
--approved-patches "KB2032276,MS10-048" \
--rejected-patches "KB2124261" \
--rejected-patches-action "ALLOW_AS_DEPENDENCY" \
--approval-rules
"PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=MSRC_SEVERITY,Values=[Important,Critical
{Key=CLASSIFICATION,Values=SecurityUpdates},
{Key=PRODUCT,Values=WindowsServer2012R2}]]},ApproveAfterDays=5}]"
```

Windows Server

```
aws ssm create-patch-baseline ^
--name "Windows-Server-2012R2" ^
--tags "Key=Environment,Value=Production" ^
--description "Windows Server 2012 R2, Important and Critical security updates"
^
--approved-patches "KB2032276,MS10-048" ^
--rejected-patches "KB2124261" ^
--rejected-patches-action "ALLOW_AS_DEPENDENCY" ^
--approval-rules
"PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=MSRC_SEVERITY,Values=[Important,Critical
{Key=CLASSIFICATION,Values=SecurityUpdates},
{Key=PRODUCT,Values=WindowsServer2012R2}]]},ApproveAfterDays=5}]"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "BaselineId":"pb-0c10e65780EXAMPLE"
}
```

Creazione di una baseline delle patch con repository personalizzati per varie versioni dei sistemi operativi

Applicabile solo per i nodi gestiti Linux. Il seguente comando mostra come specificare i repository delle patch da utilizzare per una determinata versione del sistema operativo Amazon Linux. In questo esempio viene utilizzato un repository di origine abilitato per impostazione predefinita in Amazon Linux 2017.09, ma potrebbe essere adattato per un altro repository di fonte configurato per un nodo gestito.

 Note

Per illustrare meglio questo comando più complesso, utilizziamo l'opzione `--cli-input-json` con opzioni aggiuntive archiviate in un file JSON esterno.

1. Creare un file JSON con un nome simile a `my-patch-repository.json` e aggiungervi il seguente contenuto.

```
{
  "Description": "My patch repository for Amazon Linux 2",
  "Name": "Amazon-Linux-2",
  "OperatingSystem": "AMAZON_LINUX_2",
  "ApprovalRules": {
    "PatchRules": [
      {
        "ApproveAfterDays": 7,
        "EnableNonSecurity": true,
        "PatchFilterGroup": {
          "PatchFilters": [
            {
              "Key": "SEVERITY",
              "Values": [
                "Important",
                "Critical"
              ]
            },
            {
              "Key": "CLASSIFICATION",
              "Values": [
                "Security",
                "Bugfix"
              ]
            },
            {
              "Key": "PRODUCT",
              "Values": [
                "AmazonLinux2"
              ]
            }
          ]
        }
      }
    ]
  }
}
```

```

    }
  ]
},
"Sources": [
  {
    "Name": "My-AL2",
    "Products": [
      "AmazonLinux2"
    ],
    "Configuration": "[amzn-main] \nname=amzn-main-Base
\nmirrorlist=http://repo.$awsregion.$awsdomain/$releasever/main/
mirror.list //nmirrorlist_expire=300//nmetadata_expire=300 \npriority=10
\nfailovermethod=priority \nfastestmirror_enabled=0 \ngpgcheck=1
\npgpkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-amazon-ga \nenabled=1 \nretries=3
\ntimeout=5\nreport_instanceid=yes"
  }
]
}

```

2. Nella directory in cui è stato salvato il file, eseguire il comando seguente:

```
aws ssm create-patch-baseline --cli-input-json file://my-patch-repository.json
```

Il sistema restituisce informazioni simili alle seguenti.

```

{
  "BaselineId": "pb-0c10e65780EXAMPLE"
}

```

Aggiornamento di una baseline delle patch

Il seguente comando aggiunge due patch come rifiutate e una come approvata a una baseline delle patch esistente.

Per informazioni sui formati accettati per gli elenchi delle patch approvate e di quelle rifiutate, consulta [Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate](#).

Linux & macOS

```
aws ssm update-patch-baseline \
  --baseline-id pb-0c10e65780EXAMPLE \
```

```
--rejected-patches "KB2032276" "MS10-048" \  
--approved-patches "KB2124261"
```

Windows Server

```
aws ssm update-patch-baseline ^  
  --baseline-id pb-0c10e65780EXAMPLE ^  
  --rejected-patches "KB2032276" "MS10-048" ^  
  --approved-patches "KB2124261"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "BaselineId": "pb-0c10e65780EXAMPLE",  
  "Name": "Windows-Server-2012R2",  
  "RejectedPatches": [  
    "KB2032276",  
    "MS10-048"  
  ],  
  "GlobalFilters": {  
    "PatchFilters": [  
  
    ]  
  },  
  "ApprovalRules": {  
    "PatchRules": [  
      {  
        "PatchFilterGroup": {  
          "PatchFilters": [  
            {  
              "Values": [  
                "Important",  
                "Critical"  
              ],  
              "Key": "MSRC_SEVERITY"  
            },  
            {  
              "Values": [  
                "SecurityUpdates"  
              ],  
              "Key": "CLASSIFICATION"  
            }  
          ]  
        }  
      }  
    ]  
  }  
}
```



```

        {
            "Values":[
                "WindowsServer2012R2"
            ],
            "Key":"PRODUCT"
        }
    ],
    "ApproveAfterDays":5
}
]
},
"ModifiedDate":1481001494.035,
"CreateDate":1480997823.81,
"ApprovedPatches":[
    "KB2124261"
],
"Description":"Windows Server 2012 R2, Important and Critical security updates"
}

```

Assegnazione di un nuovo nome a una baseline delle patch

Linux & macOS

```

aws ssm update-patch-baseline \
  --baseline-id pb-0c10e65780EXAMPLE \
  --name "Windows-Server-2012-R2-Important-and-Critical-Security-Updates"

```

Windows Server

```

aws ssm update-patch-baseline ^
  --baseline-id pb-0c10e65780EXAMPLE ^
  --name "Windows-Server-2012-R2-Important-and-Critical-Security-Updates"

```

Il sistema restituisce informazioni simili alle seguenti.

```

{
  "BaselineId":"pb-0c10e65780EXAMPLE",
  "Name":"Windows-Server-2012-R2-Important-and-Critical-Security-Updates",
  "RejectedPatches":[
    "KB2032276",
    "MS10-048"
  ]
}

```

```

],
"GlobalFilters":{
  "PatchFilters":[

  ]
},
"ApprovalRules":{
  "PatchRules":[
    {
      "PatchFilterGroup":{
        "PatchFilters":[
          {
            "Values":[
              "Important",
              "Critical"
            ],
            "Key":"MSRC_SEVERITY"
          },
          {
            "Values":[
              "SecurityUpdates"
            ],
            "Key":"CLASSIFICATION"
          },
          {
            "Values":[
              "WindowsServer2012R2"
            ],
            "Key":"PRODUCT"
          }
        ]
      },
      "ApproveAfterDays":5
    }
  ]
},
"ModifiedDate":1481001795.287,
"CreatedDate":1480997823.81,
"ApprovedPatches":[
  "KB2124261"
],
"Description":"Windows Server 2012 R2, Important and Critical security updates"
}

```

Eliminazione di una baseline delle patch

```
aws ssm delete-patch-baseline --baseline-id "pb-0c10e65780EXAMPLE"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "BaselineId": "pb-0c10e65780EXAMPLE"
}
```

Elenco di tutte le baseline delle patch

```
aws ssm describe-patch-baselines
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "BaselineIdentities": [
    {
      "BaselineName": "AWS-DefaultPatchBaseline",
      "DefaultBaseline": true,
      "BaselineDescription": "Default Patch Baseline Provided by AWS.",
      "BaselineId": "arn:aws:ssm:us-east-2:111122223333:patchbaseline/pb-0c10e65780EXAMPLE"
    },
    {
      "BaselineName": "Windows-Server-2012R2",
      "DefaultBaseline": false,
      "BaselineDescription": "Windows Server 2012 R2, Important and Critical security updates",
      "BaselineId": "pb-0c10e65780EXAMPLE"
    }
  ]
}
```

Di seguito è mostrato un altro comando che elenca tutte le baseline delle patch in una Regione AWS.

Linux & macOS

```
aws ssm describe-patch-baselines \
  --region us-east-2 \
```

```
--filters "Key=OWNER,Values=[All]"
```

Windows Server

```
aws ssm describe-patch-baselines ^  
--region us-east-2 ^  
--filters "Key=OWNER,Values=[All]"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "BaselineIdentities":[  
    {  
      "BaselineName":"AWS-DefaultPatchBaseline",  
      "DefaultBaseline":true,  
      "BaselineDescription":"Default Patch Baseline Provided by AWS.",  
      "BaselineId":"arn:aws:ssm:us-east-2:111122223333:patchbaseline/  
pb-0c10e65780EXAMPLE"  
    },  
    {  
      "BaselineName":"Windows-Server-2012R2",  
      "DefaultBaseline":false,  
      "BaselineDescription":"Windows Server 2012 R2, Important and Critical security  
updates",  
      "BaselineId":"pb-0c10e65780EXAMPLE"  
    }  
  ]  
}
```

Elenca tutto AWS-linee di base delle patch fornite

Linux & macOS

```
aws ssm describe-patch-baselines \  
--region us-east-2 \  
--filters "Key=OWNER,Values=[AWS]"
```

Windows Server

```
aws ssm describe-patch-baselines ^  
--region us-east-2 ^
```

```
--filters "Key=OWNER,Values=[AWS]"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "BaselineIdentities":[
    {
      "BaselineName":"AWS-DefaultPatchBaseline",
      "DefaultBaseline":true,
      "BaselineDescription":"Default Patch Baseline Provided by AWS.",
      "BaselineId":"arn:aws:ssm:us-east-2:111122223333:patchbaseline/
pb-0c10e65780EXAMPLE"
    }
  ]
}
```

Elenco di tutte le baseline delle patch personali

Linux & macOS

```
aws ssm describe-patch-baselines \
  --region us-east-2 \
  --filters "Key=OWNER,Values=[Self]"
```

Windows Server

```
aws ssm describe-patch-baselines ^
  --region us-east-2 ^
  --filters "Key=OWNER,Values=[Self]"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "BaselineIdentities":[
    {
      "BaselineName":"Windows-Server-2012R2",
      "DefaultBaseline":false,
      "BaselineDescription":"Windows Server 2012 R2, Important and Critical security
updates",
      "BaselineId":"pb-0c10e65780EXAMPLE"
    }
  ]
}
```

```
}  
]  
}
```

Visualizzazione di una baseline delle patch

```
aws ssm get-patch-baseline --baseline-id pb-0c10e65780EXAMPLE
```

Note

Per le baseline delle patch personalizzate, è possibile specificare l'ID della baseline delle patch o l'Amazon Resource Name (ARN) completo. Per una baseline AWS di patch fornita, è necessario specificare l'ARN completo. Ad esempio, `arn:aws:ssm:us-east-2:075727635805:patchbaseline/pb-0c10e65780EXAMPLE`.

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "BaselineId": "pb-0c10e65780EXAMPLE",  
  "Name": "Windows-Server-2012R2",  
  "PatchGroups": [  
    "Web Servers"  
  ],  
  "RejectedPatches": [  
  
  ],  
  "GlobalFilters": {  
    "PatchFilters": [  
  
    ]  
  },  
  "ApprovalRules": {  
    "PatchRules": [  
      {  
        "PatchFilterGroup": {  
          "PatchFilters": [  
            {  
              "Values": [  
                "Important",  
                "Critical"  
              ]  
            }  
          ]  
        }  
      ]  
    }  
  }  
}
```

```

        ],
        "Key": "MSRC_SEVERITY"
      },
      {
        "Values": [
          "SecurityUpdates"
        ],
        "Key": "CLASSIFICATION"
      },
      {
        "Values": [
          "WindowsServer2012R2"
        ],
        "Key": "PRODUCT"
      }
    ]
  },
  "ApproveAfterDays": 5
}
]
},
"ModifiedDate": 1480997823.81,
"CreatedDate": 1480997823.81,
"ApprovedPatches": [

],
"Description": "Windows Server 2012 R2, Important and Critical security updates"
}

```

Ottenimento della baseline delle patch predefinita

```
aws ssm get-default-patch-baseline --region us-east-2
```

Il sistema restituisce informazioni simili alle seguenti.

```

{
  "BaselineId": "arn:aws:ssm:us-east-2:111122223333:patchbaseline/pb-0c10e65780EXAMPLE"
}

```

Impostare una linea di baseline delle patch personalizzata come impostazione predefinita

Linux & macOS

```
aws ssm register-default-patch-baseline \  
  --region us-east-2 \  
  --baseline-id "pb-0c10e65780EXAMPLE"
```

Windows Server

```
aws ssm register-default-patch-baseline ^  
  --region us-east-2 ^  
  --baseline-id "pb-0c10e65780EXAMPLE"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "BaselineId":"pb-0c10e65780EXAMPLE"  
}
```

Reimposta un AWS baseline della patch come impostazione predefinita

Linux & macOS

```
aws ssm register-default-patch-baseline \  
  --region us-east-2 \  
  --baseline-id "arn:aws:ssm:us-east-2:123456789012:patchbaseline/  
pb-0c10e65780EXAMPLE"
```

Windows Server

```
aws ssm register-default-patch-baseline ^  
  --region us-east-2 ^  
  --baseline-id "arn:aws:ssm:us-east-2:123456789012:patchbaseline/  
pb-0c10e65780EXAMPLE"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
```



```
"BaselineId":"pb-0c10e65780EXAMPLE"
}
```

Tag di una baseline delle patch

Linux & macOS

```
aws ssm add-tags-to-resource \
  --resource-type "PatchBaseline" \
  --resource-id "pb-0c10e65780EXAMPLE" \
  --tags "Key=Project,Value=Testing"
```

Windows Server

```
aws ssm add-tags-to-resource ^
  --resource-type "PatchBaseline" ^
  --resource-id "pb-0c10e65780EXAMPLE" ^
  --tags "Key=Project,Value=Testing"
```

Elenca i tag di una baseline delle patch.

Linux & macOS

```
aws ssm list-tags-for-resource \
  --resource-type "PatchBaseline" \
  --resource-id "pb-0c10e65780EXAMPLE"
```

Windows Server

```
aws ssm list-tags-for-resource ^
  --resource-type "PatchBaseline" ^
  --resource-id "pb-0c10e65780EXAMPLE"
```

Rimozione di un tag da una baseline delle patch

Linux & macOS

```
aws ssm remove-tags-from-resource \
  --resource-type "PatchBaseline" \
  --resource-id "pb-0c10e65780EXAMPLE" \
```

```
--tag-keys "Project"
```

Windows Server

```
aws ssm remove-tags-from-resource ^  
  --resource-type "PatchBaseline" ^  
  --resource-id "pb-0c10e65780EXAMPLE" ^  
  --tag-keys "Project"
```

AWS CLI comandi per i gruppi di patch

Comandi di esempio per gruppi di patch

- [Creazione di un gruppo di patch](#)
- [Registrazione del gruppo di patch "server web" con una baseline delle patch](#)
- [Registra un gruppo di patch «Backend» con AWS-linea di base della patch fornita](#)
- [Visualizzazione delle registrazioni dei gruppi di patch](#)
- [Annullamento della registrazione di un gruppo di patch da una baseline delle patch](#)

Creazione di un gruppo di patch

Note

I gruppi di patch non vengono utilizzati nelle operazioni di applicazione di patch basate su policy di patch. Per informazioni sull'utilizzo delle policy di patch, consulta [Configurazioni delle policy sulle patch in Configurazione rapida](#).

Per organizzare i tentativi di applicazione di patch, consigliamo di aggiungere nodi gestiti ai gruppi di patch utilizzando i tag. I gruppi di patch richiedono l'utilizzo della chiave di tag Patch Group o PatchGroup. Se sono presenti [tag consentiti nei metadati dell'istanza EC2](#), è necessario utilizzare PatchGroup (senza spazio). È possibile specificare un valore tag qualsiasi, ma la chiave di tag deve essere Patch Group o PatchGroup. Per ulteriori informazioni sui gruppi di patch, consulta [Gruppi di patch](#).

Dopo aver raggruppato i nodi gestiti utilizzando i tag, aggiungere il valore del gruppo di patch a una baseline delle patch. Registrando il gruppo di patch con una baseline di patch, ci si assicura che le patch corrette siano installate durante l'operazione di patching.

Attività 1: aggiunta di istanze EC2 a un gruppo di patch mediante tag

Note

Quando si utilizza la console Amazon Elastic Compute Cloud (Amazon EC2) AWS CLI, è possibile applicare `Key = Patch Group` o contrassegnare istanze non ancora `Key = PatchGroup` configurate per l'uso con Systems Manager. Se un'istanza EC2 che ti aspetti di vedere in Patch Manager non è elencata dopo aver applicato il tag `Patch Group` o `Key = PatchGroup`, consultare [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti per la risoluzione dei problemi.

Eseguire il seguente comando per aggiungere il tag `PatchGroup` a un'istanza EC2.

```
aws ec2 create-tags --resources "i-1234567890abcdef0" --tags
"Key=PatchGroup,Value=GroupValue"
```

Attività 2: aggiunta di nodi gestiti a un gruppo di patch mediante i tag

Eseguire il comando seguente per aggiungere il tag `PatchGroup` a un nodo gestito.

Linux & macOS

```
aws ssm add-tags-to-resource \
  --resource-type "ManagedInstance" \
  --resource-id "mi-0123456789abcdefg" \
  --tags "Key=PatchGroup,Value=GroupValue"
```

Windows Server

```
aws ssm add-tags-to-resource ^
  --resource-type "ManagedInstance" ^
  --resource-id "mi-0123456789abcdefg" ^
  --tags "Key=PatchGroup,Value=GroupValue"
```

Attività 3: aggiunta di un gruppo di patch a una baseline delle patch

Eseguire il comando seguente per associare il valore di tag `PatchGroup` alla baseline delle patch specificata.

Linux & macOS

```
aws ssm register-patch-baseline-for-patch-group \  
  --baseline-id "pb-0c10e65780EXAMPLE" \  
  --patch-group "Development"
```

Windows Server

```
aws ssm register-patch-baseline-for-patch-group ^  
  --baseline-id "pb-0c10e65780EXAMPLE" ^  
  --patch-group "Development"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "PatchGroup": "Development",  
  "BaselineId": "pb-0c10e65780EXAMPLE"  
}
```

Registrazione del gruppo di patch "server web" con una baseline delle patch

Linux & macOS

```
aws ssm register-patch-baseline-for-patch-group \  
  --baseline-id "pb-0c10e65780EXAMPLE" \  
  --patch-group "Web Servers"
```

Windows Server

```
aws ssm register-patch-baseline-for-patch-group ^  
  --baseline-id "pb-0c10e65780EXAMPLE" ^  
  --patch-group "Web Servers"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "PatchGroup": "Web Servers",  
  "BaselineId": "pb-0c10e65780EXAMPLE"
```

```
}
```

Registra un gruppo di patch «Backend» con AWS-linea di base della patch fornita

Linux & macOS

```
aws ssm register-patch-baseline-for-patch-group \  
  --region us-east-2 \  
  --baseline-id "arn:aws:ssm:us-east-2:111122223333:patchbaseline/  
pb-0c10e65780EXAMPLE" \  
  --patch-group "Backend"
```

Windows Server

```
aws ssm register-patch-baseline-for-patch-group ^  
  --region us-east-2 ^  
  --baseline-id "arn:aws:ssm:us-east-2:111122223333:patchbaseline/  
pb-0c10e65780EXAMPLE" ^  
  --patch-group "Backend"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "PatchGroup": "Backend",  
  "BaselineId": "arn:aws:ssm:us-east-2:111122223333:patchbaseline/pb-0c10e65780EXAMPLE"  
}
```

Visualizzazione delle registrazioni dei gruppi di patch

```
aws ssm describe-patch-groups --region us-east-2
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "PatchGroupPatchBaselineMappings": [  
    {  
      "PatchGroup": "Backend",  
      "BaselineIdentity": {  
        "BaselineName": "AWS-DefaultPatchBaseline",  
        "DefaultBaseline": false,  
        "BaselineDescription": "Default Patch Baseline Provided by AWS.",  
      }  
    }  
  ]  
}
```

```

        "BaselineId": "arn:aws:ssm:us-east-2:111122223333:patchbaseline/
pb-0c10e65780EXAMPLE"
    },
    {
        "PatchGroup": "Web Servers",
        "BaselineIdentity": {
            "BaselineName": "Windows-Server-2012R2",
            "DefaultBaseline": true,
            "BaselineDescription": "Windows Server 2012 R2, Important and Critical
updates",
            "BaselineId": "pb-0c10e65780EXAMPLE"
        }
    }
]
}

```

Annullamento della registrazione di un gruppo di patch da una baseline delle patch

Linux & macOS

```

aws ssm deregister-patch-baseline-for-patch-group \
  --region us-east-2 \
  --patch-group "Production" \
  --baseline-id "arn:aws:ssm:us-east-2:111122223333:patchbaseline/
pb-0c10e65780EXAMPLE"

```

Windows Server

```

aws ssm deregister-patch-baseline-for-patch-group ^
  --region us-east-2 ^
  --patch-group "Production" ^
  --baseline-id "arn:aws:ssm:us-east-2:111122223333:patchbaseline/
pb-0c10e65780EXAMPLE"

```

Il sistema restituisce informazioni simili alle seguenti.

```

{
  "PatchGroup": "Production",
  "BaselineId": "arn:aws:ssm:us-east-2:111122223333:patchbaseline/pb-0c10e65780EXAMPLE"
}

```

AWS CLI comandi per visualizzare i riepiloghi e i dettagli delle patch

Comandi di esempio per la visualizzazione di riepiloghi e dettagli patch

- [Ottenimento di tutte le patch definite da una baseline delle patch](#)
- [Ottieni tutte le patch relative AmazonLinux2018.03 alle classificazioni SECURITY e Severity of Critical](#)
- [Scarica tutte le patch per Windows Server 2012 con un livello di gravità MSRC pari a Critical](#)
- [Ottenimento di tutte le patch disponibili](#)
- [Ottenimento dello stati di riepilogo delle patch per nodo gestito](#)
- [Ottenimento dei dettagli di conformità delle patch per un nodo gestito](#)
- [Visualizza i risultati della conformità all'applicazione delle patch \(AWS CLI\)](#)

Ottenimento di tutte le patch definite da una baseline delle patch

Note

Questo comando è supportato solo per le baseline delle patch Windows Server.

Linux & macOS

```
aws ssm describe-effective-patches-for-patch-baseline \  
  --region us-east-2 \  
  --baseline-id "pb-0c10e65780EXAMPLE"
```

Windows Server

```
aws ssm describe-effective-patches-for-patch-baseline ^  
  --region us-east-2 ^  
  --baseline-id "pb-0c10e65780EXAMPLE"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "NextToken": "--token string truncated--",  
  "EffectivePatches": [  
    {
```

```

    "PatchStatus":{
      "ApprovalDate":1384711200.0,
      "DeploymentStatus":"APPROVED"
    },
    "Patch":{
      "ContentUrl":"https://support.microsoft.com/en-us/kb/2876331",
      "ProductFamily":"Windows",
      "Product":"WindowsServer2012R2",
      "Vendor":"Microsoft",
      "Description":"A security issue has been identified in a Microsoft
software
      product that could affect your system. You can help protect your system
      by installing this update from Microsoft. For a complete listing of the
      issues that are included in this update, see the associated Microsoft
      Knowledge Base article. After you install this update, you may have to
      restart your system.",
      "Classification":"SecurityUpdates",
      "Title":"Security Update for Windows Server 2012 R2 Preview (KB2876331)",
      "ReleaseDate":1384279200.0,
      "MsrcClassification":"Critical",
      "Language":"All",
      "KbNumber":"KB2876331",
      "MsrcNumber":"MS13-089",
      "Id":"e74ccc76-85f0-4881-a738-59e9fc9a336d"
    }
  },
  {
    "PatchStatus":{
      "ApprovalDate":1428858000.0,
      "DeploymentStatus":"APPROVED"
    },
    "Patch":{
      "ContentUrl":"https://support.microsoft.com/en-us/kb/2919355",
      "ProductFamily":"Windows",
      "Product":"WindowsServer2012R2",
      "Vendor":"Microsoft",
      "Description":"Windows Server 2012 R2 Update is a cumulative
      set of security updates, critical updates and updates. You
      must install Windows Server 2012 R2 Update to make sure that
      your computer can continue to receive future Windows Updates,
      including security updates. For a complete listing of the
      issues that are included in this update, see the associated
      Microsoft Knowledge Base article for more information. After
      you install this item, you may have to restart your computer.",

```



```

        "Classification": "SecurityUpdates",
        "Title": "Windows Server 2012 R2 Update (KB2919355)",
        "ReleaseDate": 1428426000.0,
        "MsrcClassification": "Critical",
        "Language": "All",
        "KbNumber": "KB2919355",
        "MsrcNumber": "MS14-018",
        "Id": "8452bac0-bf53-4fbd-915d-499de08c338b"
    }
}
---output truncated---
```

Ottieni tutte le patch relative AmazonLinux2018.03 alle classificazioni **SECURITY** e Severity of Critical

Linux & macOS

```
aws ssm describe-available-patches \
  --region us-east-2 \
  --filters Key=PRODUCT,Values=AmazonLinux2018.03 Key=SEVERITY,Values=Critical
```

Windows Server

```
aws ssm describe-available-patches ^
  --region us-east-2 ^
  --filters Key=PRODUCT,Values=AmazonLinux2018.03 Key=SEVERITY,Values=Critical
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "Patches": [
    {
      "AdvisoryIds": ["ALAS-2011-1"],
      "BugzillaIds": [ "1234567" ],
      "Classification": "SECURITY",
      "CVEIds": [ "CVE-2011-3192"],
      "Name": "zziplib",
      "Epoch": "0",
      "Version": "2.71",
      "Release": "1.3.amzn1",
      "Arch": "i686",
```

```

        "Product": "AmazonLinux2018.03",
        "ReleaseDate": 1590519815,
        "Severity": "CRITICAL"
    }
]
}
---output truncated---
```

Scarica tutte le patch per Windows Server 2012 con un livello di gravità MSRC pari a Critical

Linux & macOS

```
aws ssm describe-available-patches \
  --region us-east-2 \
  --filters Key=PRODUCT,Values=WindowsServer2012 Key=MSRC_SEVERITY,Values=Critical
```

Windows Server

```
aws ssm describe-available-patches ^
  --region us-east-2 ^
  --filters Key=PRODUCT,Values=WindowsServer2012 Key=MSRC_SEVERITY,Values=Critical
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "Patches":[
    {
      "ContentUrl":"https://support.microsoft.com/en-us/kb/2727528",
      "ProductFamily":"Windows",
      "Product":"WindowsServer2012",
      "Vendor":"Microsoft",
      "Description":"A security issue has been identified that could
        allow an unauthenticated remote attacker to compromise your
        system and gain control over it. You can help protect your
        system by installing this update from Microsoft. After you
        install this update, you may have to restart your system.",
      "Classification":"SecurityUpdates",
      "Title":"Security Update for Windows Server 2012 (KB2727528)",
      "ReleaseDate":1352829600.0,
      "MsrcClassification":"Critical",
      "Language":"All",
      "KbNumber":"KB2727528",
```

```

    "MsrcNumber": "MS12-072",
    "Id": "1eb507be-2040-4eeb-803d-abc55700b715"
  },
  {
    "ContentUrl": "https://support.microsoft.com/en-us/kb/2729462",
    "ProductFamily": "Windows",
    "Product": "WindowsServer2012",
    "Vendor": "Microsoft",
    "Description": "A security issue has been identified that could
      allow an unauthenticated remote attacker to compromise your
      system and gain control over it. You can help protect your
      system by installing this update from Microsoft. After you
      install this update, you may have to restart your system.",
    "Classification": "SecurityUpdates",
    "Title": "Security Update for Microsoft .NET Framework 3.5 on
      Windows 8 and Windows Server 2012 for x64-based Systems (KB2729462)",
    "ReleaseDate": 1352829600.0,
    "MsrcClassification": "Critical",
    "Language": "All",
    "KbNumber": "KB2729462",
    "MsrcNumber": "MS12-074",
    "Id": "af873760-c97c-4088-ab7e-5219e120eab4"
  }
}

```

---output truncated---

Ottenimento di tutte le patch disponibili

```
aws ssm describe-available-patches --region us-east-2
```

Il sistema restituisce informazioni simili alle seguenti.

```

{
  "NextToken": "--token string truncated--",
  "Patches": [
    {
      "Classification": "SecurityUpdates",
      "ContentUrl": "https://support.microsoft.com/en-us/kb/4074588",
      "Description": "A security issue has been identified in a Microsoft
software
product that could affect your system. You can help protect your system by
installing this update from Microsoft. For a complete listing of the
issues

```

```

Base
system.",
    "Id": "11adea10-0701-430e-954f-9471595ae246",
    "KbNumber": "KB4074588",
    "Language": "All",
    "MsrcNumber": "",
    "MsrcSeverity": "Critical",
    "Product": "WindowsServer2016",
    "ProductFamily": "Windows",
    "ReleaseDate": 1518548400,
    "Title": "2018-02 Cumulative Update for Windows Server 2016 (1709) for x64-
based
Systems (KB4074588)",
    "Vendor": "Microsoft"
  },
  {
    "Classification": "SecurityUpdates",
    "ContentUrl": "https://support.microsoft.com/en-us/kb/4074590",
    "Description": "A security issue has been identified in a Microsoft
software
product that could affect your system. You can help protect your system by
installing this update from Microsoft. For a complete listing of the issues
that are included in this update, see the associated Microsoft Knowledge Base article.
After you install this update, you may have to restart your system.",
    "Id": "f5f58231-ac5d-4640-ab1b-9dc8d857c265",
    "KbNumber": "KB4074590",
    "Language": "All",
    "MsrcNumber": "",
    "MsrcSeverity": "Critical",
    "Product": "WindowsServer2016",
    "ProductFamily": "Windows",
    "ReleaseDate": 1518544805,
    "Title": "2018-02 Cumulative Update for Windows Server 2016 for x64-based
Systems (KB4074590)",
    "Vendor": "Microsoft"
  }
}
---output truncated---

```

Ottenimento dello stato di riepilogo delle patch per nodo gestito

Il riepilogo per nodo gestito fornisce il numero di patch nei seguenti stati per nodo: "NotApplicable", «Mancante», «Non riuscito», InstalledOther "e «Installato».

Linux & macOS

```
aws ssm describe-instance-patch-states \
  --instance-ids i-08ee91c0b17045407 i-09a618aec652973a9
```

Windows Server

```
aws ssm describe-instance-patch-states ^
  --instance-ids i-08ee91c0b17045407 i-09a618aec652973a9
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "InstancePatchStates": [
    {
      "InstanceId": "i-08ee91c0b17045407",
      "PatchGroup": "",
      "BaselineId": "pb-0c10e65780EXAMPLE",
      "SnapshotId": "6d03d6c5-f79d-41d0-8d0e-00a9aEXAMPLE",
      "InstalledCount": 50,
      "InstalledOtherCount": 353,
      "InstalledPendingRebootCount": 0,
      "InstalledRejectedCount": 0,
      "MissingCount": 0,
      "FailedCount": 0,
      "UnreportedNotApplicableCount": -1,
      "NotApplicableCount": 671,
      "OperationStartTime": "2020-01-24T12:37:56-08:00",
      "OperationEndTime": "2020-01-24T12:37:59-08:00",
      "Operation": "Scan",
      "RebootOption": "NoReboot"
    },
    {
      "InstanceId": "i-09a618aec652973a9",
      "PatchGroup": "",
      "BaselineId": "pb-0c10e65780EXAMPLE",
      "SnapshotId": "c7e0441b-1eae-411b-8aa7-973e6EXAMPLE",
```

```

    "InstalledCount": 36,
    "InstalledOtherCount": 396,
    "InstalledPendingRebootCount": 0,
    "InstalledRejectedCount": 0,
    "MissingCount": 3,
    "FailedCount": 0,
    "UnreportedNotApplicableCount": -1,
    "NotApplicableCount": 420,
    "OperationStartTime": "2020-01-24T12:37:34-08:00",
    "OperationEndTime": "2020-01-24T12:37:37-08:00",
    "Operation": "Scan",
    "RebootOption": "NoReboot"
  }
}
---output truncated---
```

Ottenimento dei dettagli di conformità delle patch per un nodo gestito

```
aws ssm describe-instance-patches --instance-id i-08ee91c0b17045407
```

Il sistema restituisce informazioni simili alle seguenti.

```

{
  "NextToken": "--token string truncated--",
  "Patches": [
    {
      "Title": "bind-libs.x86_64:32:9.8.2-0.68.rc1.60.amzn1",
      "KBId": "bind-libs.x86_64",
      "Classification": "Security",
      "Severity": "Important",
      "State": "Installed",
      "InstalledTime": "2019-08-26T11:05:24-07:00"
    },
    {
      "Title": "bind-utils.x86_64:32:9.8.2-0.68.rc1.60.amzn1",
      "KBId": "bind-utils.x86_64",
      "Classification": "Security",
      "Severity": "Important",
      "State": "Installed",
      "InstalledTime": "2019-08-26T11:05:32-07:00"
    },
    {
      "Title": "dhclient.x86_64:12:4.1.1-53.P1.28.amzn1",
      "KBId": "dhclient.x86_64",

```

```

    "Classification": "Security",
    "Severity": "Important",
    "State": "Installed",
    "InstalledTime": "2019-08-26T11:05:31-07:00"
  },
  ---output truncated---

```

Visualizza i risultati della conformità all'applicazione delle patch (AWS CLI)

Per visualizzare i risultati della conformità delle patch per un singolo nodo gestito

Esegui il seguente comando in AWS Command Line Interface (AWS CLI) per visualizzare i risultati di conformità delle patch per un singolo nodo gestito.

```
aws ssm describe-instance-patch-states --instance-id instance-id
```

Sostituiscilo *instance-id* con l'ID del nodo gestito per il quale desideri visualizzare i risultati, nel formato `i-02573cafcfEXAMPLE` o `mi-0282f7c436EXAMPLE`.

Questo sistema restituisce informazioni simili alle seguenti.

```

{
  "InstancePatchStates": [
    {
      "InstanceId": "i-02573cafcfEXAMPLE",
      "PatchGroup": "mypatchgroup",
      "BaselineId": "pb-0c10e65780EXAMPLE",
      "SnapshotId": "a3f5ff34-9bc4-4d2c-a665-4d1c1EXAMPLE",
      "CriticalNonCompliantCount": 2,
      "SecurityNonCompliantCount": 2,
      "OtherNonCompliantCount": 1,
      "InstalledCount": 123,
      "InstalledOtherCount": 334,
      "InstalledPendingRebootCount": 0,
      "InstalledRejectedCount": 0,
      "MissingCount": 1,
      "FailedCount": 2,
      "UnreportedNotApplicableCount": 11,
      "NotApplicableCount": 2063,
      "OperationStartTime": "2021-05-03T11:00:56-07:00",
      "OperationEndTime": "2021-05-03T11:01:09-07:00",
      "Operation": "Scan",
    }
  ]
}

```

```

        "LastNoRebootInstallOperationTime": "2020-06-14T12:17:41-07:00",
        "RebootOption": "RebootIfNeeded"
    }
]
}

```

Per visualizzare un riepilogo del conteggio delle patch per tutte le istanze EC2 in una Regione

`describe-instance-patch-states` supporta il recupero dei risultati di una sola istanza gestita alla volta. Tuttavia, l'utilizzo di uno script personalizzato con `describe-instance-patch-states`, è possibile generare un report più granulare.

Ad esempio, se lo [Strumento di filtro jq](#) è installato sul computer locale, è possibile eseguire il seguente comando per identificare quali delle istanze EC2 in un particolare Regione AWS hanno uno stato di `InstalledPendingReboot`.

```

aws ssm describe-instance-patch-states \
  --instance-ids $(aws ec2 describe-instances --region region | jq
  '.Reservations[].Instances[] | .InstanceId' | tr '\n|"' ' ') \
  --output text --query 'InstancePatchStates[*].{Instance:InstanceId,
  InstalledPendingRebootCount:InstalledPendingRebootCount}'

```

region rappresenta l'identificatore di una regione Regione AWS supportata da AWS Systems Manager, ad esempio `us-east-2` per la regione Stati Uniti orientali (Ohio). Per un elenco dei *region* valori supportati, vedere la colonna Regione negli endpoint [del servizio](#) Systems Manager in. Riferimenti generali di Amazon Web Services

Ad esempio:

```

aws ssm describe-instance-patch-states \
  --instance-ids $(aws ec2 describe-instances --region us-east-2 | jq
  '.Reservations[].Instances[] | .InstanceId' | tr '\n|"' ' ') \
  --output text --query 'InstancePatchStates[*].{Instance:InstanceId,
  InstalledPendingRebootCount:InstalledPendingRebootCount}'

```

Il sistema restituisce informazioni simili alle seguenti.

```

1      i-02573cafcfEXAMPLE
0      i-0471e04240EXAMPLE
3      i-07782c72faEXAMPLE
6      i-083b678d37EXAMPLE

```



```
0      i-03a530a2d4EXAMPLE
1      i-01f68df0d0EXAMPLE
0      i-0a39c0f214EXAMPLE
7      i-0903a5101eEXAMPLE
7      i-03823c2fedEXAMPLE
```

Inoltre `InstalledPendingRebootCount`, l'elenco dei tipi di conteggio che puoi cercare include quanto segue:

- `CriticalNonCompliantCount`
- `SecurityNonCompliantCount`
- `OtherNonCompliantCount`
- `UnreportedNotApplicableCount`
- `InstalledPendingRebootCount`
- `FailedCount`
- `NotApplicableCount`
- `InstalledRejectedCount`
- `InstalledOtherCount`
- `MissingCount`
- `InstalledCount`

AWS CLI comandi per la scansione e l'applicazione di patch ai nodi gestiti

Dopo aver eseguito i seguenti comandi per verificare la conformità delle patch o installare le patch, è possibile utilizzare i comandi nella sezione [AWS CLI comandi per visualizzare i riepiloghi e i dettagli delle patch](#) per visualizzare informazioni sullo stato della patch e sulla conformità.

Comandi di esempio

- [Scansiona i nodi gestiti per verificare la conformità delle patch \(AWS CLI\)](#)
- [Installa le patch sui nodi gestiti \(AWS CLI\)](#)

Scansiona i nodi gestiti per verificare la conformità delle patch (AWS CLI)

Per eseguire la scansione di nodi gestiti specifici per la conformità delle patch

Eseguire il seguente comando seguente.

Linux & macOS

```
aws ssm send-command \  
  --document-name 'AWS-RunPatchBaseline' \  
  --targets Key=InstanceIds,Values='i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE' \  
  --parameters 'Operation=Scan' \  
  --timeout-seconds 600
```

Windows Server

```
aws ssm send-command ^  
  --document-name "AWS-RunPatchBaseline" ^  
  --targets Key=InstanceIds,Values="i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE" ^  
  --parameters "Operation=Scan" ^  
  --timeout-seconds 600
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "Command": {  
    "CommandId": "a04ed06c-8545-40f4-87c2-a0babEXAMPLE",  
    "DocumentName": "AWS-RunPatchBaseline",  
    "DocumentVersion": "$DEFAULT",  
    "Comment": "",  
    "ExpiresAfter": 1621974475.267,  
    "Parameters": {  
      "Operation": [  
        "Scan"  
      ]  
    },  
    "InstanceIds": [],  
    "Targets": [  
      {  
        "Key": "InstanceIds",  
        "Values": [  
          "i-02573cafcfEXAMPLE",  
          "i-0471e04240EXAMPLE"  
        ]  
      }  
    ],  
    "RequestedDateTime": 1621952275.267,  
    "Status": "Pending",
```

```

        "StatusDetails": "Pending",
        "TimeoutSeconds": 600,

        ---output truncated---

    }
}

```

Per analizzare i nodi gestiti per verificare la conformità delle patch in base al tag del gruppo

Eseguire il seguente comando seguente.

Linux & macOS

```

aws ssm send-command \
  --document-name 'AWS-RunPatchBaseline' \
  --targets Key='tag:PatchGroup',Values='Web servers' \
  --parameters 'Operation=Scan' \
  --timeout-seconds 600

```

Windows Server

```

aws ssm send-command ^
  --document-name "AWS-RunPatchBaseline" ^
  --targets Key="tag:PatchGroup",Values="Web servers" ^
  --parameters "Operation=Scan" ^
  --timeout-seconds 600

```

Il sistema restituisce informazioni simili alle seguenti.

```

{
  "Command": {
    "CommandId": "87a448ee-8adc-44e0-b4d1-6b429EXAMPLE",
    "DocumentName": "AWS-RunPatchBaseline",
    "DocumentVersion": "$DEFAULT",
    "Comment": "",
    "ExpiresAfter": 1621974983.128,
    "Parameters": {
      "Operation": [
        "Scan"
      ]
    }
  }
}

```

```
    },
    "InstanceIds": [],
    "Targets": [
      {
        "Key": "tag:PatchGroup",
        "Values": [
          "Web servers"
        ]
      }
    ],
    "RequestedDateTime": 1621952783.128,
    "Status": "Pending",
    "StatusDetails": "Pending",
    "TimeoutSeconds": 600,

    ---output truncated---

  }
}
```

Installa le patch sui nodi gestiti (AWS CLI)

Per installare patch su nodi gestiti specifici

Eseguire il seguente comando seguente.

Note

I nodi gestiti di destinazione si riavviano in base alle necessità per completare l'installazione della patch. Per ulteriori informazioni, consulta [Documento di comando SSM per l'applicazione di patch: AWS-RunPatchBaseline](#).

Linux & macOS

```
aws ssm send-command \
  --document-name 'AWS-RunPatchBaseline' \
  --targets Key=InstanceIds,Values='i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE' \
  --parameters 'Operation=Install' \
  --timeout-seconds 600
```

Windows Server

```
aws ssm send-command ^  
  --document-name "AWS-RunPatchBaseline" ^  
  --targets Key=InstanceIds,Values="i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE" ^  
  --parameters "Operation=Install" ^  
  --timeout-seconds 600
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "Command": {  
    "CommandId": "5f403234-38c4-439f-a570-93623EXAMPLE",  
    "DocumentName": "AWS-RunPatchBaseline",  
    "DocumentVersion": "$DEFAULT",  
    "Comment": "",  
    "ExpiresAfter": 1621975301.791,  
    "Parameters": {  
      "Operation": [  
        "Install"  
      ]  
    },  
    "InstanceIds": [],  
    "Targets": [  
      {  
        "Key": "InstanceIds",  
        "Values": [  
          "i-02573cafcfEXAMPLE",  
          "i-0471e04240EXAMPLE"  
        ]  
      }  
    ],  
    "RequestedDateTime": 1621953101.791,  
    "Status": "Pending",  
    "StatusDetails": "Pending",  
    "TimeoutSeconds": 600,  
  
    ---output truncated---  
  }  
}
```

Per installare patch su nodi gestiti in un gruppo di patch specifico

Eseguire il seguente comando seguente.

Linux & macOS

```
aws ssm send-command \  
  --document-name 'AWS-RunPatchBaseline' \  
  --targets Key='tag:PatchGroup',Values='Web servers' \  
  --parameters 'Operation=Install' \  
  --timeout-seconds 600
```

Windows Server

```
aws ssm send-command ^  
  --document-name "AWS-RunPatchBaseline" ^  
  --targets Key="tag:PatchGroup",Values="Web servers" ^  
  --parameters "Operation=Install" ^  
  --timeout-seconds 600
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "Command": {  
    "CommandId": "fa44b086-7d36-4ad5-ac8d-627ecEXAMPLE",  
    "DocumentName": "AWS-RunPatchBaseline",  
    "DocumentVersion": "$DEFAULT",  
    "Comment": "",  
    "ExpiresAfter": 1621975407.865,  
    "Parameters": {  
      "Operation": [  
        "Install"  
      ]  
    },  
    "InstanceIds": [],  
    "Targets": [  
      {  
        "Key": "tag:PatchGroup",  
        "Values": [  
          "Web servers"  
        ]  
      }  
    ]  
  }  
}
```

```

    ],
    "RequestedDateTime": 1621953207.865,
    "Status": "Pending",
    "StatusDetails": "Pending",
    "TimeoutSeconds": 600,

    ---output truncated---

  }
}

```

AWS Systems Manager Patch Manager tutorial

I tutorial in questa sezione dimostrano come utilizzarlo Patch Manager, per diversi scenari di applicazione delle patch.

Tutorial: applicare patch a un server in un ambiente solo IPv6

Patch Manager supporta l'applicazione di patch ai nodi in ambienti che dispongono solo di IPv6. Aggiornando la SSM Agent configurazione, le operazioni di patching possono essere configurate per effettuare chiamate solo agli endpoint del servizio IPv6.

Per applicare patch a un server in un ambiente solo IPv6

1. Assicurati che la SSM Agent versione 3.3270.0 o successiva sia installata nel nodo gestito.
2. Nel nodo gestito, accedi al file di configurazione. SSM Agent Puoi trovare il `amazon-ssm-agent.json` file nelle seguenti directory:

- Linux: `/etc/amazon/ssm/`
- macOS: `/opt/aws/ssm/`
- Windows Server: `C:\Program Files\Amazon\SSM`

Se `amazon-ssm-agent.json` non esiste ancora, copia il contenuto della `amazon-ssm-agent.json.template` stessa cartella in `amazon-ssm-agent.json`.

3. Aggiorna la seguente voce per impostare la regione corretta e impostala `UseDualStackEndpoint` su `true`:

```

{
  -----

```

```
"Agent": {  
    "Region": "region",  
    "UseDualStackEndpoint": true  
},  
-----  
}
```

4. Riavvia il SSM Agent servizio utilizzando il comando appropriato per il tuo sistema operativo:

- Linux: `sudo systemctl restart amazon-ssm-agent`
- Ubuntu Server usando Snap: `sudo snap restart amazon-ssm-agent`
- macOS: `sudo launchctl stop com.amazon.aws.ssm` seguito da `sudo launchctl start com.amazon.aws.ssm`
- Windows Server: `Stop-Service AmazonSSMAgent` seguito da `Start-Service AmazonSSMAgent`

Per l'elenco completo dei comandi per sistema operativo, vedere [the section called “Verifica Agente SSM stato e avvio dell'agente”](#).

5. Eseguite qualsiasi operazione di patching per verificare che le operazioni di patching abbiano esito positivo nel vostro IPv6-only ambiente. Assicuratevi che i nodi a cui applicare le patch siano connessi alla fonte della patch. È possibile controllare l'Run Command output dell'esecuzione della patch per verificare la presenza di avvisi relativi a repository inaccessibili. Quando applichi una patch a un nodo in esecuzione in un ambiente solo IPv6, assicurati che il nodo sia connesso alla fonte della patch. È possibile controllare l'Run Command output dell'esecuzione delle patch per verificare la presenza di avvisi relativi a repository inaccessibili. Per i sistemi DNF-based operativi, è possibile configurare i repository non disponibili da ignorare durante l'applicazione delle patch se l'opzione è impostata su `under. skip_if_unavailable True /etc/dnf/dnf.conf`. DNF-based i sistemi operativi includono Amazon Linux 2023, Red Hat Enterprise Linux 8 e versioni successive, Oracle Linux 8 e versioni successive, Rocky Linux AlmaLinux, e CentOS 8 e versioni successive. Su Amazon Linux 2023, l'`skip_if_unavailable` opzione è impostata su per impostazione `True` predefinita.

Note

Quando utilizzi le funzionalità Install Override List o Baseline Override, assicurati che l'URL fornito sia raggiungibile dal nodo. Se l'opzione di SSM Agent configurazione

`UseDualStackEndpoint` è impostata su `true`, quando viene fornito un URL S3 viene utilizzato un client S3 dualstack.

Tutorial: creare una baseline delle patch per l'installazione di Windows Service Pack tramite la console

Quando crei una baseline delle patch personalizzata, è possibile specificare che siano installati tutti, alcuni o solo un tipo di patch supportata.

Nelle linee di base delle patch per Windows, è possibile selezionare `ServicePacks` come unica opzione di classificazione per limitare gli aggiornamenti delle patch ai soli Service Pack. I Service Pack possono essere installati automaticamente da Patch Manager, a condizione che l'aggiornamento sia disponibile in Windows Update o Windows Server Update Services (WSUS).

È possibile configurare una baseline delle patch per controllare se sono installati i Service Pack per tutte le versioni di Windows o solo quelli per versioni specifiche, ad esempio Windows 7 o Windows Server 2016.

Completa la procedura seguente per creare una baseline delle patch personalizzata da utilizzare esclusivamente per l'installazione di tutti i Service Pack nei nodi gestiti di Windows.

Per creare una baseline delle patch per l'installazione di Windows Service Pack (console)

1. Aprire la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Patch Manager.
3. Scegli la scheda Baseline delle patch e quindi Crea baseline delle patch.
4. Nel campo Nome inserisci il nome della baseline delle patch, ad esempio `MyWindowsServicePackPatchBaseline`.
5. (Facoltativo) Per Descrizione, inserisci una descrizione per questa baseline delle patch.
6. Per Sistema operativo, seleziona Windows.
7. Se desideri iniziare a utilizzare subito questa baseline delle patch appena creata come impostazione predefinita per Windows, seleziona Rendi predefinita questa baseline delle patch per le istanze di Windows Server.

 Note

Questa opzione è disponibile solo se hai effettuato l'accesso per la prima volta a Patch Manager prima del rilascio delle [policy di patch](#) del 22 dicembre 2022.

Per informazioni sull'impostazione di una baseline delle patch esistente come predefinita, consulta [Impostare una baseline delle patch esistente come predefinita](#).

8. Nella sezione Regole di approvazione per i sistemi operativi, utilizza i campi per creare una o più regole di approvazione automatica.
- **Prodotto:** le versioni del sistema operativo alle quali si applica la regola di approvazione, ad esempio `WindowsServer2012`. È possibile scegliere una, più di una o tutte le versioni supportate di Windows. L'opzione predefinita è `All`.
 - **Classificazione:** scegli `ServicePacks`.
 - **Gravità:** il valore di gravità delle patch a cui si applica la regola. Per assicurarti che tutti i Service Pack siano inclusi nella regola, scegli `All`.
 - **Auto-approval:** il metodo per selezionare le patch per l'approvazione automatica.
 - Approva le patch dopo un determinato numero di giorni: il numero di giorni in cui Patch Manager Patch Manager deve attendere dopo il rilascio o l'aggiornamento di una patch prima che una patch venga approvata automaticamente. È possibile inserire qualsiasi numero intero da zero (0) a 360. Per la maggior parte degli scenari, consigliamo di attendere non più di 100 giorni.
 - Approva le patch rilasciate fino a una data specifica: la data di rilascio delle patch per la quale Patch Manager applica automaticamente tutte le patch rilasciate o aggiornate prima di tale data (inclusa). Ad esempio, se si specifica il 7 luglio 2023, nessuna patch rilasciata o aggiornata a partire dall'8 luglio 2023 verrà installata automaticamente.
 - (Facoltativo) **Report di conformità:** il livello di gravità da assegnare ai Service Pack approvati dalla baseline, ad esempio `High`.

 Note

Se si specifica un livello di report di conformità e lo stato delle patch di un Service Pack approvato viene riportato come `Missing`, la gravità di conformità complessiva riportata dalla baseline delle patch corrisponde al livello di gravità specificato.

9. (Facoltativo) Per la gestione dei tag, applica una o più name/value coppie di tag key alla baseline della patch.

I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Per questa baseline delle patch dedicata all'aggiornamento dei Service Pack, è possibile specificare coppie chiave-valore come le seguenti:

- Key=OS, Value=Windows
- Key=Classification, Value=ServicePacks

10. Scegli Crea una baseline delle patch.

Tutorial: aggiorna le dipendenze dell'applicazione, applica patch a un nodo gestito ed esegui un controllo dell'integrità specifico dell'applicazione tramite la console

In molti casi, un nodo gestito deve essere riavviato dopo che è stata applicata la patch con l'aggiornamento software più recente. Tuttavia, il riavvio di nodo in produzione senza misure di protezione può causare diversi problemi, ad esempio richiamare allarmi, registrare dati metrici errati e interrompere le sincronizzazioni dei dati.

Questo tutorial illustra come evitare problemi come questi utilizzando il documento (documento SSM) AWS Systems Manager `AWS-RunPatchBaselineWithHooks` per ottenere una complessa operazione di applicazione di patch in più fasi che consente di eseguire le operazioni seguenti:

1. Impedire nuove connessioni all'applicazione
2. Installare gli aggiornamenti nel sistema operativo
3. Aggiornare le dipendenze del pacchetto dell'applicazione
4. Riavviare il sistema
5. Esegui un controllo dell'integrità specifico dell'applicazione

Per questo esempio, abbiamo impostato la nostra infrastruttura in questo modo:

- Le macchine virtuali di destinazione vengono registrate come nodi gestiti con Systems Manager.
- `Iptables` viene utilizzato come firewall locale.
- L'applicazione ospitata sui nodi gestiti è in esecuzione sulla porta 443.
- L'applicazione ospitata sui nodi gestiti è un'applicazione di `nodeJS`.

- L'applicazione ospitata sui nodi gestiti è gestita dal gestore di processi pm2.
- L'applicazione dispone già di un endpoint di controllo dell'integrità specificato.
- L'endpoint di controllo dell'integrità dell'applicazione non richiede l'autenticazione dell'utente finale. L'endpoint consente un controllo dell'integrità che soddisfi i requisiti dell'organizzazione per stabilire la disponibilità. Nei tuoi ambienti, potrebbe essere sufficiente accertare semplicemente che l'applicazione nodeJS sia in esecuzione e in grado di ascoltare le richieste. In altri casi, è possibile verificare anche che sia già stata stabilita una connessione al livello di memorizzazione nella cache o al livello di database.

Gli esempi riportati in questo tutorial sono esclusivamente a scopo dimostrativo e non devono essere implementati così come sono negli ambienti di produzione. Inoltre, tieni presente che la funzionalità lifecycle hook di Patch Manager, with the document può supportare numerosi altri scenari. AWS-RunPatchBaselineWithHooks Di seguito sono riportati vari esempi.

- Arresta un agente di reporting dei parametri di riferimento prima di applicare patch e riavviarlo dopo il riavvio dei nodi gestiti.
- Staccare il nodo gestito da un cluster CRM o PCS prima di applicare patch e ricollegarsi dopo il riavvio del nodo.
- Aggiornare software di terze parti (ad esempio, Java, Tomcat, applicazioni Adobe e così via) su macchine Windows Server dopo l'applicazione degli aggiornamenti del sistema operativo (OS), ma prima del riavvio del nodo gestito.

Per aggiornare le dipendenze dell'applicazione, applicare patch a un nodo gestito ed eseguire un controllo dell'integrità specifico dell'applicazione

1. Creare un documento SSM per lo script di preinstallazione con i seguenti contenuti e denominarlo NodeJSAppPrePatch. Sostituisci *your_application* con il nome della tua applicazione.

Questo script blocca immediatamente le nuove richieste in arrivo e fornisce cinque secondi per le richieste già attive da completare prima di iniziare l'operazione di applicazione delle patch. Per l'opzione sleep, specificate alcuni secondi in più rispetto a quelli normalmente necessari per il completamento delle richieste in arrivo.

```
# exit on error
set -e
```

```
# set up rule to block incoming traffic
iptables -I INPUT -j DROP -p tcp --syn --destination-port 443 || exit 1
# wait for current connections to end. Set timeout appropriate to your
  application's latency
sleep 5
# Stop your application
pm2 stop your_application
```

Per informazioni sulla creazione di un documento SSM, consulta [Creazione del contenuto del documento SSM](#).

2. Crea un altro documento SSM con il seguente contenuto per lo script post-installazione per aggiornare le dipendenze dell'applicazione e denominarlo NodeJSAppPostPatch. Sostituiscila */your/application/path* con il percorso dell'applicazione.

```
cd /your/application/path
npm update
# you can use npm-check-updates if you want to upgrade major versions
```

3. Crea un altro documento SSM con il seguente contenuto per il tuo script onExit per eseguire il backup dell'applicazione ed eseguire un controllo dell'integrità. Denomina questo documento SSM NodeJSAppOnExitPatch. Sostituisci *your_application* con il nome della tua applicazione.

```
# exit on error
set -e
# restart nodejs application
pm2 start your_application
# sleep while your application starts and to allow for a crash
sleep 10
# check with pm2 to see if your application is running
pm2 pid your_application
# re-enable incoming connections
iptables -D INPUT -j DROP -p tcp --syn --destination-port
# perform health check
/usr/bin/curl -m 10 -vk -A "" http://localhost:443/health-check || exit 1
```

4. Crea un'associazione State Manager per eseguire l'operazione eseguendo i seguenti passaggi:
 1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.

2. Nel pannello di navigazione, scegliere State Manager, quindi Create association (Crea associazione).
3. Per Nome, fornire un nome per identificare lo scopo dell'associazione.
4. Nell'elenco Document (Documento) scegliere AWS-RunPatchBaselineWithHooks.
5. Per Operation (Operazione), selezionare Install (Installa).
6. (Facoltativo) Per Snapshot Id, fornisci un GUID generato per velocizzare l'operazione e garantire la coerenza. Il valore GUID può essere semplice come 00000000-0000-0000-0000-111122223333.
7. Per Nome documento Hook pre-installazione, immettere NodeJSAppPrePatch.
8. Per Post Install Hook Doc Name (Nome documento Hook post-installazione), immetti NodeJSAppPostPatch.
9. Per On ExitHook Doc Name, inserisci. NodeJSAppOnExitPatch
5. Per Targets, identificare i nodi gestiti specificando i tag, scegliendo i nodi manualmente, scegliendo un gruppo di risorse o scegliendo tutti i nodi gestiti.
6. Per Specificare la pianificazione, specificare la frequenza di esecuzione dell'associazione. Ad esempio, per l'applicazione di patch su nodi gestiti, una volta alla settimana è una cadenza comune.
7. Nella sezione Rate control (Controllo della velocità) scegli le opzioni per controllare l'esecuzione dell'associazione su più nodi gestiti. Assicurati che solo una parte dei nodi gestiti venga aggiornata alla volta. In caso contrario, tutto o la maggior parte del parco potrebbe essere disconnesso in una sola volta. Per informazioni sull'utilizzo dei controlli di velocità, consultare [Comprendere gli obiettivi e i controlli delle tariffe in State Manager associazioni](#).
8. (Facoltativo) In Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Abilita scrittura in S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

Note

Le autorizzazioni S3 che consentono di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza assegnate al nodo gestito e non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova in un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio

IAM associato all'istanza disponga delle autorizzazioni necessarie per scrivere su quel bucket.

9. Scegli Crea associazione.

Tutorial: applicare patch a un ambiente server utilizzando AWS CLI

La procedura seguente mostra in che modo un utente potrebbe applicare patch a un ambiente server utilizzando una baseline delle patch personalizzata, gruppi di patch e una finestra di manutenzione.

Prima di iniziare

- Installazione o aggiornamento dell'SSM Agent sui tuoi nodi gestiti. Per applicare patch ai nodi gestiti Linux, i nodi devono essere in esecuzione la versione 2.0.834.0 SSM Agent o successive. Per ulteriori informazioni, consulta [Aggiornamento di SSM Agent utilizzando Run Command](#).
- Configura ruoli e autorizzazioni per Maintenance Windows. Per ulteriori informazioni, consulta [Configurazione Intervallo di manutenzione](#).
- Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

Per configurare Patch Manager e nodi gestiti con patch (riga di comando)

1. Eseguire il comando seguente per creare una baseline delle patch per Windows denominata `Production-Baseline`. Questa baseline delle patch approva le patch per un ambiente di produzione 7 giorni dopo il rilascio o l'ultimo aggiornamento. In questo modo, la baseline delle patch è stata contrassegnata per indicare che è destinata a un ambiente di produzione.

Note

Il parametro `OperatingSystem` e `PatchFilters` variano a seconda del sistema operativo dei nodi gestiti di destinazione a cui si applica la baseline delle patch. Per ulteriori informazioni, consultare [OperatingSystem](#) e [PatchFilter](#).

Linux & macOS

```
aws ssm create-patch-baseline \
  --name "Production-Baseline" \
  --operating-system "WINDOWS" \
  --tags "Key=Environment,Value=Production" \
  --approval-rules
  "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=MSRC_SEVERITY,Values=[Critical,Importan
{Key=CLASSIFICATION,Values=[SecurityUpdates,Updates,ServicePacks,UpdateRollups,CriticalU
\
  --description "Baseline containing all updates approved for production
systems"
```

Windows Server

```
aws ssm create-patch-baseline ^
  --name "Production-Baseline" ^
  --operating-system "WINDOWS" ^
  --tags "Key=Environment,Value=Production" ^
  --approval-rules
  "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=MSRC_SEVERITY,Values=[Critical,Importan
{Key=CLASSIFICATION,Values=[SecurityUpdates,Updates,ServicePacks,UpdateRollups,CriticalU
^
  --description "Baseline containing all updates approved for production
systems"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "BaselineId":"pb-0c10e65780EXAMPLE"
}
```

2. Eseguite i seguenti comandi per registrare la baseline Production-Baseline "" per due gruppi di patch. I gruppi sono denominati «Database Servers» e "Front-End Servers».

Linux & macOS

```
aws ssm register-patch-baseline-for-patch-group \
  --baseline-id pb-0c10e65780EXAMPLE \
```



```
--patch-group "Database Servers"
```

Windows Server

```
aws ssm register-patch-baseline-for-patch-group ^  
  --baseline-id pb-0c10e65780EXAMPLE ^  
  --patch-group "Database Servers"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "PatchGroup":"Database Servers",  
  "BaselineId":"pb-0c10e65780EXAMPLE"  
}
```

Linux & macOS

```
aws ssm register-patch-baseline-for-patch-group \  
  --baseline-id pb-0c10e65780EXAMPLE \  
  --patch-group "Front-End Servers"
```

Windows Server

```
aws ssm register-patch-baseline-for-patch-group ^  
  --baseline-id pb-0c10e65780EXAMPLE ^  
  --patch-group "Front-End Servers"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "PatchGroup":"Front-End Servers",  
  "BaselineId":"pb-0c10e65780EXAMPLE"  
}
```

3. Eseguire i seguenti comandi per creare due finestre di manutenzione per il server di produzione. La prima finestra viene eseguita ogni martedì alle 22:00. La seconda finestra viene eseguita ogni sabato alle 22:00. Inoltre, la finestra di manutenzione è stata contrassegnata per indicare che è destinata a un ambiente di produzione.

Linux & macOS

```
aws ssm create-maintenance-window \  
  --name "Production-Tuesdays" \  
  --tags "Key=Environment,Value=Production" \  
  --schedule "cron(0 0 22 ? * TUE *)" \  
  --duration 1 \  
  --cutoff 0 \  
  --no-allow-unassociated-targets
```

Windows Server

```
aws ssm create-maintenance-window ^  
  --name "Production-Tuesdays" ^  
  --tags "Key=Environment,Value=Production" ^  
  --schedule "cron(0 0 22 ? * TUE *)" ^  
  --duration 1 ^  
  --cutoff 0 ^  
  --no-allow-unassociated-targets
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "WindowId": "mw-0c50858d01EXAMPLE"  
}
```

Linux & macOS

```
aws ssm create-maintenance-window \  
  --name "Production-Saturdays" \  
  --tags "Key=Environment,Value=Production" \  
  --schedule "cron(0 0 22 ? * SAT *)" \  
  --duration 2 \  
  --cutoff 0 \  
  --no-allow-unassociated-targets
```

Windows Server

```
aws ssm create-maintenance-window ^
```

```
--name "Production-Saturdays" ^  
--tags "Key=Environment,Value=Production" ^  
--schedule "cron(0 0 22 ? * SAT *)" ^  
--duration 2 ^  
--cutoff 0 ^  
--no-allow-unassociated-targets
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "WindowId": "mw-9a8b7c6d5eEXAMPLE"  
}
```

4. Eseguire i comandi seguenti per registrare i gruppi di patch server Database e Front-End con le rispettive finestre di manutenzione.

Linux & macOS

```
aws ssm register-target-with-maintenance-window \  
--window-id mw-0c50858d01EXAMPLE \  
--targets "Key=tag:PatchGroup,Values=Database Servers" \  
--owner-information "Database Servers" \  
--resource-type "INSTANCE"
```

Windows Server

```
aws ssm register-target-with-maintenance-window ^  
--window-id mw-0c50858d01EXAMPLE ^  
--targets "Key=tag:PatchGroup,Values=Database Servers" ^  
--owner-information "Database Servers" ^  
--resource-type "INSTANCE"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "WindowTargetId": "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"  
}
```

Linux & macOS

```
aws ssm register-target-with-maintenance-window \  
--window-id mw-9a8b7c6d5eEXAMPLE \  
--targets "Key=tag:PatchGroup,Values=Front-End Servers" \  
--owner-information "Front-End Servers" \  
--resource-type "INSTANCE"
```

Windows Server

```
aws ssm register-target-with-maintenance-window ^  
--window-id mw-9a8b7c6d5eEXAMPLE ^  
--targets "Key=tag:PatchGroup,Values=Front-End Servers" ^  
--owner-information "Front-End Servers" ^  
--resource-type "INSTANCE"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{  
  "WindowTargetId": "faa01c41-1d57-496c-ba77-ff9caEXAMPLE"  
}
```

5. Eseguire i comandi seguenti per registrare un'attività di patch che installa aggiornamenti mancanti nei server Database e Front-End durante le rispettive finestre di manutenzione.

Linux & macOS

```
aws ssm register-task-with-maintenance-window \  
--window-id mw-0c50858d01EXAMPLE \  
--targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"  
\  
--task-arn "AWS-RunPatchBaseline" \  
--service-role-arn "arn:aws:iam::123456789012:role/MW-Role" \  
--task-type "RUN_COMMAND" \  
--max-concurrency 2 \  
--max-errors 1 \  
--priority 1 \  
--task-invocation-parameters "RunCommand={Parameters={Operation=Install}}"
```

Windows Server

```
aws ssm register-task-with-maintenance-window ^
  --window-id mw-0c50858d01EXAMPLE ^
  --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
^
  --task-arn "AWS-RunPatchBaseline" ^
  --service-role-arn "arn:aws:iam::123456789012:role/MW-Role" ^
  --task-type "RUN_COMMAND" ^
  --max-concurrency 2 ^
  --max-errors 1 ^
  --priority 1 ^
  --task-invocation-parameters "RunCommand={Parameters={Operation=Install}}"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE"
}
```

Linux & macOS

```
aws ssm register-task-with-maintenance-window \
  --window-id mw-9a8b7c6d5eEXAMPLE \
  --targets "Key=WindowTargetIds,Values=faa01c41-1d57-496c-ba77-ff9caEXAMPLE"
\
  --task-arn "AWS-RunPatchBaseline" \
  --service-role-arn "arn:aws:iam::123456789012:role/MW-Role" \
  --task-type "RUN_COMMAND" \
  --max-concurrency 2 \
  --max-errors 1 \
  --priority 1 \
  --task-invocation-parameters "RunCommand={Parameters={Operation=Install}}"
```

Windows Server

```
aws ssm register-task-with-maintenance-window ^
  --window-id mw-9a8b7c6d5eEXAMPLE ^
  --targets "Key=WindowTargetIds,Values=faa01c41-1d57-496c-ba77-ff9caEXAMPLE"
^
```

```
--task-arn "AWS-RunPatchBaseline" ^
--service-role-arn "arn:aws:iam::123456789012:role/MW-Role" ^
--task-type "RUN_COMMAND" ^
--max-concurrency 2 ^
--max-errors 1 ^
--priority 1 ^
--task-invocation-parameters "RunCommand={Parameters={Operation=Install}}"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "WindowTaskId": "8a5c4629-31b0-4edd-8aea-33698EXAMPLE"
}
```

6. Eseguire il seguente comando per ottenere il riepilogo di conformità delle patch di alto livello per un gruppo di patch. Il riepilogo della conformità patch di alto livello include il numero di nodi gestiti con patch nei rispettivi stati di patch.

Note

Si prevede di visualizzare gli zeri per il numero di nodi gestiti nel riepilogo fino a quando l'attività di patch viene eseguita durante la prima finestra di manutenzione.

Linux & macOS

```
aws ssm describe-patch-group-state \
  --patch-group "Database Servers"
```

Windows Server

```
aws ssm describe-patch-group-state ^
  --patch-group "Database Servers"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
  "Instances": number,
```

```

    "InstancesWithFailedPatches": number,
    "InstancesWithInstalledOtherPatches": number,
    "InstancesWithInstalledPatches": number,
    "InstancesWithInstalledPendingRebootPatches": number,
    "InstancesWithInstalledRejectedPatches": number,
    "InstancesWithMissingPatches": number,
    "InstancesWithNotApplicablePatches": number,
    "InstancesWithUnreportedNotApplicablePatches": number
  }

```

7. Eseguire il seguente comando per ottenere il riepilogo dello stato di un nodo gestito per le patch di un gruppo. Il riepilogo per nodo gestito include diverse patch nei rispettivi stati delle patch per nodo gestito per un gruppo di patch.

Linux & macOS

```

aws ssm describe-instance-patch-states-for-patch-group \
  --patch-group "Database Servers"

```

Windows Server

```

aws ssm describe-instance-patch-states-for-patch-group ^
  --patch-group "Database Servers"

```

Il sistema restituisce informazioni simili alle seguenti.

```

{
  "InstancePatchStates": [
    {
      "BaselineId": "string",
      "FailedCount": number,
      "InstalledCount": number,
      "InstalledOtherCount": number,
      "InstalledPendingRebootCount": number,
      "InstalledRejectedCount": number,
      "InstallOverrideList": "string",
      "InstanceId": "string",
      "LastNoRebootInstallOperationTime": number,
      "MissingCount": number,
      "NotApplicableCount": number,
      "Operation": "string",

```

```

        "OperationEndTime": number,
        "OperationStartTime": number,
        "OwnerInformation": "string",
        "PatchGroup": "string",
        "RebootOption": "string",
        "SnapshotId": "string",
        "UnreportedNotApplicableCount": number
    }
]
}

```

Per esempi di altri AWS CLI comandi che è possibile utilizzare per le attività di Patch Manager configurazione, vedere. [Lavorare con Patch Manager risorse che utilizzano AWS CLI](#)

Risoluzione dei problemi Patch Manager

Utilizza le informazioni seguenti per risolvere i problemi relativi a Patch Manager, uno strumento di AWS Systems Manager.

Problema: errore "Invoke-PatchBaselineOperation : accesso negato» o errore «Impossibile scaricare il file da S3" per **baseline_overrides.json**

Problema: quando vengono eseguite le operazioni di applicazione di patch specificate dalla policy di patch, viene visualizzato un errore simile all'esempio seguente.

Example error on Windows Server

```

-----ERROR-----
Invoke-PatchBaselineOperation : Access Denied
At C:\ProgramData\Amazon\SSM\InstanceData\i-02573cafcfEXAMPLE\document\orchestr
ation\792dd5bd-2ad3-4f1e-931d-abEXAMPLE\PatchWindows\_script.ps1:219 char:13
+ $response = Invoke-PatchBaselineOperation -Operation Install -Snapsho ...
+ ~~~~~
+ CategoryInfo          : OperationStopped: (Amazon.Patch.Ba...UpdateOpera
tion:InstallWindowsUpdateOperation) [Invoke-PatchBaselineOperation], Amazo
nS3Exception
+ FullyQualifiedErrorId : PatchBaselineOperations,Amazon.Patch.Baseline.Op
erations.PowerShellCmdlets.InvokePatchBaselineOperation
failed to run commands: exit status 0xffffffff

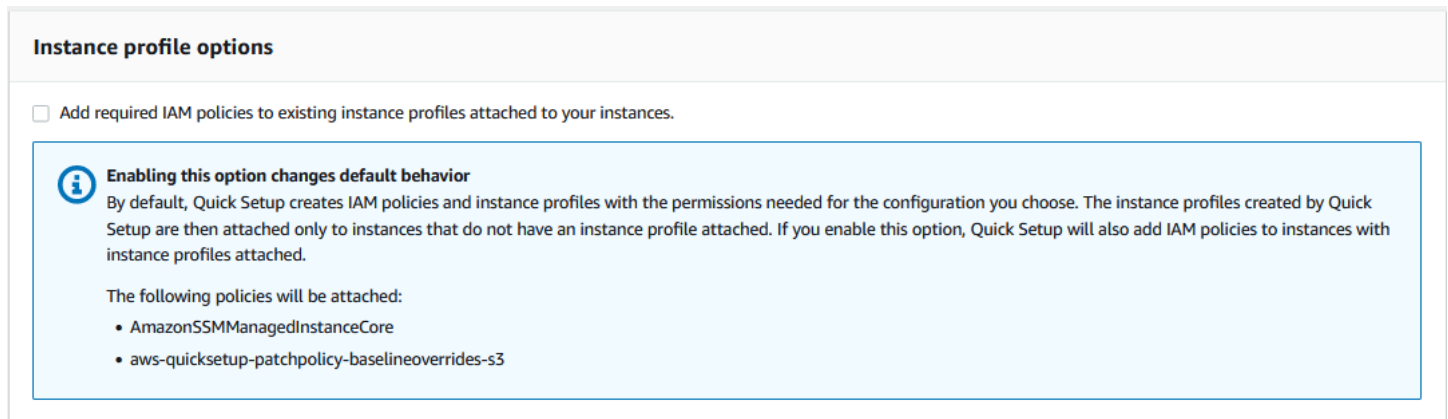
```


Example error on Linux

```
[INFO]: Downloading Baseline Override from s3://aws-quicksetup-  
patchpolicy-123456789012-abcde/baseline_overrides.json  
[ERROR]: Unable to download file from S3: s3://aws-quicksetup-  
patchpolicy-123456789012-abcde/baseline_overrides.json.  
[ERROR]: Error loading entrance module.
```

Causa: hai creato una policy di patch in Quick Setup e alcuni dei nodi gestiti presentavano già un profilo dell'istanza (per le istanze EC2) o un ruolo di servizio (per le macchine non EC2) collegato.

Tuttavia, come mostrato nell'immagine seguente, non hai selezionato la casella di controllo Aggiungi le policy IAM richieste ai profili di istanza esistenti collegati alle istanze.



Instance profile options

☐ Add required IAM policies to existing instance profiles attached to your instances.

Enabling this option changes default behavior
By default, Quick Setup creates IAM policies and instance profiles with the permissions needed for the configuration you choose. The instance profiles created by Quick Setup are then attached only to instances that do not have an instance profile attached. If you enable this option, Quick Setup will also add IAM policies to instances with instance profiles attached.

The following policies will be attached:

- AmazonSSMManagedInstanceCore
- aws-quicksetup-patchpolicy-baselineoverrides-s3

Quando crei una policy di patch, viene creato anche un bucket Amazon S3 per archiviare il file di configurazione della policy `baseline_overrides.json`. Se non selezioni la casella di controllo Aggiungi le policy IAM richieste ai profili di istanza esistenti collegati alle istanze al momento della creazione della policy, le policy IAM e i tag delle risorse necessari per accedere a `baseline_overrides.json` nel bucket S3 non vengono aggiunti automaticamente ai profili di istanza IAM e ai ruoli di servizio esistenti.

Soluzione 1: elimina la configurazione della policy di patch esistente, quindi crea una configurazione sostitutiva, assicurandoti di selezionare la casella di controllo Aggiungi le policy IAM richieste ai profili di istanza esistenti collegati alle istanze. Questa selezione applica le policy IAM create da questa configurazione di Quick Setup ai nodi a cui è già associato un profilo di istanza o un ruolo di servizio. (Per impostazione predefinita, Quick Setup aggiunge le policy richieste alle istanze e ai nodi che non dispongono già di profili di istanza o ruoli di servizio). Per ulteriori informazioni, consulta [Automatizzazione dell'applicazione di patch a livello di organizzazione utilizzando una policy di patch di Quick Setup](#).

Soluzione 2: aggiungi manualmente le autorizzazioni e i tag richiesti a ogni profilo di istanza IAM e ruolo di servizio IAM che utilizzi con Quick Setup. Per istruzioni, consulta l'argomento [Autorizzazioni per il bucket S3 con policy di patch](#).

Problema: l'applicazione di patch non riesce senza una causa apparente o un messaggio di errore

Problema: un'operazione di applicazione di patch non riesce senza restituire un messaggio di errore.

Possibile causa: quando si applicano le patch ai nodi gestiti, l'esecuzione del documento può essere interrotta e contrassegnata come non riuscita anche se le patch sono state installate correttamente. Ciò può verificarsi se il sistema avvia un riavvio imprevisto durante l'operazione di applicazione delle patch (ad esempio, per applicare aggiornamenti al firmware o a funzionalità simili). SecureBoot L'agente SSM non può persistere e riprendere lo stato di esecuzione del documento dopo i riavvii esterni, pertanto l'esecuzione viene segnalata come non riuscita. Ciò può verificarsi con i documenti `AWS-RunPatchBaseline`, `AWS-RunPatchBaselineAssociation`, `AWS-RunPatchBaselineWithHooks`, e `AWS-InstallWindowsUpdates`

Soluzione: per verificare lo stato di installazione della patch dopo un'esecuzione non riuscita, esegui un'operazione di Scan patching, quindi controlla i dati di conformità delle patch in Patch Manager per valutare lo stato di conformità corrente.

Se stabilisci che i riavvii esterni non sono stati la causa dell'errore in questo scenario, ti consigliamo di contattare. [Supporto AWS](#)

Problema: risultati imprevisti per la conformità delle patch

Problema: quando si esaminano i dettagli di conformità delle patch generati dopo un'operazione Scan, questi includono informazioni che non riflettono le regole configurate nella baseline delle patch. Ad esempio, un'eccezione aggiunta all'elenco `Rejected patches` (Patch rifiutate) in una baseline delle patch viene elencata come `Missing`. Oppure le patch classificate come `Important` sono elencate come mancanti anche se la baseline delle patch specifica solo le patch `Critical`.

Causa: Patch Manager attualmente supporta diversi metodi di esecuzione delle operazioni Scan:

- Una policy di patch configurata in Quick Setup
- Un'opzione di gestione host configurata in Quick Setup
- Una finestra di manutenzione per eseguire un'attività Scan o `Install` di patch
- Un'operazione `Applica subito una patch on demand`

L'esecuzione di un'operazione Scan, sovrascrive i dettagli di conformità della scansione più recente. Se hai impostato più metodi per eseguire un'operazione Scan e questi utilizzano baseline delle patch diverse con regole diverse, i esiti di conformità delle patch saranno diversi.

Soluzione: per evitare risultati imprevisti relativi alla conformità delle patch, ti consigliamo di utilizzare un solo metodo alla volta per eseguire l'operazione Scan di Patch Manager. Per ulteriori informazioni, consulta [Identificazione dell'esecuzione che ha creato i dati di conformità delle patch](#).

Errori durante l'esecuzione di **AWS-RunPatchBaseline** su Linux

Problema: errore "Nessun file o directory di questo tipo"

Problema: Quando si esegue AWS-RunPatchBaseline, l'applicazione di patch non riesce con uno dei seguenti errori.

```
IOError: [Errno 2] No such file or directory: 'patch-baseline-operations-X.XX.tar.gz'
```

```
Unable to extract tar file: /var/log/amazon/ssm/patch-baseline-operations/patch-baseline-operations-1.75.tar.gz.failed to run commands: exit status 155
```

```
Unable to load and extract the content of payload, abort.failed to run commands: exit status 152
```

Causa 1: due comandi per eseguire AWS-RunPatchBaseline erano in esecuzione nello stesso momento sullo stesso nodo gestito. Questo crea una condizione di competizione che fa sì che le file `patch-baseline-operations*` non sono state create o accessibili correttamente.

Causa 2: lo spazio di archiviazione insufficiente rimane sotto la directory `/var`.

Soluzione 1: assicurati che nessuna finestra di manutenzione contenga due o più Run Command attività eseguite AWS-RunPatchBaseline con lo stesso livello di priorità e che vengano eseguite sugli stessi ID di destinazione. In tal caso, riordina la priorità. Run Command è uno strumento in AWS Systems Manager.

Soluzione 2: assicuratevi che vengano eseguite solo una finestra di manutenzione alla volta per Run Command AWS-RunPatchBaseline attività che riguardano gli stessi obiettivi e la stessa pianificazione. In tal caso, modificare la pianificazione.

Soluzione 3: assicurati che solo un'associazione State Manager sia AWS-RunPatchBaseline in esecuzione con la stessa pianificazione e sia destinata agli stessi nodi gestiti. State Manager è uno strumento in AWS Systems Manager.

Soluzione 4: Liberare spazio di archiviazione sufficiente sotto la directory `/var` per i pacchetti di aggiornamento.

Problema: Errore “un altro processo ha acquisito il blocco yum”

Problema: Quando si esegue AWS-RunPatchBaseline, l'applicazione di patch ha esito negativo con il seguente errore.

```
12/20/2019 21:41:48 root [INFO]: another process has acquired yum lock, waiting 2 s and
retry.
```

Causa: Il documento AWS-RunPatchBaseline è stato avviato in esecuzione sul nodo gestito in cui è già in esecuzione in un'altra operazione e ha acquisito il processo di gestione di pacchetti yum.

Soluzione: assicurati che nessuna State Manager associazione, attività della finestra di manutenzione o altre configurazioni eseguite AWS-RunPatchBaseline in base a una pianificazione siano destinate allo stesso nodo gestito nello stesso momento.

Problema: errore “Autorizzazione negata/non riuscita a eseguire i comandi”

Problema: Quando si esegue AWS-RunPatchBaseline, l'applicazione di patch ha esito negativo con il seguente errore.

```
sh:
/var/lib/amazon/ssm/instanceid/document/orchestration/commandid/PatchLinux/_script.sh:
Permission denied
failed to run commands: exit status 126
```

Causa: `/var/lib/amazon/` potrebbe essere montato con autorizzazioni `noexec`. Questo è un problema, perché SSM Agent scarica gli script del payload in `/var/lib/amazon/ssm` e li esegue da quella posizione.

Soluzione: assicurati di aver configurato partizioni esclusive su `/var/log/amazon` e `/var/lib/amazon` che siano montate con le autorizzazioni. `exec`

Problema: errore “Impossibile scaricare il payload”

Problema: Quando si esegue AWS-RunPatchBaseline, l'applicazione di patch ha esito negativo con il seguente errore.

```
Unable to download payload: https://s3.amzn-s3-demo-bucket.region.amazonaws.com/
aws-ssm-region/patchbaselineoperations/linux/payloads/patch-baseline-operations-
X.XX.tar.gz.failed to run commands: exit status 156
```

Causa: il nodo gestito non dispone delle autorizzazioni necessarie per accedere al bucket Amazon Simple Storage Service (Amazon S3) specificato.

Soluzione: Aggiornare la configurazione di rete in modo che gli endpoint S3 siano raggiungibili. Per ulteriori informazioni, consulta le informazioni sugli accessi necessari ai bucket S3 per Patch Manager in [Agente SSM comunicazioni con AWS bucket S3 gestiti](#).

Problema: errore “gestore di pacchetti non supportato e combinazione di versione python”

Problema: Quando si esegue AWS-RunPatchBaseline, l'applicazione di patch ha esito negativo con il seguente errore.

```
An unsupported package manager and python version combination was found. Apt requires
Python3 to be installed.
failed to run commands: exit status 1
```

Causa: non è installata una versione supportata di python3 sull'istanza Debian Server oppure Ubuntu Server.

Soluzione: installa una versione supportata di Python3 (da 3.0 a 3.12) sul server, necessaria per i nodi gestiti Debian Server e Ubuntu Server.

Problema: Patch Manager non applica le regole specificate per escludere determinati pacchetti

Problema: Si è tentato di escludere determinati pacchetti specificandoli nel file `/etc/yum.conf`, nel formato `exclude=package-name`, ma non sono esclusi durante l'operazione Patch Manager Install.

Causa: Patch Manager non incorpora esclusioni specificate nel file `/etc/yum.conf`.

Soluzione: Per escludere pacchetti specifici, creare una baseline delle patch personalizzata e creare una norma per escludere i pacchetti che non si desidera installare.

Problema: l'applicazione delle patch non riesce e Patch Manager segnala che l'estensione Server Name Indication a TLS non è disponibile

Problema: L'operazione di applicazione di patch emette il seguente messaggio.

```
/var/log/amazon/ssm/patch-baseline-operations/urllib3/util/ssl_.py:369:
SNIMissingWarning: An HTTPS request has been made, but the SNI (Server Name Indication)
extension
to TLS is not available on this platform. This might cause the server to present an
incorrect TLS
certificate, which can cause validation failures. You can upgrade to a newer version of
Python
to solve this.
For more information, see https://urllib3.readthedocs.io/en/latest/advanced-
usage.html#ssl-warnings
```

Causa: questo messaggio non indica un errore. Invece, è un avvertimento che la versione precedente di Python distribuita con il sistema operativo non supporta l'indicazione del nome del server TLS. Lo script di payload della patch di Systems Manager emette questo avviso quando ci si connette alle AWS API che supportano SNI.

Soluzione: Per risolvere eventuali errori di applicazione di patch quando viene segnalato questo messaggio, esaminare il contenuto dei file `stdout` e `stderr`. Se non hai configurato la linea di base della patch per archiviare questi file in un bucket S3 o in Amazon CloudWatch Logs, puoi localizzare i file nella seguente posizione sul tuo nodo gestito Linux.

```
/var/lib/amazon/ssm/instance-id/document/orchestration/Run-Command-
execution-id/awsrunShellScript/PatchLinux
```

Problema: Patch Manager riporta «Niente più mirror da provare»

Problema: L'operazione di applicazione di patch emette il seguente messaggio.

```
[Errno 256] No more mirrors to try.
```

Causa: i repository configurati sul nodo gestito non funzionano correttamente. Tra le cause possibili sono incluse:

- La cache yum è danneggiata.
- Impossibile raggiungere un URL del repository a causa di problemi relativi alla rete.

Soluzione: Patch Manager utilizza il gestore di pacchetti predefinito del nodo gestito per eseguire l'operazione di patching. Double-check che i repository siano configurati e funzionino correttamente.

Problema: l'applicazione di patch non riesce con "Il codice di errore restituito da curl è 23"

Problema: un'operazione di applicazione di patch che utilizza AWS-RunPatchBaseline non riesce con un errore simile al seguente:

```
05/01/2025 17:04:30 root [ERROR]: Error code returned from curl is 23
```

Causa: lo strumento curl in uso sui sistemi non dispone delle autorizzazioni necessarie per scrivere sul filesystem. Ciò può verificarsi se lo strumento curl predefinito del gestore di pacchetti è stato sostituito da una versione diversa, ad esempio una versione installata con snap.

Soluzione: se la versione curl fornita dal gestore di pacchetti è stata disinstallata quando è stata installata una versione diversa, reinstallala.

Se devi mantenere installate più versioni di curl, assicurati che la versione associata al gestore di pacchetti sia nella prima directory elencata nella PATH variabile. È possibile verificarlo eseguendo il comando `echo $PATH` per vedere l'ordine corrente delle directory in cui viene controllata la presenza di file eseguibili sul sistema.

Problema: l'applicazione della patch non riesce e viene visualizzato il messaggio "Errore durante la decompressione del pacchetto rpm..."

Problema: un'operazione di applicazione di patch non riesce con un errore simile al seguente:

```
Error : Error unpacking rpm package python-urllib3-1.25.9-1.amzn2.0.2.noarch
python-urllib3-1.25.9-1.amzn2.0.1.noarch was supposed to be removed but is not!
failed to run commands: exit status 1
```

Causa 1: quando un particolare pacchetto è presente in più programmi di installazione di pacchetti, ad esempio pip e yum oppure dnf, possono verificarsi conflitti quando si utilizza il gestore di pacchetti predefinito.

Un esempio comune si verifica con il pacchetto `urllib3`, che si trova in pip, yum e dnf.

Causa 2: il pacchetto `python-urllib3` risulta danneggiato. Ciò può accadere se i file del pacchetto sono stati installati o aggiornati da pip dopo che il pacchetto rpm era stato precedentemente installato da yum o dnf.

Soluzione: rimuovi il pacchetto `python-urllib3` da pip eseguendo il comando `sudo pip uninstall urllib3`, mantenendo il pacchetto solo nel gestore di pacchetti predefinito (yum o dnf).

Problema: l'applicazione di patch non riesce con «riscontrare un errore sul lato del servizio durante il caricamento dell'inventario»

Problema: durante l'esecuzione del `AWS-RunPatchBaseline` documento, viene visualizzato il seguente messaggio di errore:

```
Encounter service side error when uploading the inventory
```

Causa: due comandi per eseguire `AWS-RunPatchBaseline` erano in esecuzione nello stesso momento sullo stesso nodo gestito. Ciò crea una condizione di gara durante l'inizializzazione del client boto3 durante le operazioni di patching.

Soluzione: assicuratevi che nessuna State Manager associazione, attività della finestra di manutenzione o altre configurazioni eseguite `AWS-RunPatchBaseline` in base a una pianificazione siano destinate allo stesso nodo gestito nello stesso momento.

Problema: l'applicazione di patch non riesce e viene visualizzato il messaggio "Sono stati rilevati errori durante il download dei pacchetti"

Problema: durante l'applicazione di patch, viene visualizzato un errore simile al seguente:

```
YumDownloadError: [u'Errors were encountered while downloading
packages.', u'libxml2-2.9.1-6.el7_9.6.x86_64: [Errno 5] [Errno 12]
Cannot allocate memory', u'libxslt-1.1.28-6.el7.x86_64: [Errno 5]
[Errno 12] Cannot allocate memory', u'libcroco-0.6.12-6.el7_9.x86_64:
[Errno 5] [Errno 12] Cannot allocate memory', u'openldap-2.4.44-25.el7_9.x86_64:
[Errno 5] [Errno 12] Cannot allocate memory',
```

Causa: questo errore può verificarsi quando la memoria disponibile su un nodo gestito è insufficiente.

Soluzione: configura la memoria di swap o aggiorna l'istanza a un tipo diverso per aumentare il supporto di memoria. Quindi inizia una nuova operazione di applicazione di patch.

Problema: l'applicazione delle patch non riesce con un errore di memoria esaurita (OOM)

Problema: durante l'esecuzione `AWS-RunPatchBaseline`, l'operazione di patching non riesce a causa della memoria insufficiente nel nodo gestito. Potresti visualizzare errori come `Cannot allocate memory`, `Killed` (dal killer OOM di Linux) o l'operazione non riesce in modo

imprevisto. Questo errore è più probabile che si verifichi su istanze con meno di 1 GB di RAM, ma può interessare anche le istanze con più memoria quando è disponibile un numero elevato di aggiornamenti.

Causa: Patch Manager esegue le operazioni di patching utilizzando il gestore di pacchetti nativo sul nodo gestito. La memoria richiesta durante un'operazione di patching dipende da diversi fattori, tra cui:

- Il numero di pacchetti installati e gli aggiornamenti disponibili sul nodo gestito.
- Il gestore di pacchetti in uso e le sue caratteristiche di memoria.
- Altri processi in esecuzione sul nodo gestito al momento dell'operazione di patching.

I nodi gestiti con un numero elevato di pacchetti installati o un numero elevato di aggiornamenti disponibili richiedono più memoria durante le operazioni di applicazione delle patch. Quando la memoria disponibile è insufficiente, il processo di patching fallirà e si concluderà con un errore. Il sistema operativo può inoltre interrompere il processo di applicazione delle patch.

Soluzione: provare una o più delle seguenti soluzioni:

- Pianifica le operazioni di applicazione delle patch durante i periodi di bassa attività del carico di lavoro sul nodo gestito, ad esempio utilizzando le finestre di manutenzione.
- Aggiorna l'istanza a un tipo con più memoria.
- Configura la memoria di swap sul nodo gestito. Tieni presente che nelle istanze con un throughput EBS limitato, un uso intensivo degli swap può causare un peggioramento delle prestazioni.
- Esamina e riduci il numero di processi in esecuzione sul nodo gestito durante le operazioni di patching.

Problema: l'applicazione di patch non riesce e viene visualizzato il messaggio "Impossibile verificare le seguenti firme perché la chiave pubblica non è disponibile"

Problema: un'operazione di applicazione di patch non riesce su Ubuntu Server con un errore simile al seguente:

```
02/17/2022 21:08:43 root [ERROR]: W:GPG error:
http://repo.mysql.com/apt/ubuntu bionic InRelease: The following
signatures couldn't be verified because the public key is not available:
NO_PUBKEY 467B942D3A79BD29, E:The repository ' http://repo.mysql.com/apt/ubuntu bionic
```

Causa: la chiave GNU Privacy Guard (GPG) è scaduta o risulta mancante.

Soluzione: aggiorna la chiave GPG o aggiungi di nuovo la chiave.

Ad esempio, utilizzando l'errore mostrato in precedenza, vediamo che la chiave 467B942D3A79BD29 risulta mancante e deve essere aggiunta. Per farlo, esegui uno dei comandi seguenti:

```
sudo apt-key adv --keyserver https://keyserver.ubuntu.com --recv-keys 467B942D3A79BD29
```

```
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 467B942D3A79BD29
```

Oppure, per aggiornare tutte le chiavi, esegui il seguente comando:

```
sudo apt-key adv --keyserver https://keyserver.ubuntu.com --refresh-keys
```

Se l'errore si ripresenta dopo questa operazione, consigliamo di segnalare il problema all'organizzazione che gestisce il repository. Fino a quando non sarà disponibile una correzione, è possibile modificare il file `/etc/apt/sources.list` in modo da omettere il repository durante il processo di applicazione di patch.

A tale scopo, apri il file `sources.list` per modificarlo, individua la riga del repository e inserisci un carattere `#` all'inizio della riga per commentarla. Salva e chiudi il file.

Problema: l'applicazione delle patch non riesce e viene visualizzato il messaggio «»
`NoMoreMirrorsRepoError`

Problema: viene visualizzato un errore simile al seguente:

```
NoMoreMirrorsRepoError: failure: repodata/repomd.xml from pgdg94: [Errno 256] No more mirrors to try.
```

Causa: si è verificato un errore nel repository di origine.

Soluzione: si consiglia di segnalare il problema all'organizzazione che gestisce il repository. Finché l'errore non viene corretto, è possibile disabilitare il repository a livello di sistema operativo. A tale scopo, esegui il comando seguente, sostituendo il valore per *repo-name* con il nome del tuo repository:

```
yum-config-manager --disable repo-name
```

Di seguito è riportato un esempio.

```
yum-config-manager --disable pgdg94
```

Dopo aver eseguito questo comando, esegui un'altra operazione di applicazione di patch.

Problema: l'applicazione di patch non riesce e viene visualizzato il messaggio "Impossibile scaricare il payload"

Problema: viene visualizzato un errore simile al seguente:

```
Unable to download payload:  
https://s3.dualstack.eu-west-1.amazonaws.com/aws-ssm-eu-west-1/patchbaselineoperations/  
linux/payloads/patch-baseline-operations-1.83.tar.gz.  
failed to run commands: exit status 156
```

Causa: la configurazione del nodo gestito contiene errori o è incompleta.

Soluzione: assicurati che il nodo gestito sia configurato con quanto segue:

- Regola TCP 443 in uscita nel gruppo di sicurezza.
- Regola TCP 443 in uscita in NACL.
- Regola TCP 1024-65535 in entrata in NACL.
- NAT/IGW nella tabella di routing per fornire connettività a un endpoint S3. Se l'istanza non dispone di accesso a Internet, forniscile la connettività con l'endpoint S3. A tale scopo, aggiungi un endpoint gateway S3 nel VPC e integralo con la tabella di routing del nodo gestito.

Problema: l'applicazione di patch non riesce e viene visualizzato il messaggio "Il frontend dpkg è bloccato da un altro processo"

Problema: un'operazione di applicazione di patch non riesce con un errore simile al seguente:

```
install errors: dpkg: error: dpkg frontend is locked by another process  
failed to run commands: exit status 2  
Failed to install package; install status Failed
```

Causa: il gestore di pacchetti sta già eseguendo un altro processo su un nodo gestito a livello di sistema operativo. Se il completamento dell'altro processo richiede molto tempo, l'operazione di applicazione di patch di Patch Manager può andare in timeout e non riuscire.

Soluzione: una volta completato l'altro processo che utilizza il gestore di pacchetti, esegui una nuova operazione di applicazione di patch.

Problema: applicazione delle patch Ubuntu Server fallisce con l'errore «dpkg è stato interrotto»

Problema: su Ubuntu Server, un'operazione di applicazione di patch non riesce con un errore simile al seguente:

```
E: dpkg was interrupted, you must manually run
'dpkg --configure -a' to correct the problem.
```

Causa: uno o più pacchetti non sono configurati correttamente.

Soluzione: Eseguire i seguenti passaggi:

1. Controlla quali pacchetti sono interessati e quali sono i problemi di ogni pacchetto eseguendo i seguenti comandi, uno alla volta:

```
sudo apt-get check
```

```
sudo dpkg -C
```

```
dpkg-query -W -f='${db:Status-Abbrev} ${binary:Package}\n' | grep -E ^.[^nci]
```

2. Correggi i pacchetti che presentano problemi eseguendo il seguente comando:

```
sudo dpkg --configure -a
```

3. Se il comando precedente non ha risolto completamente il problema, esegui il seguente comando:

```
sudo apt --fix-broken install
```

Problema: il gestore di pacchetti non è in grado di risolvere una dipendenza dal pacchetto

Problema: il gestore di pacchetti nativo sul nodo gestito non è in grado di risolvere una dipendenza dal pacchetto e l'applicazione di patch non riesce. Il seguente esempio di messaggio di errore indica questo tipo di errore su un sistema operativo che utilizza yum come gestore di pacchetti.

```
09/22/2020 08:56:09 root [ERROR]: yum update failed with result code: 1,  
message: [u'rpm-python-4.11.3-25.amzn2.0.3.x86_64 requires rpm = 4.11.3-25.amzn2.0.3',  
u'awscli-1.18.107-1.amzn2.0.1.noarch requires python2-botocore = 1.17.31']
```

Causa: nei sistemi operativi Linux, Patch Manager utilizza il gestore di pacchetti nativo sul computer per eseguire operazioni di applicazione di patch, ad esempio, yum, dnf, apt e zypper. Le applicazioni rilevano, installano, aggiornano o rimuovono automaticamente i pacchetti dipendenti in base alle esigenze. Tuttavia, alcune condizioni possono impedire al gestore di pacchetti di completare un'operazione di dipendenza, ad esempio:

- Sul sistema operativo sono configurati più repository in conflitto.
- L'URL di un repository remoto è inaccessibile a causa di problemi relativi alla rete.
- Nel repository è stato trovato un pacchetto per l'architettura sbagliata.

Soluzione: l'applicazione di patch potrebbe non riuscire a causa di un problema di dipendenza per un'ampia gamma di motivi. Pertanto, ti consigliamo di contattarci per ricevere assistenza nella risoluzione dei problemi. Supporto AWS

Problema: errori di blocco delle dipendenze dei pacchetti Zypper su SLES nodi gestiti

Problema: quando si esegue AWS-RunPatchBaseline l'Installazione su SUSE Linux Enterprise Server istanze, l'applicazione delle patch fallisce con errori di controllo delle dipendenze relativi ai blocchi dei pacchetti. Potrebbe essere visualizzato un messaggio di errore simile al seguente.

```
Problem: mock-pkg-has-dependencies-0.2.0-21.adistro.noarch requires mock-pkg-standalone  
= 0.2.0, but this requirement cannot be provided  
uninstallable providers: mock-pkg-standalone-0.2.0-21.adistro.noarch[local-repo]  
Solution 1: remove lock to allow installation of mock-pkg-  
standalone-0.2.0-21.adistro.noarch[local-repo]  
Solution 2: do not install mock-pkg-has-dependencies-0.2.0-21.adistro.noarch  
Solution 3: break mock-pkg-has-dependencies-0.2.0-21.adistro.noarch by ignoring some  
of its dependencies  
  
Choose from above solutions by number or cancel [1/2/3/c] (c): c
```

In questo esempio, il pacchetto mock-pkg-standalone è bloccato, cosa che è possibile verificare eseguendo `sudo zypper locks` e cercando il nome del pacchetto nell'output.

Oppure potresti vedere delle voci di log che indicano errori nel controllo delle dipendenze:

```
Encountered a known exception in the CLI Invoker:  
CLIInvokerError(error_message='Dependency check failure during commit process',  
error_code='4')
```

 Note

Questo problema si verifica solo durante `Install` le operazioni. Scanle operazioni non applicano blocchi ai pacchetti e non sono influenzate dai blocchi esistenti.»

Causa: questo errore si verifica quando i blocchi dei pacchetti zypper impediscono l'installazione o l'aggiornamento dei pacchetti a causa di conflitti di dipendenza. I lucchetti dei pacchetti possono essere presenti per diversi motivi:

- Customer-applied blocchi: tu o il tuo amministratore di sistema avete bloccato manualmente i pacchetti usando comandi zypper come `zypper addlock`.
- Patch Manager ha rifiutato le patch: applica Patch Manager automaticamente i blocchi dei pacchetti quando specifichi i pacchetti nell'elenco delle patch rifiutate baseline delle patch per impedirne l'installazione.
- Blocchi residui dovuti a operazioni interrotte: in rari casi, se un'operazione di patch è stata interrotta (ad esempio dal riavvio del sistema) prima di poter eliminare i blocchi temporanei, i blocchi residui dei pacchetti Patch Manager potrebbero rimanere sul nodo gestito.

Soluzione: per risolvere i problemi di blocco dei pacchetti zypper, segui questi passaggi in base alla causa:

Fase 1: identificare i pacchetti bloccati

Connettersi SLES al nodo ed eseguire il comando seguente per elencare tutti i pacchetti attualmente bloccati:

```
sudo zypper locks
```

Fase 2: Determinare l'origine dei blocchi

- Se i pacchetti bloccati sono quelli che hai bloccato intenzionalmente per la stabilità del sistema, valuta se devono rimanere bloccati o se possono essere temporaneamente sbloccati per essere patchati.
- Se i pacchetti bloccati corrispondono alle voci dell'elenco delle tue baseline delle patch Patch rifiutate, si tratta probabilmente di blocchi residui dovuti a un'operazione di patch interrotta. Durante le normali operazioni, Patch Manager applica temporaneamente questi blocchi e li rimuove automaticamente al termine dell'operazione. È possibile rimuovere i pacchetti dall'elenco dei pacchetti rifiutati o modificare le regole della baseline delle patch.
- Se non riconosci i pacchetti bloccati e non sono stati bloccati intenzionalmente, potrebbero essere blocchi residui di una precedente operazione di patch interrotta.

Fase 3: rimuovere i lucchetti in modo appropriato

Utilizza il seguente comando per rimuovere blocchi specifici dei pacchetti:

```
sudo zypper remove-lock package-name
```

Per rimuovere tutti i blocchi dei pacchetti (usare con cautela), esegui:

```
sudo zypper cleanlocks
```

Fase 4: aggiorna la baseline delle patch (se applicabile)

Se i blocchi sono stati causati da patch rifiutate nella baseline delle patch:

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Patch Manager.
3. Scegli la scheda baseline delle patch e quindi scegli la tua baseline delle patch personalizzata.
4. Scegli Operazioni, Modifica baseline delle patch.
5. Nella sezione Patch rifiutate, esamina i pacchetti elencati e rimuovi quelli di cui dovrebbe essere consentita l'installazione.
6. Scegli Save changes (Salva modifiche).

Fase 5: Riprovare a eseguire l'operazione con la patch

Dopo aver rimosso i blocchi problematici e aggiornato la baseline delle patch, se necessario, esegui nuovamente il documento `AWS-RunPatchBaseline`.

Note

Quando Patch Manager applica blocchi per le patch rifiutate durante `Install` le operazioni, è progettato per ripulire automaticamente questi blocchi al termine dell'operazione di patch. Se vedi questi blocchi durante l'esecuzione `sudo zypper locks`, significa che una precedente operazione di patch è stata interrotta prima che potesse avvenire la pulizia. Tuttavia, se l'operazione di una patch viene interrotta, potrebbe essere necessaria la pulizia manuale come descritto in questa procedura.

Prevenzione: per evitare future controversie tra zypper lock:

- Esamina attentamente l'elenco delle patch rifiutate nella baseline delle patch per accertarti che includa solo i pacchetti che desideri veramente escludere.
- Evita di bloccare manualmente i pacchetti che potrebbero essere necessari come dipendenze per gli aggiornamenti di sicurezza.
- Se devi bloccare i pacchetti manualmente, documenta i motivi e rivedi periodicamente i blocchi.
- Assicuratevi che le operazioni relative alle patch vengano completate correttamente e che non vengano interrotte dal riavvio del sistema o da altri fattori.
- Monitora le operazioni di patch fino al completamento ed evita di interromperle con riavvii del sistema o altre azioni che potrebbero impedire la corretta pulizia dei blocchi temporanei.

Problema: impossibile acquisire il lucchetto. È in corso un'altra operazione di patching.

Problema: durante l'esecuzione `AWS-RunPatchBaseline`, l'applicazione della patch non riesce con il codice di errore 4 e il seguente messaggio di errore.

```
[ERROR]: Cannot acquire lock on /var/log/amazon/ssm/patch-baseline-concurrent.lock.  
Another patching operation is in progress.
```

Causa: questo errore si verifica quando più operazioni di patching tentano di essere eseguite contemporaneamente sullo stesso nodo gestito. Il file di blocco impedisce operazioni di patching simultanee per evitare conflitti e garantire la stabilità del sistema.

Soluzione: assicurati che le operazioni di patching non siano pianificate per essere eseguite contemporaneamente sullo stesso nodo gestito. Rivedi le seguenti configurazioni per identificare e risolvere i conflitti di pianificazione:

- Politiche sulle patch: controllate le configurazioni delle politiche di patch di Quick Setup per assicurarvi che non si sovrappongano ad altre pianificazioni di patch.
- Finestre di manutenzione: rivedi le associazioni delle finestre di manutenzione per verificare che più finestre non siano destinate agli stessi nodi gestiti con attività di patch in momenti sovrapposti.
- Operazioni manuali di Patch now: evita di avviare operazioni manuali con Patch now mentre è in corso l'applicazione pianificata delle patch.

Errori durante l'esecuzione su **AWS-RunPatchBaseline** Windows Server

Problema: coppie di prodotti family/product non corrispondenti

Problema: Quando si crea una baseline delle patch nella console Systems Manager, è necessario specificare una famiglia di prodotti e un prodotto. Ad esempio si potrebbe scegliere:

- Product family (Famiglia di prodotti): `Office`

Product (Prodotto): `Office 2016`

Causa: se si tenta di creare una baseline di patch con una family/product coppia di prodotti non corrispondente, viene visualizzato un messaggio di errore. Di seguito sono elencati i motivi per cui questo può verificarsi:

- Hai selezionato una famiglia di prodotti e una coppia di prodotti validi ma poi hai rimosso la selezione della famiglia di prodotti.
- È stato scelto un prodotto dal sottoelenco *Obsolete or mismatched options* (Opzioni obsolete o non corrispondenti) anziché dal sottoelenco *Available and matching options* (Opzioni disponibili e corrispondenti).

Gli elementi nel sottoelenco delle opzioni obsolete o non corrispondenti potrebbero essere stati inseriti per errore tramite un comando SDK o (). AWS Command Line Interface `AWS CLI create-patch-baseline` Questo potrebbe significare che è stato introdotto un errore di digitazione o che un prodotto è stato assegnato alla famiglia di prodotti sbagliata. Un prodotto viene incluso anche nel sottoelenco Opzioni obsolete o non corrispondenti, se è stato specificato per una baseline delle patch precedente, ma in Microsoft non sono disponibili patch.

Soluzione: Per evitare che il problema si presenti nella console, è preferibile scegliere sempre le opzioni dai sottoelenchi **Currently available** (Attualmente disponibili).

È inoltre possibile visualizzare i prodotti per i quali attualmente sono disponibili patch utilizzando il comando [describe-patch-properties](#) in AWS CLI o il comando API [DescribePatchProperties](#).

Problema: l'**AWS-RunPatchBaseline** output restituisce un HRESULT (Windows Server)

Problema: hai ricevuto un errore simile al seguente:

```
-----ERROR-----
Invoke-PatchBaselineOperation : Exception Details: An error occurred when
attempting to search Windows Update.
Exception Level 1:
  Error Message: Exception from HRESULT: 0x80240437
  Stack Trace: at WUApiLib.IUpdateSearcher.Search(String criteria)..
(Windows updates)
11/22/2020 09:17:30 UTC | Info | Searching for Windows Updates.
11/22/2020 09:18:59 UTC | Error | Searching for updates resulted in error: Exception
from HRESULT: 0x80240437
-----ERROR-----
failed to run commands: exit status 4294967295
```

Causa: questo output indica che le API native di Windows Update non sono in grado di eseguire le operazioni di applicazione di patch.

Soluzione: controlla il codice `HRESULT` negli argomenti di microsoft.com seguenti per identificare le fasi di risoluzione dei problemi per risolvere l'errore:

- [Codici di errore di Windows Update per componente](#)
- [Errori comuni e mitigazione di Windows Update](#)

Problema: il nodo gestito non ha accesso a Windows Update Catalog o WSUS

Problema: hai ricevuto un errore simile al seguente:

```
Downloading PatchBaselineOperations PowerShell module from https://s3.aws-api-
domain/path_to_module.zip to C:\Windows\TEMP\Amazon.PatchBaselineOperations-1.29.zip.

Extracting PatchBaselineOperations zip file contents to temporary folder.
```

```
Verifying SHA 256 of the PatchBaselineOperations PowerShell module files.

Successfully downloaded and installed the PatchBaselineOperations PowerShell module.

Patch Summary for

PatchGroup :

BaselineId :

Baseline : null

SnapshotId :

RebootOption : RebootIfNeeded

OwnerInformation :

OperationType : Scan

OperationStartTime : 1970-01-01T00:00:00.0000000Z

OperationEndTime : 1970-01-01T00:00:00.0000000Z

InstalledCount : -1

InstalledRejectedCount : -1

InstalledPendingRebootCount : -1

InstalledOtherCount : -1

FailedCount : -1

MissingCount : -1

NotApplicableCount : -1

UnreportedNotApplicableCount : -1

EC2AMAZ-VL3099P - PatchBaselineOperations Assessment Results - 2020-12-30T20:59:46.169

-----ERROR-----
```

Invoke-PatchBaselineOperation : Exception Details: An error occurred when attempting to search Windows Update.

Exception Level 1:

Error Message: Exception from HRESULT: 0x80072EE2

Stack Trace: at WUApiLib.IUpdateSearcher.Search(String criteria)

at

Amazon.Patch.Baseline.Operations.PatchNow.Implementations.WindowsUpdateAgent.SearchForUpdates(

searchCriteria)

At C:\ProgramData\Amazon\SSM\InstanceData\i-02573cafcfEXAMPLE\document\orchestration\3d2d4864-04b7-4316-84fe-eafff1ea58

e3\PatchWindows_script.ps1:230 char:13

+ \$response = Invoke-PatchBaselineOperation -Operation Install -Snapsho ...

+ ~~~~~

+ CategoryInfo : OperationStopped:

(Amazon.Patch.Ba...UpdateOperation:InstallWindowsUpdateOperation) [Inv

oke-PatchBaselineOperation], Exception

+ FullyQualifiedErrorId : Exception Level 1:

Error Message: Exception Details: An error occurred when attempting to search Windows Update.

Exception Level 1:

Error Message: Exception from HRESULT: 0x80072EE2

Stack Trace: at WUApiLib.IUpdateSearcher.Search(String criteria)

at

Amazon.Patch.Baseline.Operations.PatchNow.Implementations.WindowsUpdateAgent.SearchForUpdates(

searc

```
---Error truncated---
```

Causa: questo errore potrebbe essere correlato ai componenti di Windows Update o a una mancanza di connettività al catalogo di Windows Update o Windows Server Update Services (WSUS).

Soluzione: verifica che il nodo gestito disponga di connettività al [Catalogo Microsoft Update](#) tramite un gateway Internet, un gateway NAT o un'istanza NAT. Se si utilizza WSUS, verificare che il nodo gestito disponga della connettività al server WSUS nell'ambiente in uso. Se la connettività è disponibile per la destinazione desiderata, consulta la documentazione Microsoft per altre potenziali cause di HRESULT 0x80072EE2. Questo potrebbe indicare un problema a livello di sistema operativo.

Problema: il PatchBaselineOperations PowerShell modulo non è scaricabile

Problema: hai ricevuto un errore simile al seguente.

```
Preparing to download PatchBaselineOperations PowerShell module from S3.

Downloading PatchBaselineOperations PowerShell module from https://s3.aws-api-
domain/path_to_module.zip to C:\Windows\TEMP\Amazon.PatchBaselineOperations-1.29.zip.
-----ERROR-----

C:\ProgramData\Amazon\SSM\InstanceData\i-02573cafcfEXAMPLE\document\orchestration
\aaaaaaaa-bbbb-cccc-dddd-4f6ed6bd5514\

PatchWindows\_script.ps1 : An error occurred when executing PatchBaselineOperations:
Unable to connect to the remote server

+ CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException

+ FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,_script.ps1

failed to run commands: exit status 4294967295
```

Soluzione: controlla la connettività del nodo gestito e le autorizzazioni per Amazon Simple Storage Service (Amazon S3). Il ruolo del nodo gestito AWS Identity and Access Management (IAM) deve utilizzare le autorizzazioni minime citate in. [Agente SSM comunicazioni con AWS bucket S3 gestiti](#) Il nodo deve comunicare con l'endpoint Amazon S3 tramite l'endpoint gateway Amazon S3, il gateway NAT o il gateway Internet. Per ulteriori informazioni sui requisiti di VPC Endpoint per AWS Systems Manager SSM Agent (SSM Agent), consulta. [Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager](#)

Problema: patch mancanti

Problema: AWS-RunPatchbaseline completato con successo, ma ci sono alcune patch mancanti.

Di seguito sono elencate alcune cause comuni e le loro soluzioni.

Causa 1: la baseline non è efficace.

Soluzione 1: per verificare se questa è la causa, procedi come indicato di seguito.

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Run Command.
3. Seleziona la scheda Cronologia dei comandi e quindi seleziona il comando di cui si desidera controllare la baseline.
4. Seleziona il nodo gestito con patch mancanti.
5. Seleziona Fase 1 - Output e trova il valore BaselineId.
6. Controlla la [Configurazione della patch](#) assegnata, ovvero il sistema operativo, il nome del prodotto, la classificazione e la gravità per la baseline delle patch.
7. Accedi a [Catalogo Microsoft Update](#).
8. Eseguire una ricerca negli ID articolo Microsoft Knowledge Base (KB), ad esempio KB3216916.
9. Verifica che il valore in Prodotto corrisponda a quello del tuo nodo e seleziona il Titolo corrispondente. Si aprirà una nuova finestra Dettagli aggiornamento.
10. Nella scheda Panoramica, classificazione e Gravità MSRC devono corrispondere alla configurazione della baseline delle patch trovata in precedenza.

Causa 2: la patch è stata sostituita.

Soluzione 2: Per verificare che sia vero, procedi come indicato di seguito.

1. Accedi a [Catalogo Microsoft Update](#).
2. Eseguire una ricerca negli ID articolo Microsoft Knowledge Base (KB), ad esempio KB3216916.
3. Verifica che il valore in Prodotto corrisponda a quello del tuo nodo e seleziona il Titolo corrispondente. Si aprirà una nuova finestra Dettagli aggiornamento.
4. Accedi alla scheda Package details. Cerca una voce sotto l'intestazione Questo aggiornamento è stato sostituito dagli aggiornamenti seguenti:

Causa 3: la stessa patch potrebbe avere numeri KB diversi, perché gli aggiornamenti in linea di WSUS e Windows vengono gestiti come canali di rilascio indipendenti da Microsoft.

Soluzione 3: verifica l'idoneità della patch. Se il pacchetto non è disponibile in WSUS, installa [Sistema operativo Build 14393.3115](#). Se il pacchetto è disponibile per tutte le build del sistema operativo, installa [Build del sistema operativo 18362.1256 e 18363.1256](#).

Problema: impossibile acquisire il lucchetto. È in corso un'altra operazione di patching.

Problema: durante l'esecuzione `AWS-RunPatchBaseline`, l'applicazione della patch non riesce con il codice di errore 4 e il seguente messaggio di errore.

```
Cannot acquire lock on C:\ProgramData\Amazon\SSM\patch-baseline-concurrent.lock.  
Another patching operation is in progress.
```

Causa: questo errore si verifica quando più operazioni di patching tentano di essere eseguite contemporaneamente sullo stesso nodo gestito. Il file di blocco impedisce operazioni di patching simultanee per evitare conflitti e garantire la stabilità del sistema.

Soluzione: assicurati che le operazioni di patching non siano pianificate per essere eseguite contemporaneamente sullo stesso nodo gestito. Rivedi le seguenti configurazioni per identificare e risolvere i conflitti di pianificazione:

- Politiche sulle patch: controllate le configurazioni delle politiche di patch di Quick Setup per assicurarvi che non si sovrappongano ad altre pianificazioni di patch.
- Finestre di manutenzione: rivedi le associazioni delle finestre di manutenzione per verificare che più finestre non siano destinate agli stessi nodi gestiti con attività di patch in momenti sovrapposti.
- Operazioni manuali di Patch now: evita di avviare operazioni manuali con Patch now mentre è in corso l'applicazione pianificata delle patch.

Errori durante l'esecuzione su macOS **AWS-RunPatchBaseline**

Problema: impossibile acquisire il lucchetto. È in corso un'altra operazione di patching.

Problema: durante l'esecuzione `AWS-RunPatchBaseline`, l'applicazione della patch non riesce con il codice di errore 4 e il seguente messaggio di errore.

```
[ERROR]: Cannot acquire lock on /var/log/amazon/ssm/patch-baseline-concurrent.lock.  
Another patching operation is in progress.
```

Causa: questo errore si verifica quando più operazioni di patching tentano di essere eseguite contemporaneamente sullo stesso nodo gestito. Il file di blocco impedisce operazioni di patching simultanee per evitare conflitti e garantire la stabilità del sistema.

Soluzione: assicurati che le operazioni di patching non siano pianificate per essere eseguite contemporaneamente sullo stesso nodo gestito. Rivedi le seguenti configurazioni per identificare e risolvere i conflitti di pianificazione:

- **Politiche sulle patch:** controllate le configurazioni delle politiche di patch di Quick Setup per assicurarvi che non si sovrappongano ad altre pianificazioni di patch.
- **Finestre di manutenzione:** rivedi le associazioni delle finestre di manutenzione per verificare che più finestre non siano destinate agli stessi nodi gestiti con attività di patch in momenti sovrapposti.
- **Operazioni manuali di Patch now:** evita di avviare operazioni manuali con Patch now mentre è in corso l'applicazione pianificata delle patch.

Utilizzo Supporto AWS Runbook di automazione

Supporto AWS fornisce due runbook di automazione che è possibile utilizzare per risolvere determinati problemi relativi all'applicazione di patch.

- **AWSSupport-TroubleshootWindowsUpdate** - Il runbook [AWSSupport-TroubleshootWindowsUpdate](#) viene utilizzato per identificare problemi che potrebbero causare errori negli aggiornamenti di Windows Server per le istanze Windows Server Amazon Elastic Compute Cloud (Amazon EC2).
- **AWSSupport-TroubleshootPatchManagerLinux**— Il [AWSSupport-TroubleshootPatchManagerLinux](#) runbook risolve i problemi più comuni che possono causare un errore di patch sui nodi gestiti utilizzando Linux-based Patch Manager. L'obiettivo principale di questo runbook è identificare la causa principale dell'errore del comando patch e suggerire un piano di correzione.

Note

L'esecuzione dei runbook di automazione è a pagamento. Per informazioni, consulta [AWS Systems Manager Pricing for Automation](#).

Contattare Supporto AWS

Se non riesci a trovare soluzioni per la risoluzione dei problemi in questa sezione o nei problemi di Systems Manager in [AWS re:Post](#), e se disponi di un [piano Sviluppatore, Business o Enterprise Supporto](#), è possibile creare un caso di supporto tecnico a [Supporto AWS](#).

Prima di contattare Supporto, raccogli i seguenti articoli:

- [Log di SSM Agent](#)
- Run CommandID comando, ID finestra di manutenzione o ID esecuzione Automation
- Per i nodi gestiti Windows Server, raccogli anche quanto segue:
 - %PROGRAMDATA%\Amazon\PatchBaselineOperations\Log come descritto nella scheda Windows di [Come vengono installate le patch](#)
 - Log degli aggiornamenti di Windows: per Windows Server 2012 R2 e versioni precedenti, usa %windir%/WindowsUpdate.log. Per il Windows Server 2016 e versioni successive, esegui prima il PowerShell comando [Get-WindowsUpdateLog](#) prima di utilizzarlo %windir%/WindowsUpdate.log
- Per i nodi gestiti da Linux, raccogli anche quanto segue:
 - Il contenuto della directory /var/lib/amazon/ssm/*instance-id*/document/orchestration/*Run-Command-execution-id*/awsrunShellScript/PatchLinux

AWS Systems Manager Run Command

Usando Run Command, puoi gestire in remoto e in sicurezza la configurazione dei tuoi nodi gestiti. Un nodo gestito è qualsiasi istanza Amazon Elastic Compute Cloud (Amazon EC2) o macchina non EC2 nel tuo [ambiente](#) ibrido e multicloud che è stata configurata per Systems Manager. Con Run Command, puoi automatizzare le attività amministrative comuni ed eseguire modifiche di configurazione una tantum su larga scala. Puoi utilizzarlo Run Command da Console di gestione AWS, the AWS Command Line Interface (AWS CLI) o AWS Tools for Windows PowerShell SDK. AWS Run Command è offerto senza costi aggiuntivi. Per cominciare a utilizzare Run Command, apri la [console di Systems Manager](#). Nel pannello di navigazione, scegli Run Command.

Questa sezione contiene gli argomenti seguenti.

- [Configurazione Run Command](#)
- [Aggiornamento del software utilizzando Run Command](#)

- [Utilizzo dei codici di uscita nei comandi](#)
- [Esecuzione di comandi utilizzando una versione specifica del documento](#)
- [Risoluzione dei problemi di Systems Manager](#)

Gli amministratori utilizzano Run Command per installare o avviare le applicazioni, creare una pipeline di distribuzione, acquisire i file di registro quando un'istanza viene rimossa da un gruppo Auto Scaling e unire le istanze a un dominio Windows.

L'API Run Command segue un modello di consistenza finale dovuto alla natura distribuita del sistema che supporta l'API. Ciò significa che il risultato di un comando API eseguito che influisce sulle risorse non è immediatamente visibile a tutti i comandi successivi eseguiti. È necessario tenerlo a mente quando si esegue un comando API che segue immediatamente un comando API precedente.

Nozioni di base

La tabella seguente include informazioni utili per iniziare a usare Run Command.

Topic	Informazioni
Configurazione dei nodi gestiti per AWS Systems Manager	Verifica di aver completato i requisiti di configurazione per le istanze Amazon Elastic Compute Cloud (Amazon EC2) e le macchine non EC2 in un ambiente ibrido e multicloud .
Gestione dei nodi in ambienti ibridi e multicloud con Systems Manager	(Facoltativo) Registra server e VM locali con in modo da poterli gestire utilizzando AWS Run Command
the section called “Gestione dei dispositivi edge con Systems Manager”	(Facoltativo) Configura i dispositivi edge in modo da poterli gestire utilizzando Run Command.
Esecuzione di comandi su nodi gestiti	Scopri come eseguire un comando rivolto a uno o più nodi gestiti utilizzando il Console di gestione AWS.
Run Command Spiegazioni passo per passo di	Scopri come eseguire comandi utilizzando Tools for Windows PowerShell o. AWS CLI

EventBridge supporto

Questo strumento Systems Manager è supportato sia come tipo di evento che come tipo di destinazione nelle EventBridge regole di Amazon. Per informazioni, consulta [Monitoraggio degli eventi di Systems Manager con Amazon EventBridge](#) e [Riferimento: modelli e tipi di EventBridge eventi Amazon per Systems Manager](#).

Ulteriori informazioni

- [Esecuzione di comandi da remoto Run Command su un'istanza EC2 \(tutorial di 10 minuti\)](#)
- [Service Quotas di Systems Manager](#) nella Riferimenti generali di Amazon Web Services
- [AWS Systems Manager Documentazione di riferimento delle API](#)

Configurazione Run Command

Prima di poter gestire i nodi utilizzando Run Command, configura una policy AWS Identity and Access Management (IAM) per qualsiasi utente che eseguirà i comandi. Quando utilizzi delle chiavi di condizione globali per l'azione SendCommand nelle policy IAM, è necessario includere la chiave di condizione `aws:ViaAWSService` e impostare il valore booleano su `true`. Di seguito è riportato un esempio di :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand"
      ],
      "Resource": [
        "arn:aws:ssm:us-east-1:111122223333:document/YourDocument"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceVpce": [
            "vpce-1234567890abcdef0"
          ]
        }
      }
    }
  ]
}
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand"
      ],
      "Resource": [
        "arn:aws:ssm:us-east-1:111122223333:document/YourDocument"
      ],
      "Condition": {
        "Bool": {
          "aws:ViaAWSService": "true"
        }
      }
    }
  ]
}
```

È necessario anche configurare i nodi per Systems Manager. Per ulteriori informazioni, consulta [Configurazione dei nodi gestiti per AWS Systems Manager](#).

Si consiglia inoltre di completare le seguenti attività di configurazione facoltative per ridurre al minimo la posizione di sicurezza e la gestione quotidiana dei nodi gestiti.

Monitora le esecuzioni dei comandi utilizzando Amazon EventBridge

Puoi utilizzarlo EventBridge per registrare le modifiche allo stato di esecuzione dei comandi. È possibile scegliere di creare una regola che venga eseguita ogni volta che si verifica una transizione di stato o quando si verifica una transizione verso uno o più stati di interesse. È inoltre possibile specificare Run Command come azione target quando si verifica un EventBridge evento. Per ulteriori informazioni, consulta [Configurazione EventBridge per gli eventi di Systems Manager](#).

Monitora le esecuzioni dei comandi utilizzando Amazon Logs CloudWatch

Puoi configurare l'invio periodico Run Command di tutti gli output dei comandi e i log degli errori a un gruppo di CloudWatch log di Amazon. È possibile monitorare i log di output in tempo quasi reale, cercare locuzioni, valori o modelli specifici e creare allarmi in base alla ricerca. Per ulteriori informazioni, consulta [Configurazione di Amazon CloudWatch Logs per Run Command](#).

Restrict Run Command accesso a nodi gestiti specifici

Puoi limitare la capacità di un utente di eseguire comandi su nodi gestiti utilizzando AWS Identity and Access Management (IAM). In particolare, è possibile creare una policy IAM con una condizione in base alla quale l'utente può eseguire i comandi solo sui nodi gestiti contrassegnati con tag specifici. Per ulteriori informazioni, consulta [Limitazione Run Command accesso basato su tag](#).

Limitazione Run Command accesso basato su tag

Questa sezione descrive come limitare la capacità di un utente di eseguire comandi sui nodi gestiti specificando una condizione di tag in una policy IAM. I nodi gestiti includono istanze Amazon EC2 e nodi non EC2 in un [ambiente ibrido e multicloud](#) configurato per Systems Manager. Sebbene le informazioni non siano presentate in modo esplicito, puoi anche limitare l'accesso ai dispositivi AWS IoT Greengrass principali gestiti. Per iniziare, devi tagging dei dispositivi AWS IoT Greengrass . Per ulteriori informazioni, consulta [Applicazione di tag alle risorse di AWS IoT Greengrass Version 2](#) nella Guida per gli sviluppatori di AWS IoT Greengrass Version 2 .

È possibile limitare l'esecuzione dei comandi a nodi gestiti specifici creando una policy IAM che include una condizione in base alla quale l'utente può eseguire i comandi solo sui nodi a cui sono applicati tag specifici. Nell'esempio seguente, l'utente può utilizzare Run Command (Effect: Allow, Action: ssm:SendCommand) utilizzando qualsiasi documento SSM (Resource: arn:aws:ssm:*:*:document/*) su qualsiasi nodo (Resource: arn:aws:ec2:*:*:instance/*) a condizione che il nodo sia un Finance WebServer (ssm:resourceTag/Finance: WebServer). Se l'utente invia un comando a un nodo privo di tag o con un tag diverso da Finance: WebServer, i risultati dell'esecuzione mostrano AccessDenied.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand"
      ],
      "Resource": [
        "arn:aws:ssm:*:*:document/*"
      ]
    }
  ]
}
```

```

    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "ssm:SendCommand"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition": {
      "StringLike": {
        "ssm:resourceTag/Finance": [
          "WebServers"
        ]
      }
    }
  }
]
}

```

È possibile creare policy IAM che permettono a un utente di eseguire comandi su nodi gestiti contrassegnati con più tag. La policy seguente consente all'utente di eseguire comandi su nodi gestiti che dispongono di due tag. Se l'utente invia un comando a un nodo non contrassegnato con questi due tag, i risultati dell'esecuzione mostrano AccessDenied.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ssm:resourceTag/tag_key1": [
            "tag_value1"
          ]
        }
      }
    }
  ]
}

```

```

        ],
        "ssm:resourceTag/tag_key2": [
            "tag_value2"
        ]
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ssm:SendCommand"
    ],
    "Resource": [
        "arn:aws:ssm:us-west-1::document/AWS-*",
        "arn:aws:ssm:us-east-2::document/AWS-*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ssm:UpdateInstanceInformation",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:GetDocument"
    ],
    "Resource": "*"
}
]
}

```

È anche possibile creare policy IAM che consentono a un utente di eseguire comandi su più gruppi di nodi gestiti con tag. La policy di esempio seguente consente all'utente di eseguire comandi su uno o su entrambi i gruppi di nodi con tag.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",

```

```

    "Action":[
      "ssm:SendCommand"
    ],
    "Resource":"*",
    "Condition":{"
      "StringLike":{"
        "ssm:resourceTag/tag_key1":[
          "tag_value1"
        ]
      }
    }
  },
  {
    "Effect":"Allow",
    "Action":[
      "ssm:SendCommand"
    ],
    "Resource":"*",
    "Condition":{"
      "StringLike":{"
        "ssm:resourceTag/tag_key2":[
          "tag_value2"
        ]
      }
    }
  },
  {
    "Effect":"Allow",
    "Action":[
      "ssm:SendCommand"
    ],
    "Resource":[
      "arn:aws:ssm:us-west-1::document/AWS-*",
      "arn:aws:ssm:us-east-2::document/AWS-*"
    ]
  },
  {
    "Effect":"Allow",
    "Action":[
      "ssm:UpdateInstanceInformation",
      "ssm:ListCommands",
      "ssm:ListCommandInvocations",
      "ssm:GetDocument"
    ]
  },

```



```
    "Resource": "*"
  }
]
}
```

Per ulteriori informazioni sulla creazione di policy IAM, consulta la pagina [Policy gestite e policy in linea](#) nella Guida per l'utente IAM. Per ulteriori informazioni sull'aggiunta di tag ai nodi gestiti, consulta [Editor di tag](#) nella AWS Resource Groups Guida per l'utente di.

Esecuzione di comandi su nodi gestiti

Questa sezione include informazioni su come inviare i comandi dalla console AWS Systems Manager a nodi gestiti. Questa sezione include anche informazioni su come annullare un comando.

Nota che se il tuo nodo è configurato con l'opzione di montaggio noexec per la directory var, Run Command non è in grado di eseguire correttamente i comandi.

Important

Quando si invia un comando utilizzando Run Command, non includere informazioni riservate formattate come testo normale, ad esempio password, dati di configurazione o altri segreti. Tutte le attività dell'API Systems Manager nel tuo account vengono registrate in un bucket S3 per i log. AWS CloudTrail Ciò significa che qualsiasi utente con accesso a quel bucket S3 può visualizzare i valori in testo normale di quei segreti. Per questo motivo, si consiglia vivamente di creare e utilizzare parametri SecureString per crittografare i dati sensibili utilizzati nelle operazioni di Systems Manager.

Per ulteriori informazioni, consulta [Gestire l'accesso a Parameter Store parametri che utilizzano le politiche IAM](#).

La cronologia di esecuzione dell'esecuzione

La cronologia di ciascun comando è disponibile per 30 giorni. Inoltre è possibile archiviare una copia di tutti i file di log in Amazon Simple Storage Service oppure ottenere un audit trail di tutte le chiamate API in AWS CloudTrail.

Informazioni correlate

Per informazioni su come inviare comandi tramite altri strumenti, consulta i seguenti argomenti:

- [Procedura dettagliata: usa il AWS Tools for Windows PowerShell con Run Command](#) o gli esempi nella [AWS Systems Manager sezione del Cmdlet Reference. AWS Strumenti per PowerShell](#)
- [Procedura dettagliata: usa il AWS CLI con Run Command](#) o gli esempi nel [Documento di riferimento alla CLI di SSM](#)

Indice

- [Esecuzione di comandi dalla console](#)
- [Esecuzione di comandi utilizzando una versione specifica del documento](#)
- [Esecuzione di comandi su vasta scala](#)
- [Annullamento di un comando](#)

Esecuzione di comandi dalla console

È possibile utilizzare Run Command from Console di gestione AWS per configurare i nodi gestiti senza dovervi accedere. Questo argomento include un esempio che mostra come [aggiornare SSM Agent](#) su un nodo gestito utilizzando Run Command.

Prima di iniziare

Prima di inviare un comando utilizzando Run Command verifica che i nodi gestiti soddisfino tutti i [requisiti di configurazione](#) di Systems Manager.

Per inviare un comando usando Run Command

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Run Command.
3. Seleziona Esegui comando.
4. Nell'elenco Command document (Documento comando), scegliere un documento di Systems Manager.
5. Nella sezione Command parameters (Parametri di comando) specificare i valori per i parametri necessari.
6. In Destinazioni, scegli i nodi gestiti in cui si desidera eseguire questa operazione specificando i tag, selezionando le istanze o i dispositivi edge manualmente o indicando un gruppo di risorse.

 Tip

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

7. In Altri parametri:

- In Commento, digita le informazioni su questo comando.
- In Timeout (secondi), specifica il numero di secondi che il sistema dovrà attendere prima di generare un errore per l'intera esecuzione del comando.

8. Per Controllo velocità:

- In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti presi di mira, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.
9. (Facoltativo) Scegliete un CloudWatch allarme da applicare al comando per il monitoraggio. Per allegare un CloudWatch allarme al comando, il responsabile IAM che esegue il comando deve disporre dell'autorizzazione per `iam:createServiceLinkedRole`. Per ulteriori informazioni sugli CloudWatch allarmi, consulta [Utilizzo degli CloudWatch](#) allarmi Amazon. Si noti che se l'allarme si attiva, qualsiasi chiamata di comando in sospeso non viene eseguita.
10. (Facoltativo) Nella sezione Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Scrivi l'output del comando in un bucket S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

 Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

11. Se vuoi che vengano inviate notifiche sullo stato dell'esecuzione del comando, nella sezione Notifiche SNS selezionare la casella di controllo Abilita notifiche SNS.

Per ulteriori informazioni sulla configurazione delle notifiche Amazon SNS per Run Command, consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

12. Scegli Esegui.

Per informazioni su come annullare un comando, consulta [Annullamento di un comando](#).

Riesecuzione dei comandi

Systems Manager include due opzioni che consentono di eseguire nuovamente un comando dalla pagina Esegui comando nella console Systems Manager.

- **Riesegui:** questo pulsante consente di eseguire lo stesso comando senza apportarvi modifiche.
- **Copia su nuovo:** questo pulsante copia le impostazioni di un comando in un nuovo comando e ti dà la possibilità di modificare tali impostazioni prima di eseguirlo.

Per eseguire nuovamente un comando

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Run Command.

3. Scegliere un comando da eseguire nuovamente. È possibile eseguire nuovamente un comando immediatamente dopo averlo eseguito dalla pagina dei dettagli del comando. In alternativa, è possibile scegliere un comando eseguito in precedenza dalla scheda Cronologia comandi .
4. Scegliere Rieseguire per eseguire lo stesso comando senza modifiche oppure scegliere Copia in nuovo per modificare le impostazioni dei comandi prima di eseguirli.

Esecuzione di comandi utilizzando una versione specifica del documento

Il parametro `document-version` consente di specificare quale versione di un documento AWS Systems Manager utilizzare quando viene eseguito il comando. È possibile specificare una delle seguenti opzioni per questo parametro:

- `$DEFAULT`
- `$LATEST`
- Numero di versione

Usa la procedura seguente per eseguire un comando utilizzando il parametro `document-version`.

Linux

Per eseguire comandi utilizzando AWS CLI le macchine Linux locali

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Creare un elenco di tutti i documenti disponibili

Questo comando elenca tutti i documenti disponibili per il tuo account in base alle autorizzazioni AWS Identity and Access Management (IAM).

```
aws ssm list-documents
```

3. Esegui il comando seguente per visualizzare le diverse versioni di un documento. *document name* Sostituiscili con le tue informazioni.

```
aws ssm list-document-versions \  
  --name "document name"
```

4. Esegui il comando seguente per eseguire un comando che usa una versione del documento SSM. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
aws ssm send-command \  
  --document-name "AWS-RunShellScript" \  
  --parameters commands="echo Hello" \  
  --instance-ids instance-ID \  
  --document-version '$LATEST'
```

Windows

Per eseguire comandi utilizzando i AWS CLI computer Windows locali

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Creare un elenco di tutti i documenti disponibili

Questo comando elenca tutti i documenti disponibili per il tuo account in base alle autorizzazioni AWS Identity and Access Management (IAM).

```
aws ssm list-documents
```

3. Esegui il comando seguente per visualizzare le diverse versioni di un documento. *document name* Sostituiscili con le tue informazioni.

```
aws ssm list-document-versions ^  
  --name "document name"
```

4. Esegui il comando seguente per eseguire un comando che usa una versione del documento SSM. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
aws ssm send-command ^  
  --document-name "AWS-RunShellScript" ^  
  --parameters commands="echo Hello" ^  
  --instance-ids instance-ID ^  
  --document-version "$LATEST"
```

PowerShell

Per eseguire comandi utilizzando gli strumenti per PowerShell

1. Installa e configura AWS Strumenti per PowerShell (Strumenti per Windows PowerShell), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione di AWS Strumenti per PowerShell](#).

2. Creare un elenco di tutti i documenti disponibili

Questo comando elenca tutti i documenti disponibili per il tuo account in base alle autorizzazioni AWS Identity and Access Management (IAM).

```
Get-SSMDocumentList
```

3. Esegui il comando seguente per visualizzare le diverse versioni di un documento. *document name* Sostituiscili con le tue informazioni.

```
Get-SSMDocumentVersionList `
    -Name "document name"
```

4. Esegui il comando seguente per eseguire un comando che usa una versione del documento SSM. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
Send-SSMCommand `
    -DocumentName "AWS-RunShellScript" `
    -Parameter @{commands = "echo helloWorld"} `
    -InstanceIds "instance-ID" `
    -DocumentVersion $LATEST
```

Esecuzione di comandi su vasta scala

È possibile utilizzare Run Command per eseguire comandi su una flotta di nodi gestiti utilizzando `targets`. Il parametro `targets` accetta una combinazione Key, Value in base ai tag specificati per i nodi gestiti. Quando si esegue il comando, il sistema individua e tenta di eseguire il comando su tutti i nodi gestiti che corrispondono ai tag specificati. Per ulteriori informazioni sull'etichettatura delle istanze gestite, consulta [Tagging your AWS resources](#) nella Tagging Resources User AWS Guide. Per informazioni sulla codifica dei dispositivi IoT gestiti, consulta

[Etichettare AWS IoT Greengrass Version 2 le tue risorse](#) nella Guida per gli sviluppatori. AWS IoT Greengrass Version 2

È anche possibile utilizzare il parametro `targets` per impostare come destinazione un elenco di ID di nodi gestiti specifici, come descritto nella sezione successiva.

Per controllare il modo in cui i comandi vengono eseguiti su centinaia o migliaia di nodi gestiti, `Run Command` include parametri per limitare la concorrenza. È possibile limitare il numero di nodi che elaborano una richiesta contemporaneamente e il numero di errori che possono verificarsi prima che il comando venga annullato.

Indice

- [Impostare come destinazione più nodi gestiti](#)
- [Utilizzo dei controlli di velocità](#)

Impostare come destinazione più nodi gestiti

Puoi eseguire un comando e definire come destinazione i nodi gestiti specificando tag, nomi di gruppi di risorse AWS o ID nodi gestiti.

Gli esempi seguenti mostrano il formato del comando quando si utilizza `Run Command` from the AWS Command Line Interface (AWS CLI). Sostituisci ogni *example resource placeholder* con le tue informazioni. I comandi di esempio in questa sezione sono troncati utilizzando [...].

Esempio 1: definizione di tag come target

Linux & macOS

```
aws ssm send-command \  
  --document-name document-name \  
  --targets Key=tag:tag-name,Values=tag-value \  
  [...]
```

Windows

```
aws ssm send-command ^  
  --document-name document-name ^  
  --targets Key=tag:tag-name,Values=tag-value ^  
  [...]
```


Esempio 2: indirizzamento di un gruppo di AWS risorse in base al nome

Puoi specificare un massimo di un nome del gruppo di risorse per comando. Quando crei un gruppo di risorse, ti consigliamo di includere `AWS::SSM:ManagedInstance` e `AWS::EC2::Instance` come tipi di risorse nei criteri di raggruppamento.

Note

Per inviare comandi destinati a un gruppo di risorse, è necessario disporre delle autorizzazioni AWS Identity and Access Management (IAM) per elencare o visualizzare le risorse che appartengono a quel gruppo. Per ulteriori informazioni, consulta [Impostazione delle autorizzazioni](#) nella Guida per l'utente di AWS Resource Groups .

Linux & macOS

```
aws ssm send-command \  
  --document-name document-name \  
  --targets Key=resource-groups:Name,Values=resource-group-name \  
  [...]
```

Windows

```
aws ssm send-command ^  
  --document-name document-name ^  
  --targets Key=resource-groups:Name,Values=resource-group-name ^  
  [...]
```

Esempio 3: indirizzamento di un gruppo di risorse per tipo di AWS risorsa

Puoi specificare un massimo di un nome del gruppo di risorse per comando. Quando crei un gruppo di risorse, ti consigliamo di includere `AWS::SSM:ManagedInstance` e `AWS::EC2::Instance` come tipi di risorse nei criteri di raggruppamento.

Note

Per inviare comandi destinati a un gruppo di risorse, è necessario disporre delle autorizzazioni IAM per elencare o visualizzare le risorse che appartengono a quel gruppo. Per

ulteriori informazioni, consulta [Impostazione delle autorizzazioni](#) nella Guida per l'utente di AWS Resource Groups .

Linux & macOS

```
aws ssm send-command \  
  --document-name document-name \  
  --targets Key=resource-groups:ResourceTypeFilters,Values=resource-  
type-1,resource-type-2 \  
  [...]
```

Windows

```
aws ssm send-command ^  
  --document-name document-name ^  
  --targets Key=resource-groups:ResourceTypeFilters,Values=resource-  
type-1,resource-type-2 ^  
  [...]
```

Esempio 4: definizione di ID di istanze come target

Gli esempi seguenti mostrano come destinazione i nodi gestiti utilizzando il `instanceids` Chiave con il parametro `targets`. È possibile utilizzare questa chiave per indirizzare i dispositivi AWS IoT Greengrass core gestiti perché a ciascun dispositivo è assegnato un *mi-ID_number*. È possibile visualizzare gli ID dei dispositivi in Fleet Manager.

Linux & macOS

```
aws ssm send-command \  
  --document-name document-name \  
  --targets Key=instanceids,Values=instance-ID-1,instance-ID-2,instance-ID-3 \  
  [...]
```

Windows

```
aws ssm send-command ^  
  --document-name document-name ^  
  --targets Key=instanceids,Values=instance-ID-1,instance-ID-2,instance-ID-3 ^  
  [...]
```

Se hai aggiunto tag ai nodi gestiti per diversi ambienti usando una Key denominata `Environment` e Values pari a `Development`, `Test`, `Pre-production` e `Production`, puoi inviare un comando a tutti i nodi gestiti in uno degli ambienti utilizzando il parametro `targets` con la seguente sintassi.

Linux & macOS

```
aws ssm send-command \  
  --document-name document-name \  
  --targets Key=tag:Environment,Values=Development \  
  [...]
```

Windows

```
aws ssm send-command ^  
  --document-name document-name ^  
  --targets Key=tag:Environment,Values=Development ^  
  [...]
```

Puoi definire altri nodi gestiti come destinazione in altri ambienti aggiungendo voci all'elenco Values. Separa gli elementi con le virgole.

Linux & macOS

```
aws ssm send-command \  
  --document-name document-name \  
  --targets Key=tag:Environment,Values=Development,Test,Pre-production \  
  [...]
```

Windows

```
aws ssm send-command ^  
  --document-name document-name ^  
  --targets Key=tag:Environment,Values=Development,Test,Pre-production ^  
  [...]
```

Variazione: perfezionamento dei target utilizzando più criteri Key

È possibile perfezionare il numero di target per il comando includendo più criteri Key. Se si includono più criteri Key, vengono definite come destinazioni i nodi gestiti che soddisfano tutti i criteri. Il

comando seguente definisce come destinazione tutti i nodi gestiti taggati per il reparto finanze e taggati per il ruolo server di database.

Linux & macOS

```
aws ssm send-command \  
  --document-name document-name \  
  --targets Key=tag:Department,Values=Finance Key=tag:ServerRole,Values=Database \  
  [...]
```

Windows

```
aws ssm send-command ^  
  --document-name document-name ^  
  --targets Key=tag:Department,Values=Finance Key=tag:ServerRole,Values=Database ^  
  [...]
```

Variazione: utilizzo di più criteri Key e Value

Espandendo l'esempio precedente, è possibile definire più reparti e più ruoli server come target includendo altri elementi nei criteri Values.

Linux & macOS

```
aws ssm send-command \  
  --document-name document-name \  
  --targets Key=tag:Department,Values=Finance,Marketing  
Key=tag:ServerRole,Values=WebServer,Database \  
  [...]
```

Windows

```
aws ssm send-command ^  
  --document-name document-name ^  
  --targets Key=tag:Department,Values=Finance,Marketing  
Key=tag:ServerRole,Values=WebServer,Database ^  
  [...]
```

Variazione: definizione di nodi gestiti con tag come destinazione utilizzando più criteri Values

Se hai applicato tag a nodi gestiti per diversi ambienti usando un oggetto Key denominato `Department` e `Values` corrispondente a `Sales` e `Finance`, puoi inviare un comando a tutti i nodi gestiti in questi ambienti utilizzando il parametro `targets` con la sintassi seguente.

Linux & macOS

```
aws ssm send-command \  
  --document-name document-name \  
  --targets Key=tag:Department,Values=Sales,Finance \  
  [...]
```

Windows

```
aws ssm send-command ^  
  --document-name document-name ^  
  --targets Key=tag:Department,Values=Sales,Finance ^  
  [...]
```

È possibile specificare un massimo di cinque chiavi e cinque valori per ogni chiave.

Se una chiave tag (il nome del tag) o un valore tag include spazi, devi racchiudere tra virgolette la chiave o il valore tag, come mostrato nei seguenti esempi.

Esempio: spazi nel tag Value

Linux & macOS

```
aws ssm send-command \  
  --document-name document-name \  
  --targets Key=tag:OS,Values="Windows Server 2016" \  
  [...]
```

Windows

```
aws ssm send-command ^  
  --document-name document-name ^  
  --targets Key=tag:OS,Values="Windows Server 2016" ^  
  [...]
```

Esempio: spazi nella chiave tag e Value

Linux & macOS

```
aws ssm send-command \  
  --document-name document-name \  
  --targets Key="tag:Operating System",Values="Windows Server 2016" \  
  [...]
```

Windows

```
aws ssm send-command ^  
  --document-name document-name ^  
  --targets Key="tag:Operating System",Values="Windows Server 2016" ^  
  [...]
```

Esempio: spazi in un elemento in un elenco di Values

Linux & macOS

```
aws ssm send-command \  
  --document-name document-name \  
  --targets Key=tag:Department,Values="Sales","Finance","Systems Mgmt" \  
  [...]
```

Windows

```
aws ssm send-command ^  
  --document-name document-name ^  
  --targets Key=tag:Department,Values="Sales","Finance","Systems Mgmt" ^  
  [...]
```

Utilizzo dei controlli di velocità

Puoi controllare la velocità con cui i comandi vengono inviati ai nodi gestiti di un gruppo utilizzando controlli di concorrenza e controlli di errore.

Utilizzo di controlli di concorrenza

Puoi controllare il numero di nodi gestiti che eseguono il comando contemporaneamente utilizzando il parametro `max-concurrency` (le opzioni Simultaneità nella pagina Esegui un comando). Puoi specificare un numero assoluto di nodi gestiti, ad esempio **10**, oppure una percentuale del set di

target, ad esempio **10%**. Il sistema di accodamento invia il comando a un singolo nodo e attende il completamento dell'invocazione iniziale prima di inviare il comando ad altri due nodi. Il sistema invia comandi ad altri nodi in modo esponenziale fino al raggiungimento del valore max-concurrency. Il valore predefinito per max-concurrency è 50. Gli esempi seguenti mostrano come specificare valori per il parametro max-concurrency.

Linux & macOS

```
aws ssm send-command \  
  --document-name document-name \  
  --max-concurrency 10 \  
  --targets Key=tag:Environment,Values=Development \  
  [...]
```

```
aws ssm send-command \  
  --document-name document-name \  
  --max-concurrency 10% \  
  --targets Key=tag:Department,Values=Finance,Marketing \  
  Key=tag:ServerRole,Values=WebServer,Database \  
  [...]
```

Windows

```
aws ssm send-command ^  
  --document-name document-name ^  
  --max-concurrency 10 ^  
  --targets Key=tag:Environment,Values=Development ^  
  [...]
```

```
aws ssm send-command ^  
  --document-name document-name ^  
  --max-concurrency 10% ^  
  --targets Key=tag:Department,Values=Finance,Marketing ^  
  Key=tag:ServerRole,Values=WebServer,Database ^  
  [...]
```

Utilizzo dei controlli degli errori

Puoi anche controllare l'esecuzione di un comando su centinaia o migliaia di nodi gestiti impostando un limite di errori usando i parametri max-errors (il campo Soglia di errore nella pagina Esegui

un comando). Il parametro specifica il numero di errori consentiti prima che il sistema smetta di inviare il comando ad altri nodi gestiti. Puoi specificare un numero assoluto di errori, ad esempio **10**, oppure una percentuale della serie di target, ad esempio **10%**. Se ad esempio specifichi **3**, il sistema smette di inviare il comando quando riceve il quarto errore. Se specifichi **0**, il sistema smette di inviare il comando ad altri nodi gestiti non appena viene restituito il primo risultato di errore. Se invii un comando a 50 nodi gestiti e imposti max-errors su **10%**, il sistema smette di inviare il comando ad altri nodi quando riceve il sesto errore.

Per le invocazioni che stanno già eseguendo un comando quando viene raggiunto il valore max-errors, viene consentito il completamento dell'operazione, ma alcune di queste invocazioni potrebbero non riuscire. Se devi assicurarti che non ci siano più chiamate max-errors fallite, imposta max-concurrency in **1** modo che le chiamate procedano una alla volta. Il valore predefinito per max-errors è 0. Gli esempi seguenti mostrano come specificare valori per il parametro max-errors.

Linux & macOS

```
aws ssm send-command \  
  --document-name document-name \  
  --max-errors 10 \  
  --targets Key=tag:Database,Values=Development \  
  [...]
```

```
aws ssm send-command \  
  --document-name document-name \  
  --max-errors 10% \  
  --targets Key=tag:Environment,Values=Development \  
  [...]
```

```
aws ssm send-command \  
  --document-name document-name \  
  --max-concurrency 1 \  
  --max-errors 1 \  
  --targets Key=tag:Environment,Values=Production \  
  [...]
```

Windows

```
aws ssm send-command ^  
  --document-name document-name ^
```



```
--max-errors 10 ^  
--targets Key=tag:Database,Values=Development ^  
[...]
```

```
aws ssm send-command ^  
--document-name document-name ^  
--max-errors 10% ^  
--targets Key=tag:Environment,Values=Development ^  
[...]
```

```
aws ssm send-command ^  
--document-name document-name ^  
--max-concurrency 1 ^  
--max-errors 1 ^  
--targets Key=tag:Environment,Values=Production ^  
[...]
```

Annullamento di un comando

Puoi tentare di annullare un comando finché il servizio mostra che il suo stato è in attesa o in esecuzione. Anche se un comando si trova in uno di questi stati, però, non siamo in grado di garantire che verrà terminato e che il processo sottostante verrà arrestato.

Per annullare un comando usando la console

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Run Command.
3. Selezionare l'invocazione del comando da annullare.
4. Scegli Annulla comando.

Per annullare un comando utilizzando il AWS CLI

Eseguire il seguente comando seguente. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux & macOS

```
aws ssm cancel-command \
```

```
--command-id "command-ID" \  
--instance-ids "instance-ID"
```

Windows

```
aws ssm cancel-command ^  
--command-id "command-ID" ^  
--instance-ids "instance-ID"
```

Per ulteriori informazioni sullo stato di un comando annullato, consulta [Informazioni sugli stati dei comandi](#).

Utilizzo dei codici di uscita nei comandi

In alcuni casi, potrebbe essere necessario controllare la modalità di gestione dei comandi utilizzando i codici di uscita.

Specifica dei codici di uscita nei comandi

Utilizzando `Run Command`, è possibile specificare i codici di uscita per determinare come vengono gestiti i comandi. 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, si dispone di uno script che contiene tre comandi. Il primo non riesce, ma i seguenti riescono. Poiché il comando finale è riuscito, lo stato dell'esecuzione viene segnalato come `succeeded`.

Script di shell

Per chiudere con esito negativo l'intero comando al primo errore, è possibile includere un'istruzione condizionale della shell per uscire dallo script se un comando precedente a quello finale non riesce. Utilizzare l'approccio seguente.

```
<command 1>  
  if [ $? != 0 ]  
  then  
    exit <N>  
  fi  
<command 2>  
<command 3>
```

Nell'esempio seguente, l'intero script ha esito negativo se il primo comando non riesce.

```
cd /test
if [ $? != 0 ]
then
    echo "Failed"
    exit 1
fi
date
```

PowerShell script

PowerShell richiede una chiamata `exit` esplicita negli script per acquisire correttamente il codice Run Command di uscita.

```
<command 1>
if ($?) {<do something>}
else {exit <N>}
<command 2>
<command 3>
exit <N>
```

Ecco un esempio:

```
cd C:\
if ($?) {echo "Success"}
else {exit 1}
date
```

Gestione di riavvii durante l'esecuzione dei comandi

Se si utilizzano Run Command script che riavviano i nodi gestiti, si consiglia di specificare un codice di uscita nello script. Se tenti di riavviare un nodo da uno script utilizzando altri meccanismi, lo stato di esecuzione di script potrebbe non essere aggiornato correttamente, anche se il riavvio è l'ultimo passaggio nel tuo script. Per i nodi gestiti da Windows, è necessario specificare `exit 3010` nello script. Per i nodi gestiti Linux e macOS, è necessario specificare `exit 194`. Il codice di uscita indica ad AWS Systems Manager Agent (SSM Agent) di riavviare il nodo gestito e quindi di riavviare lo script al termine del riavvio. Prima di iniziare il riavvio, SSM Agent notifica al servizio Systems Manager nel cloud che le comunicazioni verranno interrotte durante il riavvio dei server.

 Note

Lo script di riavvio non può fare parte di `aws:runDocument`. Se un documento contiene lo script di riavvio e un altro documento tenta di eseguirlo tramite il plug-in `aws:runDocument`, SSM Agent causerà un errore.

Creare script idempotenti

Quando sviluppi script che riavviano i nodi gestiti, rendi idempotenti gli script in modo che la loro esecuzione prosegua dal punto in cui si è interrotta dopo il riavvio. Gli script idempotenti gestiscono lo stato e verificano se l'operazione è stata eseguita o meno. Questo evita che una fase venga eseguita più volte quando è concepita per un'esecuzione singola.

Ecco un esempio generale di script idempotente che riavvia il nodo gestito più volte.

```
$name = Get current computer name
If ($name -ne $desiredName)
{
    Rename computer
    exit 3010
}

$domain = Get current domain name
If ($domain -ne $desiredDomain)
{
    Join domain
    exit 3010
}

If (desired package not installed)
{
    Install package
    exit 3010
}
```

Esempi

I seguenti esempi di script usano codici di uscita per riavviare i nodi gestiti. L'esempio Linux installa gli aggiornamenti del pacchetto in e riavvia il nodo. L'Windows Server esempio installa lo Telnet-Client sul nodo e quindi lo riavvia.

Amazon Linux 2

```
#!/bin/bash
yum -y update
needs-restarting -r
if [ $? -eq 1 ]
then
    exit 194
else
    exit 0
fi
```

Windows

```
$telnet = Get-WindowsFeature -Name Telnet-Client
if (-not $telnet.Installed)
{
    # Install Telnet and then send a reboot request to SSM Agent.
    Install-WindowsFeature -Name "Telnet-Client"
    exit 3010
}
```

Informazioni sugli stati dei comandi

Run Command riporta informazioni dettagliate sullo stato dei diversi stati in cui si verifica un comando durante l'elaborazione e per ogni nodo gestito che ha elaborato il comando. È possibile monitorare lo stato dei comandi usando i metodi seguenti.

- Scegli l'icona Refresh (Aggiorna) della scheda Commands (Comandi) nell'interfaccia della console Run Command.
- Chiama [list-commands](#) o <https://docs.aws.amazon.com/cli/latest/reference/ssm/list-command-invocations.html> list-command-invocations utilizzando (). AWS Command Line Interface AWS CLI [Get-SSMCommand](#) Oppure [Get-SSMCommandInvocation](#) chiama o AWS Tools for Windows PowerShell usa.
- Configura Amazon EventBridge per rispondere alle modifiche di stato o di stato.
- Configura Amazon Simple Notification Service (Amazon SNS) per l'invio di notifiche relative a tutte le modifiche di stato o a stati specifici come Failed o TimedOut.

Run Command status

Run Command indica dettagli di stato per tre aree: plugin, invocazioni e stato generale dei comandi. Un plugin è un blocco di esecuzione di codice definito nel documento del comando. Per ulteriori informazioni sui plugin, consulta [Documentazione di riferimento del plugin per i documenti di comando](#).

Quando si invia un comando a più nodi gestiti contemporaneamente, ogni copia del documento destinata a ogni nodo è denominata invocazione di comando. Ad esempio, se usi il documento `AWS-RunShellScript` e invii un comando `ifconfig` a 20 istanze, quel comando ha 20 invocazioni. Ogni invocazione di comando segnala lo stato individualmente. Anche i plugin per una determinata invocazione di comando segnalano lo stato individualmente.

Infine, Run Command include uno stato di comando aggregato per tutti i plugin e le invocazioni. Lo stato di comando aggregato può essere diverso rispetto allo stato segnalato dai plugin o dalle invocazioni, come mostrato nelle tabelle seguenti.

Note

Se si eseguono comandi su un numero elevato di nodi gestiti utilizzando i parametri `max-concurrency` o `max-errors`, lo stato dei comandi riflette le limitazioni imposte da quei parametri, come descritto nelle tabelle seguenti. Per ulteriori informazioni su questi parametri, consultare [Esecuzione di comandi su vasta scala](#).

Stato dettagliato per i plugin e le invocazioni dei comandi

Stato	Informazioni
Pending (In attesa)	Il comando non è stato ancora inviato al nodo gestito o non è stato ricevuto da SSM Agent. Se il comando non viene ricevuto dall'agente prima che passi il tempo che è uguale alla somma di <code>Timeout</code> (secondi) e il parametro <code>Execution timeout</code> (Timeout di esecuzione) Parametro, lo stato cambia in <code>Delivery Timed Out</code> .

Stato	Informazioni
InProgress	Systems Manager sta tentando di inviare il comando al nodo gestito oppure il comando è stato ricevuto da SSM Agent e ha iniziato a funzionare sull'istanza. A seconda del risultato di tutti i plugin dei comandi, lo stato passerà a Success, Failed, Delivery Timed Out o Execution Timed Out. Eccezione: se l'agente non è in esecuzione o è disponibile nel nodo, lo stato del comando rimane in In Progress finché l'agente non è nuovamente disponibile o fino al raggiungimento del limite di timeout di esecuzione. Lo stato passerà quindi a uno stato terminale.
Ritardato	Il sistema ha tentato di inviare il comando al nodo gestito, ma non è riuscito. Il sistema riprova.

Stato	Informazioni
Completato	<p>Questo stato viene restituito in diverse condizioni. Questo stato non significa che il comando è stato elaborato correttamente sul nodo. Ad esempio, il comando può essere ricevuto dal SSM Agent nodo gestito e restituire un codice di uscita pari a zero perché <code>PowerShell ExecutionPolicy</code> impedito l'esecuzione del comando. Si tratta di uno stato terminale. Le condizioni che determinano la restituzione di uno stato <code>Success</code> da un comando sono:</p> <ul style="list-style-type: none">• Quando si utilizza come destinazione un'istanza, il comando è stato ricevuto da SSM Agent sul nodo gestito e ha restituito un codice di uscita zero.• Quando si utilizzano come destinazione più istanze, il numero di invocazioni non riuscite non ha superato la soglia di errore specificata nel comando.• Quando si utilizzano come destinazione più istanze, almeno un'invocazione è riuscita mentre le altre sono scadute. La soglia di errore specificata è ancora valida.• Quando si utilizza come destinazione un tag, non viene trovata alcuna istanza associata al tag.• Quando si sceglie come destinazione un tag, il numero di invocazioni fallite non ha superato la soglia di errore specificata nel comando.• Quando si utilizza come destinazione un tag, almeno un'invocazione è riuscita mentre

Stato	Informazioni
	<p>le altre sono scadute. La soglia di errore specificata è ancora valida.</p> <ul style="list-style-type: none"> Esistono applicazioni o policy applicate a livello di sistema operativo che impediscono o sovrascrivono l'esecuzione di un comando con conseguente restituzione di un codice di uscita pari a zero. <div data-bbox="829 615 1507 1167"> <p> Note</p> <p>Le stesse condizioni si applicano quando si sceglie come destinazione i gruppi di risorse. Per risolvere gli errori o ottenere ulteriori informazioni sull'esecuzione del comando, invia un comando che gestisce gli errori o le eccezioni restituendo codici di uscita appropriati (codici di uscita diversi da zero in caso di errore del comando).</p> </div>
DeliveryTimedOut	<p>Il comando non è stato recapitato al nodo gestito prima della scadenza del timeout complessivo. I timeout complessivi non vengono conteggiati per il limite <code>max-errors</code> del comando padre, ma sono rilevanti per la definizione dello stato del comando come <code>Success</code>, <code>Incomplete</code> o <code>Delivery Timed Out</code>. Si tratta di uno stato terminale.</p>

Stato	Informazioni
ExecutionTimedOut	L'esecuzione del comando è iniziata sul nodo gestito, ma non è stata completata prima della scadenza. I timeout di esecuzione contano come un errore che invierà una risposta diversa da zero e Systems Manager interromperà il tentativo di esecuzione dell'automazione dei comandi, segnalando lo stato di errore.
Non riuscito	Il comando non è riuscito sul nodo gestito. Per un plugin, questo indica che il codice del risultato non era zero. Per un'invocazione del comando, questo indica che il codice del risultato per uno o più plugin non era zero. Le invocazioni non riuscite vengono conteggiate per il limite <code>max-errors</code> del comando padre. Si tratta di uno stato terminale.
Annullato	Il comando è stato terminato prima del completamento. Si tratta di uno stato terminale.
Non consegnabile	Il comando non può essere recapitato al nodo gestito. Il nodo potrebbe non esistere o non rispondere. Le invocazioni non consegnabili non vengono conteggiate per il limite <code>max-errors</code> del comando padre e non sono rilevanti per la definizione dello stato del comando come <code>Success</code> o <code>Incomplete</code> . Ad esempio, se tutte le invocazioni in un comando dispongono dello stato <code>Undeliverable</code> , lo stato del comando restituito è <code>Failed</code> . Tuttavia, se un comando dispone di cinque chiamate, quattro delle quali restituiscono lo stato <code>Undeliverable</code> e una restituisce lo stato <code>Success</code> , lo stato del comando padre è <code>Success</code> . Si tratta di uno stato terminale.

Stato	Informazioni
Terminato	Il comando padre ha superato il limite <code>max-errors</code> e le successive invocazioni del comando sono state annullate dal sistema. Si tratta di uno stato terminale.
InvalidPlatform	<p>Il comando è stato inviato a un nodo gestito che non corrisponde alle piattaforme richieste specificate dal documento scelto. <code>InvalidPlatform</code> non viene conteggiato per il limite massimo di errori del comando padre, ma contribuisce a determinare lo stato del comando come <code>Successo</code> o <code>Failed</code>. Ad esempio, se tutte le invocazioni in un comando dispongono dello stato <code>InvalidPlatform</code>, lo stato del comando restituito è <code>Failed</code>. Tuttavia, se un comando dispone di cinque chiamate, quattro delle quali restituiscono lo stato <code>InvalidPlatform</code> e una restituisce lo stato <code>Success</code>, lo stato del comando padre è <code>Success</code>. Si tratta di uno stato terminale.</p>

Stato	Informazioni
AccessDenied	L'utente o il ruolo AWS Identity and Access Management (IAM) che avvia il comando non ha accesso al nodo gestito di destinazione. <code>Access Denied</code> non viene conteggiato nel <code>max-errors</code> limite del comando principale, ma contribuisce a determinare se lo stato del comando principale è <code>Success</code> o <code>Failed</code> . Ad esempio, se tutte le invocazioni in un comando dispongono dello stato <code>Access Denied</code> , lo stato del comando restituito è <code>Failed</code> . Tuttavia, se un comando dispone di cinque chiamate, quattro delle quali restituiscono lo stato <code>Access Denied</code> e una restituisce lo stato <code>Success</code> , lo stato del comando padre è <code>Success</code> . Si tratta di uno stato terminale.

Stato dettagliato per un comando

Stato	Informazioni
Pending (In attesa)	Il comando non è ancora stato ricevuto da un agente su qualsiasi nodo gestito.
InProgress	Il comando è stato inviato ad almeno un'istanza, ma non ha raggiunto lo stato finale su ogni nodo gestito.
Ritardato	Il sistema ha tentato di inviare il comando al nodo, ma non è riuscito. Il sistema riprova.
Completato	Il comando è stato ricevuto da SSM Agent su tutti i nodi gestiti specificati o destinazione e ha restituito un codice di uscita zero. Tutte le invocazioni di comando hanno raggiunto uno stato terminale e non è stato raggiunto il valore

Stato	Informazioni
	<p><code>max-errors</code> . Questo stato non significa che il comando è stato elaborato correttamente su tutti i nodi gestiti specificati o destinazione. Si tratta di uno stato terminale.</p> <div data-bbox="829 430 1507 888"> <p> Note</p> <p>Per risolvere gli errori o ottenere ulteriori informazioni sull'esecuzione del comando, invia un comando che gestisce gli errori o le eccezioni restituendo codici di uscita appropriati (codici di uscita diversi da zero in caso di errore del comando).</p> </div>
DeliveryTimedOut	<p>Il comando non è stato recapitato al nodo gestito prima della scadenza del timeout complessivo. I valore di <code>max-errors</code> o altre invocazioni del comando mostra lo stato <code>Delivery Timed Out</code>. Si tratta di uno stato terminale.</p>
Non riuscito	<p>Il comando non è riuscito sul nodo gestito. I valore di <code>max-errors</code> o altre invocazioni del comando mostra lo stato <code>Failed</code>. Si tratta di uno stato terminale.</p>
Incomplete (Incompleto)	<p>Il comando è stato tentato su tutti i nodi gestiti e una o più invocazioni non hanno il valore <code>Success</code>. Il numero delle invocazioni non riuscite, però, non è sufficiente perché lo stato sia <code>Failed</code>. Si tratta di uno stato terminale.</p>
Annullato	<p>Il comando è stato terminato prima del completamento. Si tratta di uno stato terminale.</p>

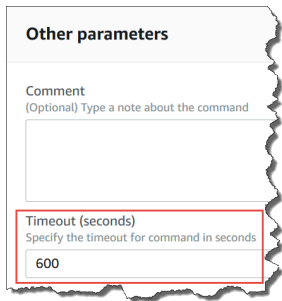
Stato	Informazioni
RateExceeded	Il numero di nodi gestiti definiti come target dal comando ha superato la quota dell'account per le invocazioni in attesa. Il sistema ha annullato il comando prima di eseguirlo su qualsiasi nodo. Si tratta di uno stato terminale.
AccessDenied	L'utente o il ruolo che avvia il comando non dispone dell'accesso al gruppo di risorse target. <code>AccessDenied</code> non viene conteggiato ai fini del limite di <code>max-errors</code> del comando padre, ma contribuisce a stabilire se lo stato del comando padre è <code>Success</code> o <code>Failed</code> . Ad esempio, se tutte le invocazioni in un comando dispongono dello stato <code>AccessDenied</code> , lo stato del comando restituito è <code>Failed</code> . Tuttavia, se un comando dispone di 5 invocazioni, 4 delle quali restituiscono lo stato <code>AccessDenied</code> e 1 dei quali restituisce lo stato <code>Success</code> , lo stato del comando genitore è <code>Success</code> .) Si tratta di uno stato terminale.
Nessuna istanza nel tag	Il valore del tag chiave-coppia o il gruppo di risorse cui fa riferimento il comando non corrisponde ad alcun nodo gestito. Si tratta di uno stato terminale.

Informazioni sui valori di timeout dei comandi

Systems Manager applica i seguenti valori di timeout durante l'esecuzione dei comandi.

Timeout totale

Nella console Systems Manager, specifica il valore di timeout nel campo Timeout (secondi). Dopo l'invio di un comando, Run Command controlla se il comando è scaduto o meno. Se un comando raggiunge il limite di scadenza del comando (timeout totale), lo stato viene modificato in `DeliveryTimedOut` per tutte le chiamate che hanno lo stato `InProgress`, `Pending` o `Delayed`.



Other parameters

Comment
(Optional) Type a note about the command

Timeout (seconds)
Specify the timeout for command in seconds

600

A livello più tecnico, il timeout complessivo, ossia Timeout (secondi), è una combinazione di due valori di timeout, come illustrato di seguito:

Total timeout = "Timeout(seconds)" from the console + "timeoutSeconds":
"{{ executionTimeout }}" from your SSM document

Ad esempio, il valore predefinito di Timeout (secondi) Nella console Systems Manager è di 600 secondi. Se si esegue un comando utilizzando il comando AWS-RunShellScript SSM, il valore predefinito di "timeoutSeconds": "{{ executionTimeout }}" è di 3.600 secondi, come mostrato nell'esempio del documento seguente:

```
"executionTimeout": {
  "type": "String",
  "default": "3600",

  "runtimeConfig": {
    "aws:runShellScript": {
      "properties": [
        {
          "timeoutSeconds": "{{ executionTimeout }}"
```

Ciò significa che il comando viene eseguito per 4.200 secondi (70 minuti) prima che il sistema imposti lo stato del comando su DeliveryTimedOut.

Timeout di esecuzione

Nella console Systems Manager specificare il valore di timeout di esecuzione nel campo Timeout di esecuzione, se disponibile. Non tutti i documenti SSM richiedono di specificare un timeout di esecuzione. Il campo Timeout di esecuzione viene visualizzato solo quando un parametro di input corrispondente è stato definito nel documento SSM. Se specificato, il comando deve essere completato entro questo periodo di tempo.

Note

Run Command si basa sulla risposta del SSM Agent document terminal per determinare se il comando è stato consegnato all'agente. SSM Agent deve inviare un `ExecutionTimedOut` segnale affinché una chiamata o un comando siano contrassegnati come `ExecutionTimedOut`.



Timeout di esecuzione predefinito

Se un documento SSM non richiede di specificare esplicitamente un valore di timeout di esecuzione, Systems Manager applica il timeout di esecuzione predefinito hard-coded.

Come Systems Manager segnala i timeout

Se Systems Manager riceve una risposta `execution timeout` da SSM Agent su una destinazione, Systems Manager contrassegna la chiamata del comando come `executionTimeout`.

Se Run Command non riceve una risposta terminale di documenti da SSM Agent, l'invocazione del comando è contrassegnata come `deliveryTimeout`.

Per determinare lo stato di timeout su una destinazione, SSM Agent combina tutti i parametri e il contenuto del documento SSM da calcolare per `executionTimeout`. Quando SSM Agent determina che un comando è scaduto, invia `executionTimeout` al servizio.

Il valore predefinito per Timeout (secondi) è 3.600 secondi. Il valore predefinito per Timeout di esecuzione è anche 3.600 secondi. Pertanto, il timeout predefinito totale per un comando è 7200 secondi.

Note

SSM Agent elabora `executionTimeout` in modo diverso a seconda del tipo di documento SSM e della versione del documento.

Run Command Spiegazioni passo per passo di

Le procedure dettagliate di questa sezione mostrano come eseguire comandi con Run Command uno strumento in AWS Systems Manager AWS Command Line Interface (AWS CLI) o. AWS Tools for Windows PowerShell

Indice

- [Aggiornamento del software utilizzando Run Command](#)
- [Procedura dettagliata: usa il AWS CLI con Run Command](#)
- [Procedura dettagliata: usa il AWS Tools for Windows PowerShell con Run Command](#)

I comandi di esempio sono disponibili anche nei seguenti riferimenti.

- [Guida di riferimento al AWS CLI di Systems Manager](#)
- [AWS Tools for Windows PowerShell - AWS Systems Manager](#)

Aggiornamento del software utilizzando Run Command

Le procedure seguenti descrivono come aggiornare il software nei nodi gestiti.

Aggiornamento di SSM Agent utilizzando Run Command

La procedura seguente descrive come aggiornare rapidamente SSM Agent in esecuzione sui tuoi nodi gestiti. È possibile eseguire l'aggiornamento alla versione più recente di SSM Agent o il downgrade a una versione precedente. Quando si esegue il comando, il sistema scarica la versione da AWS, la installa e quindi disinstalla la versione esistente prima dell'esecuzione del comando. Se si verifica un errore durante il processo, il sistema torna alla versione presente sul server prima dell'esecuzione di questo comando e lo stato del comando indica che il comando non è riuscito.

Note

Se un'istanza sta eseguendo la versione 13.0 (Ventura) o successiva di macOS, l'istanza deve avere la versione SSM Agent 3.1.941.0 o successiva per eseguire il documento AWS-UpdateSSMAgent. Se l'istanza esegue una versione di SSM Agent precedente alla 3.1.941.0, è possibile aggiornare il tuo SSM Agent per eseguire il documento AWS-UpdateSSMAgent eseguendo i comandi `brew update` e `brew upgrade amazon-ssm-agent`.

Per ricevere notifiche sugli aggiornamenti dell'SSM Agent, iscriviti alla pagina [Note di rilascio dell'SSM Agent](#) su GitHub.

Per aggiornare SSM Agent utilizzando Run Command

1. Apri la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Run Command.
3. Seleziona Esegui comando.
4. Nell'elenco Command document (Documento comando) scegliere **AWS-UpdateSSMAgent**.
5. Nella sezione Command parameters (Parametri comando) specificare i valori per i parametri seguenti, se necessario:
 - a. (Facoltativo) Per Versione, digita la versione di SSM Agent da installare. È possibile installare [versioni precedenti](#) dell'agente. Se non si specifica una versione, viene installata quella più recente.
 - b. (Facoltativo) Per Consenti downgrade, scegli true per installare una versione precedente di SSM Agent. Se si seleziona questa opzione, è necessario specificare il numero della versione [precedente](#). Scegliere false per installare solo la versione più recente del servizio.
6. In Targets (Destinazioni), scegliere i nodi gestiti in cui si desidera eseguire questa operazione specificando i tag, selezionando le istanze o i dispositivi edge manualmente o indicando un gruppo di risorse.

 Tip

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

7. In Altri parametri:
 - In Commento, digita le informazioni su questo comando.
 - In Timeout (secondi), specifica il numero di secondi che il sistema dovrà attendere prima di generare un errore per l'intera esecuzione del comando.
8. Per Controllo velocità:

- In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti come target, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.
9. (Facoltativo) Nella sezione Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Scrivi l'output del comando in un bucket S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

 Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

10. Se vuoi che vengano inviate notifiche sullo stato dell'esecuzione del comando, nella sezione Notifiche SNS selezionare la casella di controllo Abilita notifiche SNS.

Per ulteriori informazioni sulla configurazione delle notifiche Amazon SNS per Run Command, consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

11. Scegli Esegui.

Aggiornamento tramite PowerShell Run Command

La procedura seguente descrive come eseguire l'aggiornamento PowerShell alla versione 5.1 sui nodi gestiti Windows Server 2012 e 2012 R2. Lo script fornito in questa procedura scarica l'aggiornamento 5.1 di Windows Management Framework (WMF) e avvia l'installazione dell'aggiornamento. Il nodo si riavvia durante questo processo perché questo è necessario durante l'installazione di WMF 5.1. Il download e l'installazione dell'aggiornamento richiedono circa cinque minuti.

Per eseguire l'aggiornamento utilizzando PowerShell Run Command

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Run Command.
3. Seleziona Esegui comando.
4. Nell'elenco Command document (Documento comando) scegliere **AWS-RunPowerShellScript**.
5. Nella Comandi Incollare i comandi seguenti per il sistema operativo in uso.

Windows Server 2012 R2

```
Set-Location -Path "C:\Windows\Temp"

Invoke-WebRequest "https://go.microsoft.com/fwlink/?linkid=839516" -OutFile
"Win8.1AndW2K12R2-KB3191564-x64.msu"

Start-Process -FilePath "$env:systemroot\system32\wusa.exe" -Verb RunAs -
ArgumentList ('Win8.1AndW2K12R2-KB3191564-x64.msu', '/quiet')
```

Windows Server 2012

```
Set-Location -Path "C:\Windows\Temp"

Invoke-WebRequest "https://go.microsoft.com/fwlink/?linkid=839513" -OutFile
"W2K12-KB3191565-x64.msu"

Start-Process -FilePath "$env:systemroot\system32\wusa.exe" -Verb RunAs -
ArgumentList ('W2K12-KB3191565-x64.msu', '/quiet')
```

6. In **Targets (Destinazioni)**, scegliere i nodi gestiti in cui si desidera eseguire questa operazione specificando i tag, selezionando le istanze o i dispositivi edge manualmente o indicando un gruppo di risorse.

 Tip

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

7. In **Altri parametri**:

- In **Commento**, digita le informazioni su questo comando.
- In **Timeout (secondi)**, specifica il numero di secondi che il sistema dovrà attendere prima di generare un errore per l'intera esecuzione del comando.

8. Per **Controllo velocità**:

- In **Simultaneità**, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti come target, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.
9. (Facoltativo) Nella sezione **Opzioni di output**, per salvare l'output del comando in un file, seleziona la casella **Scrivi l'output del comando in un bucket S3**. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

 Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

10. Se vuoi che vengano inviate notifiche sullo stato dell'esecuzione del comando, nella sezione Notifiche SNS selezionare la casella di controllo Abilita notifiche SNS.

Per ulteriori informazioni sulla configurazione delle notifiche Amazon SNS per Run Command, consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

11. Scegli Esegui.

Dopo il riavvio del nodo gestito e il completamento dell'installazione dell'aggiornamento, connettiti al nodo per confermare che l'aggiornamento alla versione 5.1 di PowerShell è stato eseguito correttamente. Per verificare la versione di PowerShell sul tuo nodo, apri PowerShell e accedi. `$PSVersionTable` Il valore `PSVersion` nella tabella di output mostra 5.1, se l'aggiornamento è riuscito.

Se il valore di `PSVersion` è diverso da 5.1, ad esempio 3.0 o 4.0, rivedi i log di configurazione nel Visualizzatore eventi in Log di Windows. Questi log indicano perché l'installazione dell'aggiornamento non è riuscita.

Procedura dettagliata: usa il AWS CLI con Run Command

La seguente procedura dettagliata di esempio mostra come utilizzare AWS Command Line Interface (AWS CLI) per visualizzare informazioni su comandi e parametri di comando, come eseguire comandi e come visualizzare lo stato di tali comandi.

⚠ Important

Solo gli amministratori attendibili devono essere autorizzati a utilizzare i documenti AWS Systems Manager preconfigurati mostrati in questo argomento. I comandi o gli script specificati nei documenti Systems Manager vengono eseguiti con privilegi amministrativi sui nodi gestiti. Se un utente è autorizzato a eseguire uno dei documenti Systems Manager predefiniti (qualsiasi documento che inizia con AWS-), lo stesso utente avrà anche accesso al nodo come amministratore. Per tutti gli altri utenti, è consigliabile creare documenti restrittivi e condividerli con utenti specifici.

Fase 1. Nozioni di base

Devi disporre dei privilegi di amministratore sui nodi gestiti da configurare oppure delle autorizzazioni appropriate in AWS Identity and Access Management (IAM). Nota inoltre che questo esempio utilizza la regione Stati Uniti orientali (Ohio) (us-east-2). Run Command è disponibile negli endpoint del servizio Regioni AWS elencati in [Systems Manager nella](#). Riferimenti generali di Amazon Web Services Per ulteriori informazioni, consulta [Configurazione dei nodi gestiti per AWS Systems Manager](#).

Per eseguire comandi utilizzando il AWS CLI

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Creare un elenco di tutti i documenti disponibili

Questo comando elenca tutti i documenti disponibili per il tuo account in base alle (IAM) autorizzazioni.

```
aws ssm list-documents
```

3. Verificare che un nodo gestito sia pronto a ricevere comandi

L'output del comando seguente mostra se i nodi gestiti sono online.

Linux & macOS

```
aws ssm describe-instance-information \
```

```
--output text --query "InstanceInformationList[*]"
```

Windows

```
aws ssm describe-instance-information ^  
--output text --query "InstanceInformationList[*]"
```

4. Utilizzare il comando seguente per visualizzare i dettagli su uno determinato nodo gestito.

Note

Per eseguire i comandi in questa procedura guidata, è necessario sostituire gli ID delle istanze e dei comandi. Per i dispositivi AWS IoT Greengrass core gestiti, usa l'ID *mi-ID_number* for instance. L'ID comando viene restituito come risposta a send-command. Gli ID di istanza sono disponibili presso Fleet Manager.

Linux & macOS

```
aws ssm describe-instance-information \  
--instance-information-filter-list key=InstanceIds,valueSet=instance-ID
```

Windows

```
aws ssm describe-instance-information ^  
--instance-information-filter-list key=InstanceIds,valueSet=instance-ID
```

Fase 2: esecuzione di script di shell per visualizzare i dettagli delle risorse

Se utilizzi Run Command e il documento AWS-RunShellScript, puoi eseguire qualsiasi comando o script su un nodo gestito come se fossi connesso localmente.

Visualizzare la descrizione e i parametri disponibili

Usa il comando seguente per visualizzare una descrizione del documento JSON .

Linux & macOS

```
aws ssm describe-document \  

```



```
--name "AWS-RunShellScript" \  
--query "[Document.Name,Document.Description]"
```

Windows

```
aws ssm describe-document ^  
--name "AWS-RunShellScript" ^  
--query "[Document.Name,Document.Description]"
```

Usa il comando seguente per visualizzare i parametri disponibili e i dettagli su tali parametri.

Linux & macOS

```
aws ssm describe-document \  
--name "AWS-RunShellScript" \  
--query "Document.Parameters[*]"
```

Windows

```
aws ssm describe-document ^  
--name "AWS-RunShellScript" ^  
--query "Document.Parameters[*]"
```

Fase 3: invio di comandi semplici utilizzando il documento **AWS-RunShellScript**

Usa il comando seguente per ottenere le informazioni IP per un nodo gestito.

Se prendi come target un nodo gestito Windows Server, cambia il document-name a AWS-RunPowerShellScript e cambia il command da ifconfig a ipconfig.

Linux & macOS

```
aws ssm send-command \  
--instance-ids "instance-ID" \  
--document-name "AWS-RunShellScript" \  
--comment "IP config" \  
--parameters commands=ifconfig \  
--output text
```

Windows

```
aws ssm send-command ^
  --instance-ids "instance-ID" ^
  --document-name "AWS-RunShellScript" ^
  --comment "IP config" ^
  --parameters commands=ifconfig ^
  --output text
```

Ottenere informazioni sul comando con i dati di risposta

Il comando seguente usa l'ID comando restituito dal comando precedente per ottenere i dettagli e i dati di risposta dell'esecuzione del comando. Il sistema restituisce i dati di risposta se il comando è stato completato. Se l'esecuzione del comando mostra "Pending" o "InProgress", esegui di nuovo il comando per visualizzare i dati di risposta.

Linux & macOS

```
aws ssm list-command-invocations \
  --command-id $sh-command-id \
  --details
```

Windows

```
aws ssm list-command-invocations ^
  --command-id $sh-command-id ^
  --details
```

Identificazione dell'utente

Il comando seguente mostra l'utente predefinito che esegue i comandi.

Linux & macOS

```
sh_command_id=$(aws ssm send-command \
  --instance-ids "instance-ID" \
  --document-name "AWS-RunShellScript" \
  --comment "Demo run shell script on Linux managed node" \
  --parameters commands=whoami \
  --output text \
```

```
--query "Command.CommandId")
```

Ottenere lo stato del comando

Il comando seguente usa l'ID comando per ottenere lo stato di esecuzione del comando sul nodo gestito. Questo esempio usa l'ID di comando restituito nel comando precedente.

Linux & macOS

```
aws ssm list-commands \  
  --command-id "command-ID"
```

Windows

```
aws ssm list-commands ^  
  --command-id "command-ID"
```

Ottenere i dettagli del comando

Il comando seguente usa l'ID comando del comando precedente per ottenere lo stato di esecuzione del comando per singoli nodo gestito.

Linux & macOS

```
aws ssm list-command-invocations \  
  --command-id "command-ID" \  
  --details
```

Windows

```
aws ssm list-command-invocations ^  
  --command-id "command-ID" ^  
  --details
```

Ottenere informazioni sul comando con i dati di risposta per un nodo gestito specifico

Il comando seguente restituisce l'output della richiesta `aws ssm send-command` originale per un nodo gestito specifico.

Linux & macOS

```
aws ssm list-command-invocations \  
  --instance-id instance-ID \  
  --command-id "command-ID" \  
  --details
```

Windows

```
aws ssm list-command-invocations ^  
  --instance-id instance-ID ^  
  --command-id "command-ID" ^  
  --details
```

Visualizzare la versione Python

Il comando seguente restituisce la versione di Python in esecuzione su un nodo.

Linux & macOS

```
sh_command_id=$(aws ssm send-command \  
  --instance-ids "instance-ID" \  
  --document-name "AWS-RunShellScript" \  
  --comment "Demo run shell script on Linux Instances" \  
  --parameters commands='python -V' \  
  --output text --query "Command.CommandId") \  
sh -c 'aws ssm list-command-invocations \  
  --command-id "$sh_command_id" \  
  --details \  
  --query "CommandInvocations[].CommandPlugins[].{Status:Status,Output:Output}"'
```

Fase 4: Esegui un semplice script Python usando Run Command

Il seguente comando esegue un semplice script Python "Hello World" utilizzando Run Command.

Linux & macOS

```
sh_command_id=$(aws ssm send-command \  
  --instance-ids "instance-ID" \  
  --document-name "AWS-RunShellScript" \  
  --parameters commands='python -V'
```

```
--comment "Demo run shell script on Linux Instances" \
--parameters '{"commands":["#!/usr/bin/python","print \"Hello World from python
\\\"\"']}' \
--output text \
--query "Command.CommandId") \
sh -c 'aws ssm list-command-invocations \
--command-id "$sh_command_id" \
--details \
--query "CommandInvocations[].CommandPlugins[].{Status:Status,Output:Output}"'
```

Passo 5: Esegui uno script Bash usando Run Command

Gli esempi in questa sezione mostrano come eseguire il seguente script bash usando Run Command.

Per esempi di utilizzo di Run Command per eseguire script archiviati in posizioni remote, vedere [Esecuzione di script da Amazon S3](#) e [Esecuzione di script da GitHub](#).

```
#!/bin/bash
yum -y update
yum install -y ruby
cd /home/ec2-user
curl -O https://aws-codedeploy-us-east-2.s3.amazonaws.com/latest/install
chmod +x ./install
./install auto
```

Questo script installa l' AWS CodeDeploy agente sulle istanze Amazon Linux e Red Hat Enterprise Linux (RHEL), come descritto in [Creare un'istanza Amazon EC2 per CodeDeploy](#) nella Guida per l'utente. AWS CodeDeploy

Lo script installa l' CodeDeploy agente da un bucket S3 AWS gestito nella regione Stati Uniti orientali (Ohio) (us-east-2),. aws-codedeploy-us-east-2

Esegui uno script bash in un comando AWS CLI

Nell'esempio seguente viene illustrato come includere lo script bash in un comando CLI utilizzando l'opzione `--parameters`.

Linux & macOS

```
aws ssm send-command \
--document-name "AWS-RunShellScript" \
```

```
--targets ' [{"Key": "InstanceIds", "Values": ["instance-id"]} ]' \
--parameters '{"commands": ["#!/bin/bash", "yum -y update", "yum
install -y ruby", "cd /home/ec2-user", "curl -O https://aws-codedeploy-us-
east-2.s3.amazonaws.com/latest/install", "chmod +x ./install", "./install auto"]}'
```

Esegui uno script bash in un file JSON

Nell'esempio seguente, il contenuto dello script bash viene archiviato in un file JSON e il file viene incluso nel comando usando l'`--cli-input-json` opzione.

Linux & macOS

```
aws ssm send-command \
--document-name "AWS-RunShellScript" \
--targets "Key=InstanceIds,Values=instance-id" \
--cli-input-json file://installCodeDeployAgent.json
```

Windows

```
aws ssm send-command ^
--document-name "AWS-RunShellScript" ^
--targets "Key=InstanceIds,Values=instance-id" ^
--cli-input-json file://installCodeDeployAgent.json
```

Il comando `installCodeDeployAgent.json` che fa riferimento al file JSON viene visualizzato nell'esempio seguente.

```
{
  "Parameters": {
    "commands": [
      "#!/bin/bash",
      "yum -y update",
      "yum install -y ruby",
      "cd /home/ec2-user",
      "curl -O https://aws-codedeploy-us-east-2.s3.amazonaws.com/latest/install",
      "chmod +x ./install",
      "./install auto"
    ]
  }
}
```

Procedura dettagliata: usa il AWS Tools for Windows PowerShell con Run Command

Gli esempi seguenti mostrano come utilizzare il AWS Tools for Windows PowerShell per visualizzare informazioni sui comandi e sui parametri dei comandi, come eseguire i comandi e come visualizzare lo stato di tali comandi. Questa procedura guidata include un esempio per ognuno dei documenti AWS Systems Manager predefiniti.

Important

Solo gli amministratori fidati dovrebbero essere autorizzati a usare i documenti Systems Manager preconfigurati mostrati in questo argomento. I comandi o gli script specificati nei documenti Systems Manager vengono eseguiti con privilegi amministrativi sui nodi gestiti. Se un utente dispone dell'autorizzazione per eseguire uno qualsiasi dei documenti di Systems Manager predefiniti (qualsiasi documento che inizia con AWS), tale utente dispone anche dell'accesso come amministratore al nodo. Per tutti gli altri utenti, è consigliabile creare documenti restrittivi e condividerli con utenti specifici.

Configura AWS Tools for Windows PowerShell impostazioni della sessione

Specificare le credenziali

Apri **Strumenti per Windows PowerShell** sul tuo computer locale ed esegui il comando seguente per specificare le tue credenziali. È necessario disporre delle autorizzazioni di amministratore sui nodi gestiti che si desidera configurare oppure è necessario disporre dell'autorizzazione appropriata in AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta [Configurazione dei nodi gestiti per AWS Systems Manager](#).

```
Set-AWSCredentials -AccessKey key-name -SecretKey key-name
```

Imposta un valore predefinito Regione AWS

Esegui il comando seguente per impostare la regione per la tua PowerShell sessione. L'esempio utilizza la regione Stati Uniti orientali (Ohio) (us-east-2). Run Command è disponibile negli endpoint del servizio Regioni AWS elencati in [Systems Manager nella](#). Riferimenti generali di Amazon Web Services

```
Set-DefaultAWSRegion `
    -Region us-east-2
```

Creare un elenco di tutti i documenti disponibili

Questo comando elenca tutti i documenti disponibili per il tuo account:

```
Get-SSMDocumentList
```

Esegui PowerShell comandi o script

Se utilizzi Run Command e il documento **AWS-RunPowerShell**, è possibile eseguire qualsiasi comando o script su un nodo gestito come se fossi connesso localmente. È possibile inviare comandi o digitare il percorso di uno script locale per eseguire il comando.

Note

Per ulteriori informazioni sul riavvio dei nodi gestiti quando usi Run Command per chiamare gli script, consulta [Gestione di riavvii durante l'esecuzione dei comandi](#).

Visualizzare la descrizione e i parametri disponibili

```
Get-SSMDocumentDescription `
    -Name "AWS-RunPowerShellScript"
```

Visualizzare ulteriori informazioni sui parametri

```
Get-SSMDocumentDescription `
    -Name "AWS-RunPowerShellScript" | Select -ExpandProperty Parameters
```

Inviare comandi utilizzando il documento **AWS-RunPowerShellScript**

Il comando seguente mostra il contenuto della directory "C:\Users" e il contenuto della directory "C:\" su due nodi gestiti.

```
$runPSCommand = Send-SSMCommand `
    -InstanceIds @("instance-ID-1", "instance-ID-2") `
    -DocumentName "AWS-RunPowerShellScript" `
    -Comment "Demo AWS-RunPowerShellScript with two instances" `
    -Parameter @{ 'commands'=@('dir C:\Users', 'dir C:\')}
```

Ottenere i dettagli della richiesta del comando

Il comando seguente usa `CommandId` per ottenere lo stato di esecuzione del comando su entrambi i nodi gestiti. Questo esempio usa `CommandId` restituito nel comando precedente.

```
Get-SSMCommand `
  -CommandId $runPSCCommand.CommandId
```

Lo stato del comando in questo esempio può essere `Riuscito`, `In sospeso` o `InProgress`.

Ottenere informazioni sul comando per nodo gestito

Il comando seguente usa `CommandId` del comando precedente per ottenere lo stato di esecuzione del comando per singoli nodi gestiti.

```
Get-SSMCommandInvocation `
  -CommandId $runPSCCommand.CommandId
```

Ottenere informazioni sul comando con i dati di risposta per un nodo gestito specifico

Il comando seguente restituisce l'output del comando `Send-SSMCommand` originale per un nodo gestito specifico.

```
Get-SSMCommandInvocation `
  -CommandId $runPSCCommand.CommandId `
  -Details $true `
  -InstanceId instance-ID | Select -ExpandProperty CommandPlugins
```

Annullare un comando

Il comando seguente annulla `Send-SSMCommand` per il documento `AWS-RunPowerShellScript`.

```
$cancelCommand = Send-SSMCommand `
  -InstanceIds @("instance-ID-1", "instance-ID-2") `
  -DocumentName "AWS-RunPowerShellScript" `
  -Comment "Demo AWS-RunPowerShellScript with two instances" `
  -Parameter @{'commands'='Start-Sleep -Seconds 120; dir C:\'}

Stop-SSMCommand -CommandId $cancelCommand.CommandId
```

Controllare lo stato del comando

Il comando seguente controlla lo stato del comando `Cancel`.

```
Get-SSMCommand `
    -CommandId $cancelCommand.CommandId
```

Installare un'applicazione usando **AWS-InstallApplication** documento

Utilizzando Run Command e il documento AWS-InstallApplication, è possibile installare, riparare o disinstallare applicazioni su nodi gestiti. Il comando richiede il percorso o l'indirizzo di un file MSI.

Note

Per ulteriori informazioni sul riavvio dei nodi gestiti quando usi Run Command per chiamare gli script, consulta [Gestione di riavvii durante l'esecuzione dei comandi](#).

Visualizzare la descrizione e i parametri disponibili

```
Get-SSMDocumentDescription `
    -Name "AWS-InstallApplication"
```

Visualizzare ulteriori informazioni sui parametri

```
Get-SSMDocumentDescription `
    -Name "AWS-InstallApplication" | Select -ExpandProperty Parameters
```

Inviare comandi utilizzando il documento **AWS-InstallApplication**

Il comando seguente installa una versione di Python nel nodo gestito in modalità automatica e registra l'output in un file di testo locale nell'unità C :.

```
$installAppCommand = Send-SSMCommand `
    -InstanceId instance-ID `
    -DocumentName "AWS-InstallApplication" `
    -Parameter @{ 'source'='https://www.python.org/ftp/python/2.7.9/python-2.7.9.msi';
    'parameters'='/norestart /quiet /log c:\pythoninstall.txt' }
```

Ottenere informazioni sul comando per nodo gestito

Il comando seguente usa CommandId per ottenere lo stato di esecuzione del comando.

```
Get-SSMCommandInvocation `
  -CommandId $installAppCommand.CommandId `
  -Details $true
```

Ottenere informazioni sul comando con i dati di risposta per un nodo gestito specifico

Il comando seguente restituisce i risultati dell'installazione di Python.

```
Get-SSMCommandInvocation `
  -CommandId $installAppCommand.CommandId `
  -Details $true `
  -InstanceId instance-ID | Select -ExpandProperty CommandPlugins
```

Installa un PowerShell modulo utilizzando il documento **AWS-InstallPowerShellModule** JSON

È possibile utilizzarlo Run Command per installare PowerShell moduli su nodi gestiti. Per ulteriori informazioni sui PowerShell moduli, vedere PowerShell Moduli [Windows](#).

Visualizzare la descrizione e i parametri disponibili

```
Get-SSMDocumentDescription `
  -Name "AWS-InstallPowerShellModule"
```

Visualizzare ulteriori informazioni sui parametri

```
Get-SSMDocumentDescription `
  -Name "AWS-InstallPowerShellModule" | Select -ExpandProperty Parameters
```

Installare un PowerShell modulo

Il comando seguente scarica il EZOut.zip file, lo installa e quindi esegue un comando aggiuntivo per installare XPS Viewer. Infine, l'output di questo comando viene caricato in un bucket S3 denominato "amzn-s3-demo-bucket".

```
$installPSCommand = Send-SSMCommand `
  -InstanceId instance-ID `
  -DocumentName "AWS-InstallPowerShellModule" `
  -Parameter @{ 'source'='https://gallery.technet.microsoft.com/EZOut-33ae0fb7/file/110351/1/EZOut.zip'; 'commands'=@('Add-WindowsFeature -name XPS-Viewer -restart')} `
```

```
-OutputS3BucketName amzn-s3-demo-bucket
```

Ottenere informazioni sul comando per nodo gestito

Il comando seguente usa CommandId per ottenere lo stato di esecuzione del comando.

```
Get-SSMCommandInvocation `
  -CommandId $installPSCommand.CommandId `
  -Details $true
```

Ottenere informazioni sul comando con i dati di risposta per il nodo gestito

Il comando seguente restituisce l'output del comando Send-SSMCommand originale per il CommandId specifico.

```
Get-SSMCommandInvocation `
  -CommandId $installPSCommand.CommandId `
  -Details $true | Select -ExpandProperty CommandPlugins
```

Aggiungere un nodo gestito a un dominio usando il Documento JSON **AWS-JoinDirectoryServiceDomain**

Utilizzando Run Command, è possibile aggiungere rapidamente un nodo gestito a un Servizio di directory AWS dominio. Prima di eseguire il comando, è necessario [creare una directory](#). Ti consigliamo anche di consultare Directory Service. Per ulteriori informazioni, consulta la [Guida di amministrazione di Servizio di directory AWS](#).

Al momento è possibile solo aggiungere un nodo gestito a un dominio. Non è possibile rimuovere un nodo gestito da un dominio.

Note

Per informazioni sui nodi gestiti durante l'utilizzo di Run Command per chiamare script, vedi [Gestione di riavvii durante l'esecuzione dei comandi](#).

Visualizzare la descrizione e i parametri disponibili

```
Get-SSMDocumentDescription `
  -Name "AWS-JoinDirectoryServiceDomain"
```

Visualizzare ulteriori informazioni sui parametri

```
Get-SSMDocumentDescription `
    -Name "AWS-JoinDirectoryServiceDomain" | Select -ExpandProperty Parameters
```

Unisci un nodo gestito a un dominio

Il comando seguente unisce un nodo gestito al Directory Service dominio specificato e carica qualsiasi output generato nel bucket Amazon Simple Storage Service (Amazon S3) di esempio.

```
$domainJoinCommand = Send-SSMCommand `
    -InstanceId instance-ID `
    -DocumentName "AWS-JoinDirectoryServiceDomain" `
    -Parameter @{ 'directoryId'='d-example01'; 'directoryName'='ssm.example.com';
    'dnsIpAddresses'=@('192.168.10.195', '192.168.20.97')} `
    -OutputS3BucketName amzn-s3-demo-bucket
```

Ottenere informazioni sul comando per nodo gestito

Il comando seguente usa CommandId per ottenere lo stato di esecuzione del comando.

```
Get-SSMCommandInvocation `
    -CommandId $domainJoinCommand.CommandId `
    -Details $true
```

Ottenere informazioni sul comando con i dati di risposta per il nodo gestito

Questo comando restituisce l'output dell'originale Send-SSMCommand per lo specifico CommandId.

```
Get-SSMCommandInvocation `
    -CommandId $domainJoinCommand.CommandId `
    -Details $true | Select -ExpandProperty CommandPlugins
```

Invia le metriche di Windows ad Amazon Logs utilizzando il documento CloudWatch **AWS-ConfigureCloudWatch**

Puoi inviare Windows Server messaggi nei log di applicazione, sistema, sicurezza ed Event Tracing for Windows (ETW) ad Amazon Logs. CloudWatch Quando abiliti la registrazione per la prima volta, invia tutti i log generati entro un (1) minuto dal momento in cui inizi il caricamento per i log applicazioni, di sistema, di sicurezza e di ETW. I log precedenti a questo intervallo non sono inclusi. Se disabiliti la registrazione e la riattivi in seguito, Systems Manager invia i log dal momento che è

stata interrotta. Per tutti i file di log personalizzati e log IIS (Internet Information Services), Systems Manager legge i file di log dall'inizio. Inoltre, Systems Manager può anche inviare i dati dei contatori delle prestazioni a CloudWatch Logs.

Se in precedenza è stata attivata CloudWatch l'integrazione in EC2Config, le impostazioni di Systems Manager hanno la precedenza su tutte le impostazioni archiviate localmente nel nodo gestito del file. C:\Program Files\Amazon\EC2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json Per ulteriori informazioni sull'utilizzo di EC2Config per gestire i contatori delle prestazioni e i log su un singolo nodo gestito, consulta [Raccolta di metriche e registri da istanze Amazon EC2 e server locali con l'agente nella Amazon User Guide. CloudWatch CloudWatch](#)

Visualizzare la descrizione e i parametri disponibili

```
Get-SSMDocumentDescription `
    -Name "AWS-ConfigureCloudWatch"
```

Visualizzare ulteriori informazioni sui parametri

```
Get-SSMDocumentDescription `
    -Name "AWS-ConfigureCloudWatch" | Select -ExpandProperty Parameters
```

Invia i log delle applicazioni a CloudWatch

Il comando seguente configura il nodo gestito e sposta i registri delle applicazioni Windows in CloudWatch.

```
$cloudWatchCommand = Send-SSMCommand `
    -InstanceID instance-ID `
    -DocumentName "AWS-ConfigureCloudWatch" `
    -Parameter @{'properties'='{ "engineConfiguration": { "PollInterval": "00:00:15",
"Components": [{ "Id": "ApplicationEventLog",
"FullName": "AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent, AWS.EC2.Windows.CloudWa
"Parameters": { "LogName": "Application", "Levels": "7" } }, { "Id": "CloudWatch",
"FullName": "AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput, AWS.EC2.Windows.CloudWatch",
"Parameters": { "Region": "region", "LogGroup": "my-log-group", "LogStream": "instance-
id" } } ], "Flows": { "Flows": [ "ApplicationEventLog, CloudWatch" ] } } }
```

Ottenere informazioni sul comando per nodo gestito

Il comando seguente usa CommandId per ottenere lo stato di esecuzione del comando.

```
Get-SSMCommandInvocation `
  -CommandId $cloudWatchCommand.CommandId `
  -Details $true
```

Ottenere informazioni sul comando con i dati di risposta per un nodo gestito specifico

Il comando seguente restituisce i risultati della CloudWatch configurazione Amazon.

```
Get-SSMCommandInvocation `
  -CommandId $cloudWatchCommand.CommandId `
  -Details $true `
  -InstanceId instance-ID | Select -ExpandProperty CommandPlugins
```

Invia i contatori delle prestazioni all' CloudWatch uso del documento **AWS-ConfigureCloudWatch**

Il seguente comando dimostrativo carica i contatori delle prestazioni in. CloudWatch Per ulteriori informazioni, consulta la [Amazon CloudWatch User Guide](#).

```
$cloudWatchMetricsCommand = Send-SSMCommand `
  -InstanceId instance-ID `
  -DocumentName "AWS-ConfigureCloudWatch" `
  -Parameter @{'properties'='{ "engineConfiguration": { "PollInterval": "00:00:15",
"Components": [{ "Id": "PerformanceCounter",
"FullName": "AWS.EC2.Windows.CloudWatch.PerformanceCounterComponent.PerformanceCounterInputComp
"Parameters": { "CategoryName": "Memory", "CounterName": "Available
MBytes", "InstanceName": "", "MetricName": "AvailableMemory",
"Unit": "Megabytes", "DimensionName": "", "DimensionValue": "" }}, { "Id": "CloudWatch",
"FullName": "AWS.EC2.Windows.CloudWatch.CloudWatch.CloudWatchOutputComponent, AWS.EC2.Windows.Cl
"Parameters": { "AccessKey": "", "SecretKey": "", "Region": "region", "NameSpace": "Windows-
Default" } } ] }, "Flows": { "Flows": [ "PerformanceCounter, CloudWatch" ] } } }
```

Attivare o disattivare l'aggiornamento automatico di Windows utilizzando il **AWS-ConfigureWindowsUpdate** documento

Con Run Command e il documento AWS-ConfigureWindowsUpdate è possibile abilitare o disabilitare gli aggiornamenti automatici di Windows nei nodi gestiti Windows Server. Questo comando configura l'agente di aggiornamento di Windows in modo da scaricare e installare gli aggiornamenti di Windows nel giorno e all'ora specificati. Se un aggiornamento richiede il riavvio, il nodo gestito si riavvia automaticamente 15 minuti dopo l'installazione degli aggiornamenti. Con questo comando è possibile anche configurare Windows Update in modo da controllare la

disponibilità di aggiornamenti senza installarli. Il documento AWS-ConfigureWindowsUpdate è ufficialmente supportato in Windows Server 2012 e nelle versioni successive.

Visualizzare la descrizione e i parametri disponibili

```
Get-SSMDocumentDescription `
    -Name "AWS-ConfigureWindowsUpdate"
```

Visualizzare ulteriori informazioni sui parametri

```
Get-SSMDocumentDescription `
    -Name "AWS-ConfigureWindowsUpdate" | Select -ExpandProperty Parameters
```

Attivare l'aggiornamento automatico di Windows

Il comando seguente configura Windows Update in modo da scaricare e installare automaticamente gli aggiornamenti ogni giorno alle 10:00.

```
$configureWindowsUpdateCommand = Send-SSMCommand `
    -InstanceId instance-ID `
    -DocumentName "AWS-ConfigureWindowsUpdate" `
    -Parameters @{'updateLevel'='InstallUpdatesAutomatically';
    'scheduledInstallDay'='Daily'; 'scheduledInstallTime'='22:00'}
```

Visualizzare lo stato del comando per abilitare l'aggiornamento automatico di Windows

Il comando seguente usa CommandId per ottenere lo stato di esecuzione del comando e abilitare l'aggiornamento automatico di Windows.

```
Get-SSMCommandInvocation `
    -Details $true `
    -CommandId $configureWindowsUpdateCommand.CommandId | Select -ExpandProperty
    CommandPlugins
```

Disabilitare l'aggiornamento automatico di Windows

Il comando seguente riduce il livello della notifica di Windows Update in modo che il sistema verifichi la disponibilità di aggiornamenti senza aggiornare automaticamente il nodo gestito.

```
$configureWindowsUpdateCommand = Send-SSMCommand `
    -InstanceId instance-ID `
```



```
-DocumentName "AWS-ConfigureWindowsUpdate" `
-Parameters @{'updateLevel'='NeverCheckForUpdates'}
```

Visualizzare lo stato del comando per disabilitare l'aggiornamento automatico di Windows

Il comando seguente usa `CommandId` per ottenere lo stato di esecuzione del comando e abilitare l'aggiornamento automatico di Windows.

```
Get-SSMCommandInvocation `
  -Details $true `
  -CommandId $configureWindowsUpdateCommand.CommandId | Select -ExpandProperty
  CommandPlugins
```

Gestisci gli aggiornamenti di Windows utilizzando Run Command

Utilizzando Run Command e il documento `AWS-InstallWindowsUpdates` è possibile gestire gli aggiornamenti per i nodi gestiti Windows Server. Questo comando analizza o installa gli aggiornamenti mancanti sui nodi gestiti e, facoltativamente, si riavvia dopo l'installazione. È possibile anche specificare le classificazioni e i livelli di gravità appropriati per gli aggiornamenti da installare nell'ambiente.

Note

Per ulteriori informazioni sul riavvio dei nodi gestiti quando usi Run Command per chiamare gli script, consulta [Gestione di riavvii durante l'esecuzione dei comandi](#).

Gli esempi seguenti dimostrano come eseguire le attività di gestione di Windows Update specificate.

Cercare tutti gli aggiornamenti di Windows mancanti

```
Send-SSMCommand `
  -InstanceId instance-ID `
  -DocumentName "AWS-InstallWindowsUpdates" `
  -Parameters @{'Action'='Scan'}
```

Installare specifici aggiornamenti di Windows

```
Send-SSMCommand `
  -InstanceId instance-ID `
  -DocumentName "AWS-InstallWindowsUpdates" `
```

```
-Parameters @{'Action'='Install';'IncludeKbs'='kb-ID-1,kb-ID-2,kb-ID-3';'AllowReboot'='True'}
```

Installare importanti aggiornamenti di Windows mancanti

```
Send-SSMCommand `
  -InstanceId instance-ID `
  -DocumentName "AWS-InstallWindowsUpdates" `
  -Parameters @{'Action'='Install';'SeverityLevels'='Important';'AllowReboot'='True'}
```

Installare gli aggiornamenti di Windows mancanti con specifiche esclusioni

```
Send-SSMCommand `
  -InstanceId instance-ID `
  -DocumentName "AWS-InstallWindowsUpdates" `
  -Parameters @{'Action'='Install';'ExcludeKbs'='kb-ID-1,kb-ID-2';'AllowReboot'='True'}
```

Risoluzione dei problemi di Systems Manager

Run Command fornisce dettagli di stato per ogni esecuzione di comandi. Per ulteriori informazioni sui dettagli degli stati dei comandi, consulta [Informazioni sugli stati dei comandi](#). Puoi usare anche le informazioni in questo argomento per la risoluzione dei problemi relativi a Run Command.

Alcuni dei miei nodi gestiti mancano

Nella pagina Esegui un comando, dopo avere scelto un documento SSM da eseguire e aver selezionato Selezione manuale delle istanze) nella sezione Destinazioni, viene visualizzato un elenco dei nodi gestiti su cui puoi decidere di eseguire il comando.

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

Dopo aver creato, attivato, riavviato o riavviato un nodo gestito, installato Run Command su un nodo o associato un profilo di istanza AWS Identity and Access Management (IAM) a un nodo, possono essere necessari alcuni minuti prima che il nodo gestito venga aggiunto all'elenco.

Una fase nel mio script non è riuscita, ma lo stato generale è "riuscito"

È possibile utilizzare Run Command 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. È tuttavia possibile includere un'istruzione

condizionale per uscire dallo script se un comando precedente a quello finale non riesce. Per maggiori informazioni ed esempi, consulta [Specifica dei codici di uscita nei comandi](#).

Agente SSM non funziona correttamente

Se si verificano problemi durante l'esecuzione di comandi con Run Command, è possibile che sia presente un problema relativo a SSM Agent. Per informazioni su come indagare i problemi con SSM Agent, consulta [Risoluzione dei problemi Agente SSM](#).

AWS Systems Manager Session Manager

 Il Session Manager la pagina precedente sarà obsoleta il 31 dicembre 2026.

Session Manager le funzionalità fanno ora parte dell'esperienza di console unificata di Systems Manager. Sarai comunque in grado di avviare sessioni, visualizzare la cronologia e gestire le preferenze. [Ulteriori informazioni](#)

Session Manager è uno AWS Systems Manager strumento completamente gestito. Con Session Manager è possibile gestire le istanze Amazon Elastic Compute Cloud (Amazon EC2), dispositivi edge, server on-premises e macchine virtuali (VM). È possibile utilizzare una shell interattiva basata su browser o la AWS Command Line Interface (AWS CLI). Session Manager fornisce una gestione sicura dei nodi senza la necessità di aprire le porte in entrata, mantenere gli host bastion o gestire le chiavi SSH. Session Manager consente inoltre di rispettare le politiche aziendali che richiedono un accesso controllato ai nodi gestiti, rigide pratiche di sicurezza e registri con dettagli di accesso ai nodi, fornendo al contempo agli utenti finali un semplice accesso multiplatforma ai nodi gestiti. Per cominciare a utilizzare Session Manager, apri la [console di Systems Manager](#). Nel pannello di navigazione, scegli Session Manager.

Come può Session Manager avvantaggiare la mia organizzazione?

Session Manager offre questi vantaggi:

- Controllo degli accessi centralizzato ai nodi che utilizzano policy IAM

Gli amministratori dispongono di un'unica posizione da cui concedere e revocare l'accesso ai nodi gestiti. Utilizzando solo le policy AWS Identity and Access Management (IAM), puoi controllare quali singoli utenti o gruppi della tua organizzazione possono utilizzare Session Manager e a quali nodi gestiti possono accedere.

- Nessuna porta in entrata aperta e nessuna necessità di gestire bastion host o chiavi SSH

Lasciando le porte PowerShell remote o SSH in entrata aperte sui nodi gestiti aumenta notevolmente il rischio che le entità eseguano comandi non autorizzati o dannosi sui nodi gestiti. Session Manager ti aiuta a migliorare la tua posizione di sicurezza consentendoti di chiudere le porte in entrata e liberandoti quindi dalla gestione di certificati e chiavi SSH, host bastione e jumpbox.

- Accesso diretto ai nodi gestiti dalla console e dalla CLI

Utilizzando la AWS Systems Manager console o la console Amazon EC2, puoi avviare una sessione con un solo clic. Usando il AWS CLI, puoi anche avviare una sessione che esegue un singolo comando o una sequenza di comandi. Poiché le autorizzazioni ai nodi gestiti vengono fornite tramite le policy IAM anziché le chiavi SSH o altri meccanismi, il tempo di connessione viene notevolmente ridotto.

- Connessione sia alle istanze Amazon EC2 che ai nodi gestiti non EC2 in ambienti [ibridi e multicloud](#)

È possibile connetterti sia alle istanze Amazon Elastic Compute Cloud (Amazon EC2) che ai nodi non EC2 nell'ambiente [ibrido e multicloud](#).

- Inoltro alla porta

Reindirizzare qualsiasi porta all'interno del nodo gestito a una porta locale su un client. Successivamente, connettersi alla porta locale e accedere all'applicazione server in esecuzione all'interno del nodo.

- Cross-platform supporto per WindowsLinux, e macOS

Session Manager fornisce supporto per Windows, Linux e macOS da un unico strumento. Ad esempio, non è necessario utilizzare un client SSH per i nodi gestiti Linux e macOS o una connessione RDP per i nodi gestiti Windows Server.

- Attività di registrazione delle sessioni

Per soddisfare i requisiti operativi o di sicurezza della tua organizzazione, potresti dover fornire un registro delle connessioni effettuate ai nodi gestiti e dei comandi che sono stati eseguiti su di essi. È possibile anche ricevere notifiche quando un utente nella tua organizzazione inizia o termina un'attività della sessione.

Le funzionalità di registrazione vengono fornite tramite l'integrazione con i seguenti Servizi AWS:

- **AWS CloudTrail**— AWS CloudTrail acquisisce informazioni sulle chiamate Session Manager API effettuate nel tuo account Account AWS e le scrive in file di log archiviati in un bucket Amazon Simple Storage Service (Amazon S3) specificato. Viene utilizzato un bucket per tutti i CloudTrail log del tuo account. Per ulteriori informazioni, consulta [Registrazione dei log AWS Systems Manager Chiamate API con AWS CloudTrail](#).
- **Amazon Simple Storage Service**: è possibile decidere di archiviare i dati di log delle sessioni in un bucket Amazon S3 di tua scelta a scopi di debug e risoluzione dei problemi. I dati di log possono essere inviati al tuo bucket Amazon S3 con o senza crittografia utilizzando la tua chiave AWS KMS key. Per ulteriori informazioni, consulta [Registrazione dei dati delle sessioni mediante Amazon S3 \(console\)](#).
- **Amazon CloudWatch Logs**: con CloudWatch Logs, puoi monitorare, archiviare e accedere a file di registro da diversi Servizi AWS. Puoi inviare i dati del registro delle sessioni a un gruppo di CloudWatch log Logs per scopi di debug e risoluzione dei problemi. I dati di registro possono essere inviati al gruppo di log con o senza AWS KMS crittografia utilizzando la chiave KMS. Per ulteriori informazioni, consulta [Registrazione dei dati della sessione tramite Amazon CloudWatch Logs \(console\)](#).
- **Amazon EventBridge** e **Amazon Simple Notification Service**: ti EventBridge consentono di impostare regole per rilevare quando vengono apportate modifiche alle AWS risorse specificate. È possibile creare una regola per rilevare quando un utente della tua organizzazione avvia o arresta una sessione e quindi ricevere una notifica tramite Amazon SNS (ad esempio, un testo o un messaggio e-mail) sull'evento. Puoi anche configurare un CloudWatch evento per avviare altre risposte. Per ulteriori informazioni, consulta [Monitoraggio dell'attività della sessione tramite Amazon EventBridge \(console\)](#).

Note

La registrazione non è disponibile per sessioni Session Manager che si connettono tramite port forwarding o SSH. Questo perché SSH crittografa tutti i dati della sessione all'interno della connessione TLS sicura stabilita tra gli endpoint e gli Session Manager endpoint AWS CLI e funge Session Manager solo da tunnel per le connessioni SSH.

Chi dovrebbe usare Session Manager?

- Qualsiasi AWS cliente che desideri migliorare il proprio livello di sicurezza, ridurre i costi operativi centralizzando il controllo degli accessi sui nodi gestiti e ridurre l'accesso ai nodi in entrata.

- Gli esperti di sicurezza delle informazioni che desiderano monitorare e tracciare l'accesso e le attività dei nodi e chiudere le porte in entrata sui nodi gestiti o permettere le connessioni ai nodi gestiti che non dispongono di un indirizzo IP pubblico.
- Gli amministratori che desiderano concedere e revocare l'accesso da una singola postazione e fornire agli utenti una soluzione per i nodi gestiti Linux, macOS e Windows Server.
- Utenti che desiderano connettersi a un nodo gestito direttamente dal browser o AWS CLI senza dover fornire chiavi SSH.

Quali sono le caratteristiche principali di Session Manager?

- Supporto per i nodi gestiti Windows Server, Linux e macOS

Session Manager consente di stabilire connessioni protette alle istanze Amazon Elastic Compute Cloud (EC2), ai dispositivi edge, ai server on-premises e alle macchine virtuali (VM). Per un elenco dei tipi di sistema operativo dell'istanza supportati, consulta [Configurazione di Session Manager](#).

- Accesso alle funzionalità del Session Manager tramite console, interfaccia a riga di comando (CLI) e SDK

È possibile utilizzare Session Manager nei modi seguenti:

La console AWS Systems Manager include l'accesso a tutte le funzionalità del Session Manager sia per gli amministratori sia per gli utenti finali. Tramite la console Systems Manager, è possibile eseguire qualsiasi processo correlato alle tue sessioni.

La console Amazon EC2 consente agli utenti finali di connettersi alle istanze EC2 per le quali sono state concesse autorizzazioni di sessione.

AWS CLI include l'accesso alle funzionalità del Session Manager per gli utenti finali. È possibile avviare una sessione, visualizzare un elenco di sessioni e terminare definitivamente una sessione utilizzando il AWS CLI.

Note

Per utilizzare i comandi di sessione AWS CLI per eseguire, è necessario utilizzare la versione 1.16.12 della CLI (o successiva) e aver installato il Session Manager plug-in sul computer locale. Per informazioni, consulta [Installa il Session Manager plugin per AWS CLI](#). Per visualizzare il plug-in su GitHub, consulta [session-manager-plugin](#).

- Controllo degli accessi IAM

Mediante le policy IAM, è possibile controllare quali membri della tua organizzazione possono avviare sessioni ai nodi gestiti e a quali nodi possono accedere. È possibile anche fornire un accesso temporaneo ai tuoi nodi gestiti. Ad esempio, è possibile assegnare a un tecnico reperibile (o a un gruppo di tecnici reperibili) l'accesso al server di produzione solo per la durata della loro rotazione.

- Supporto per la registrazione

Session Manager fornisce opzioni per la registrazione delle cronologie delle sessioni nel tuo Account AWS tramite l'integrazione con diversi altri. Servizi AWS Per ulteriori informazioni, consulta [Attività di registrazione delle sessioni](#) e [Abilitazione e disabilitazione della registrazione di sessione](#).

- Profili della shell configurabili

Session Manager fornisce opzioni per configurare le preferenze all'interno delle sessioni. Questi profili personalizzabili permettono di definire preferenze quali le preferenze della shell, le variabili di ambiente, le directory di lavoro ed eseguire più comandi all'avvio di una sessione.

- Supporto per la crittografia dei dati della chiave del cliente

Puoi configurare Session Manager per crittografare i log dei dati di sessione che invii a un bucket Amazon Simple Storage Service (Amazon S3) o trasmessi a un gruppo di log Logs. CloudWatch È possibile anche configurare Session Manager per crittografare ulteriormente i dati trasmessi tra computer client e i tuoi nodi gestiti durante le sessioni. Per informazioni, consulta [Abilitazione e disabilitazione della registrazione di sessione](#) e [Configurare le preferenze delle sessioni](#).

- AWS PrivateLink supporto per nodi gestiti senza indirizzi IP pubblici

Puoi anche configurare VPC Endpoints for Systems Manager per AWS PrivateLink proteggere ulteriormente le tue sessioni. AWS PrivateLink limita tutto il traffico di rete tra i nodi gestiti, Systems Manager e Amazon EC2 alla rete Amazon. Per ulteriori informazioni, consulta [Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager](#).

- Tunneling

In una sessione, utilizza un documento Session-type AWS Systems Manager (SSM) per incanalare il traffico, ad esempio http o un protocollo personalizzato, tra una porta locale su un computer client e una porta remota su un nodo gestito.

- Comandi interattivi

Crea un documento Session-type SSM che utilizzi una sessione per eseguire in modo interattivo un singolo comando, offrendoti un modo per gestire ciò che gli utenti possono fare su un nodo gestito.

Che cos'è una sessione?

Una sessione è una connessione effettuata a un nodo gestito utilizzando Session Manager. Le sessioni si basano su un canale di comunicazione bidirezionale sicuro tra il client (l'utente) e il nodo gestito remoto che trasmette input e output per i comandi. Il traffico tra un client e un nodo gestito viene crittografato utilizzando TLS 1.2 e le richieste per creare la connessione sono firmate utilizzando Sigv4. Questa comunicazione bidirezionale consente un bash interattivo e PowerShell l'accesso ai nodi gestiti. È inoltre possibile utilizzare una chiave AWS Key Management Service (AWS KMS) per crittografare ulteriormente i dati oltre alla crittografia TLS predefinita.

Ad esempio, supponi che John sia un tecnico reperibile del tuo reparto IT. Riceve una notifica di un problema che richiede di connettersi da remoto a un nodo gestito, ad esempio un errore che richiede la risoluzione del problema o una direttiva per modificare una semplice opzione di configurazione su un nodo gestito. Utilizzando la AWS Systems Manager console, la console Amazon EC2 o la AWS CLI, John avvia una sessione di connessione al nodo gestito, esegue i comandi sul nodo necessari per completare l'attività e quindi termina la sessione.

Quando John invia il primo comando per avviare la sessione, il servizio Session Manager autentica il suo ID, verifica le autorizzazioni concesse da una policy IAM, controlla le impostazioni di configurazione (ad esempio verifica i limiti consentiti per le sessioni) e invia un messaggio all'SSM Agent per aprire il collegamento bidirezionale. Una volta stabilita la connessione e dopo aver digitato il comando successivo, l'output del comando da parte dell'SSM Agent viene caricato su questo canale di comunicazione e inviato nuovamente al computer locale di John.

Argomenti

- [Configurazione di Session Manager](#)
- [Utilizzo di Session Manager](#)
- [Attività di registrazione delle sessioni](#)
- [Abilitazione e disabilitazione della registrazione di sessione](#)
- [Schema documento di sessione](#)
- [Risoluzione dei problemi relativi a Session Manager](#)

Configurazione di Session Manager

Prima di utilizzare la connessione AWS Systems Manager Session Manager ai nodi gestiti del tuo account, completa i passaggi descritti nei seguenti argomenti.

Argomenti

- [Fase 1: Completare Session Manager prerequisiti](#)
- [Fase 2: Verifica o aggiungi le autorizzazioni delle istanze per Session Manager](#)
- [Fase 3: Controlla l'accesso della sessione ai nodi gestiti](#)
- [Fase 4: configurazione delle preferenze delle sessioni](#)
- [Fase 5: \(facoltativo\) limitazione dell'accesso ai comandi in una sessione](#)
- [Fase 6: \(Facoltativo\) Uso AWS PrivateLink per configurare un endpoint VPC per Session Manager](#)
- [Fase 7 \(facoltativo\): abilitazione o disabilitazione delle autorizzazioni amministrative dell'account ssm-account](#)
- [Passaggio 8: \(Facoltativo\) Consenti e controlla le autorizzazioni per le connessioni SSH tramite Session Manager](#)

Fase 1: Completare Session Manager prerequisiti

Prima di utilizzare il Session Manager, verifica che il tuo ambiente soddisfi i requisiti seguenti.

Session Manager prerequisiti

Requisito	Description
Sistemi operativi supportati	<p>Session Manager supporta la connessione a istanze Amazon Elastic Compute Cloud (Amazon EC2), oltre a macchine non EC2 nel tuo ambiente ibrido e multicloud.</p> <p>Session Manager supporta le seguenti versioni dei sistemi operativi:</p> <p>Linux e macOS</p> <p>Session Manager supporta tutte le versioni di e che sono supportate da. Linux macOS AWS</p>

Requisito	Description
	<p>Systems Manager Per informazioni, consulta Sistemi operativi e tipi di macchine supportati.</p> <p>Windows</p> <p>Session Manager supporta la versione Windows Server 2012 e le successive.</p> <div> Note Microsoft Windows Server 2016 Nano non è supportato.</div>

Requisito	Description
SSM Agent	<p>Come minimo, AWS Systems Manager SSM Agent la versione 2.3.68.0 o successiva deve essere installata nei nodi gestiti a cui ci si desidera connettere tramite sessioni.</p> <p>Per utilizzare l'opzione per crittografare i dati della sessione utilizzando una chiave creata in AWS Key Management Service (AWS KMS), è necessario installare la versione 2.3.539.0 o successiva sul nodo gestito. SSM Agent</p> <p>Per utilizzare i profili di shell in una sessione, la versione 3.0.161.0 o successiva di SSM Agent deve essere installata sul nodo gestito.</p> <p>Per avviare un Port forwarding o una sessione SSH su Session Manager, la versione 3.0.222.0 o successiva di SSM Agent deve essere installata sul nodo gestito.</p> <p>Per eseguire lo streaming dei dati delle sessioni utilizzando Amazon CloudWatch Logs, è necessario SSM Agent installare la versione 3.0.284.0 o successiva sul nodo gestito.</p> <p>Per informazioni su come determinare il numero di versione in esecuzione su un'istanza, consulta Verifica del Agente SSM numero di versione. Per informazioni sull'installazione o l'aggiornamento di SSM Agent, consulta Lavorare con Agente SSM.</p> <p>Informazioni sull'account ssm-user</p> <p>A partire dalla versione 2.3.50.0 di SSM Agent, l'agente crea un account utente nel nodo gestito, con autorizzazioni di amministratore o</p>

Requisito	Description
	<p>root, denominato <code>ssm-user</code>. (Nelle versioni precedenti alla 2.3.612.0, l'account viene creato quando SSM Agent viene avviato o riavviato. Nella versione 2.3.612.0 e successive, <code>ssm-user</code> viene creato la prima volta che si avvia una sessione sul nodo gestito). Le sessioni vengono avviate utilizzando le credenziali amministrative di questo account utente. Per informazioni su come limitare il controllo amministrativo per questo account, consulta Disattivare o attivare le autorizzazioni amministrative dell'account ssm-user.</p> <p><code>ssm-user</code> attivo Windows Server controller di dominio</p> <p>A partire dalla versione 2.3.612.0 di SSM Agent, l'account <code>ssm-user</code> non viene creato automaticamente su nodi gestiti utilizzate come controller di dominio Windows Server. Per utilizzare Session Manager su un sistema Windows Server utilizzato come controller di dominio, è necessario creare l'account <code>ssm-user</code> manualmente, se non è già presente, e assegnare le autorizzazioni di amministratore di dominio all'utente. In Windows Server, SSM Agent imposta una nuova password per l'account <code>ssm-user</code> ogni volta che viene avviata una sessione, pertanto non è necessario specificare una password quando si crea l'account.</p>

Requisito	Description
Connettività agli endpoint	<p>In questo caso, i nodi gestiti devono consentire e anche il traffico in uscita HTTPS (porta 443) verso i seguenti endpoint:</p> <ul style="list-style-type: none">• messaggi ec2. <i>region</i>.amazonaws.com• sms. <i>region</i>.amazonaws.com• messaggi sms. <i>region</i>.amazonaws.com <p>Per ulteriori informazioni, consulta i seguenti argomenti:</p> <ul style="list-style-type: none">• Referenza: ec2messages, ssmmessages e altre operazioni API• Come posso creare endpoint VPC in modo da poter utilizzare Systems Manager per gestire istanze EC2 private senza accesso a Internet? nel Knowledge Center. AWS re:Post <p>In alternativa, è possibile connettersi agli endpoint richiesti utilizzando gli endpoint di interfaccia. Per ulteriori informazioni, consulta Fase 6: (Facoltativo) Uso AWS PrivateLink per configurare un endpoint VPC per Session Manager.</p>

Requisito	Description
AWS CLI	<p>(Facoltativo) Se utilizzi AWS Command Line Interface (AWS CLI) per avviare le sessioni (anziché utilizzare la AWS Systems Manager console o la console Amazon EC2), la versione 1.16.12 o successiva della CLI deve essere installata sul computer locale.</p> <p>È possibile chiamare <code>aws --version</code> per controllare la versione.</p> <p>Se devi installare o aggiornare la CLI, consulta Installazione nella Guida per l' AWS Command Line Interfaceutente. AWS Command Line Interface</p> <div><p> Important</p><p>Una versione aggiornata di SSM Agent viene distribuita ogni volta che vengono aggiunti nuovi strumenti a Systems Manager o eseguiti aggiornamenti degli strumenti esistenti. Il mancato utilizzo della versione più recente dell'agente può impedire al nodo gestito di utilizzare vari strumenti e funzionalità di Systems Manager. Per questo motivo, ti consigliamo di automatizzare il processo di aggiornamento di SSM Agent sulle macchine. Per informazioni, consulta Automatizzazione degli aggiornamenti a Agente SSM. Iscriviti alla pagina Note di rilascio di SSM Agent su GitHub per ricevere notifiche sugli aggiornamenti di SSM Agent.</p></div>

Requisito	Description
	<p>Inoltre, per utilizzare la CLI per gestire i tuoi nodi con il Session Manager, devi prima installare il plug-in Session Manager sul computer locale. Per informazioni, consulta Installa il Session Manager plugin per AWS CLI.</p>
<p>Verifica delle autorizzazioni del ruolo di servizio IAM (ambienti ibridi e multicloud)</p>	<p>Hybrid-activated i nodi utilizzano il ruolo di servizio AWS Identity and Access Management (IAM) specificato nell'attivazione ibrida per comunicare con le operazioni dell'API di Systems Manager. Questo ruolo di servizio deve contenere le autorizzazioni necessari e per connettersi alle macchine ibride e multicloud utilizzando Session Manager. Se il tuo ruolo di servizio contiene la policy AWS gestita <code>AmazonSSMManagedInstanceCore</code>, le autorizzazioni richieste per Session Manager sono già fornite.</p> <p>Se si scopre che il ruolo di servizio non contiene le autorizzazioni richieste, è necessario annullare la registrazione dell'istanza gestita e registrarla con una nuova attivazione ibrida che utilizza un ruolo di servizio IAM con le autorizzazioni richieste. Per ulteriori informazioni sull'annullamento delle registrazioni delle istanze gestite, consulta Annullamento della registrazione dei nodi gestiti in un ambiente ibrido e multicloud. Per ulteriori informazioni sulla creazione di policy IAM con autorizzazioni Session Manager, vedi Fase 2: Verifica o aggiungi autorizzazioni di istanze per Session Manager.</p>

Fase 2: Verifica o aggiungi le autorizzazioni delle istanze per Session Manager

Per impostazione predefinita, AWS Systems Manager non dispone dell'autorizzazione per eseguire azioni sulle tue istanze. È possibile fornire le autorizzazioni di istanza a livello di account utilizzando un ruolo AWS Identity and Access Management (IAM) o a livello di istanza utilizzando un profilo dell'istanza. Se il caso d'uso lo consente, ti consigliamo di concedere l'accesso a livello di account utilizzando la configurazione di gestione host predefinita. Se hai già impostato la configurazione di gestione host predefinita per il tuo account utilizzando la policy `AmazonSSMManagedEC2InstanceDefaultPolicy`, è possibile procedere con il passaggio successivo. Per ulteriori informazioni sulla configurazione di gestione host predefinita, consulta [Gestione automatica delle istanze EC2 con la configurazione di gestione host predefinita](#).

In alternativa, è possibile utilizzare i profili di istanza per fornire le autorizzazioni necessarie alle tue istanze. Un profilo dell'istanza passa un ruolo IAM a un'istanza Amazon EC2. È possibile collegare un profilo dell'istanza IAM a un'istanza Amazon EC2 all'avvio o a un'istanza avviata in precedenza. Per ulteriori informazioni, consulta [Utilizzo dei profili dell'istanza](#).

Per i server locali o le macchine virtuali (VM), le autorizzazioni sono fornite dal ruolo del servizio IAM associato all'attivazione ibrida utilizzata per registrare i server e le macchine virtuali locali con Systems Manager. On-premises i server e le macchine virtuali non utilizzano profili di istanza.

Se utilizzi già altri strumenti di Systems Manager, ad esempio Run Command o Parameter Store, un profilo dell'istanza con le autorizzazioni di base richieste per il Session Manager potrebbe essere già associato alle tue istanze Amazon EC2. Se un profilo di istanza che contiene la policy AWS gestita `AmazonSSMManagedInstanceCore` è già collegato alle istanze, le autorizzazioni richieste per Session Manager sono già state fornite. Ciò vale anche se il ruolo di servizio IAM utilizzato nell'attivazione ibrida contiene la policy gestita `AmazonSSMManagedInstanceCore`.

Tuttavia, in alcuni casi, potrebbe essere necessario modificare le autorizzazioni collegate al profilo dell'istanza. Ad esempio, desideri fornire un set più ristretto di autorizzazioni per l'istanza, hai creato una policy personalizzata per il tuo profilo di istanza o desideri utilizzare le opzioni di crittografia o () di crittografia di Amazon Simple Storage Service (Amazon S3) AWS Key Management Service o AWS KMS() per proteggere i dati della sessione. Per questi casi, procedi in uno dei seguenti modi per consentire l'esecuzione di operazioni Session Manager sulle istanze:

- Incorpora autorizzazioni per azioni Session Manager in un ruolo IAM personalizzato

Per aggiungere Session Manager autorizzazioni per azioni a un ruolo IAM esistente che non si basa sulla policy predefinita AWS fornita, segui i passaggi riportati di seguito.

AmazonSSMManagedInstanceCore [Aggiunta di autorizzazioni Session Manager per un ruolo IAM esistente](#)

- Crea un ruolo IAM personalizzato solo con le autorizzazioni del Session Manager

Per creare un ruolo IAM che contenga solo le autorizzazioni per le operazioni del Session Manager, segui i passaggi riportati in [Crea un ruolo IAM personalizzato per Session Manager](#).

- Crea e utilizza un nuovo ruolo IAM con le autorizzazioni per tutte le operazioni di Systems Manager

Per creare un ruolo IAM per le istanze gestite di Systems Manager che utilizza una policy predefinita fornita da AWS per concedere tutte le autorizzazioni di Systems Manager, segui i passaggi in [Configurare le autorizzazioni delle istanze richieste per Systems Manager](#).

Argomenti

- [Aggiunta di autorizzazioni Session Manager per un ruolo IAM esistente](#)
- [Crea un ruolo IAM personalizzato per Session Manager](#)

Aggiunta di autorizzazioni Session Manager per un ruolo IAM esistente

Utilizza la procedura seguente per aggiungere autorizzazioni Session Manager a un ruolo AWS Identity and Access Management (IAM) esistente. Aggiungendo autorizzazioni a un ruolo esistente, è possibile migliorare la sicurezza dell'ambiente informatico senza dover utilizzare la AWS AmazonSSMManagedInstanceCore policy, ad esempio le autorizzazioni.

Note

Prendi nota delle seguenti informazioni:

- Questa procedura presuppone che il tuo ruolo esistente includa già altre autorizzazioni di Systems Manager ssm per le operazioni a cui desideri permettere l'accesso. Questa policy da sola non è sufficiente per l'utilizzo di Session Manager.
- Il seguente esempio di policy include un'azione `s3:GetEncryptionConfiguration`. Questa azione è necessaria se hai scelto l'opzione Applica crittografia dei log S3 nelle preferenze di registrazione di Session Manager.
- Se l'`ssmmessages:OpenControlChannel` autorizzazione viene rimossa dalle policy allegate al profilo dell'istanza IAM o al ruolo del servizio IAM, SSM Agent sul nodo gestito perde la connettività al servizio Systems Manager nel cloud. Tuttavia, può essere

necessaria fino a 1 ora prima che una connessione venga interrotta dopo la rimozione dell'autorizzazione. Si tratta dello stesso comportamento che si verifica quando il ruolo dell'istanza IAM o il ruolo del servizio IAM vengono eliminati.

Per aggiungere le autorizzazioni Session Manager per il ruolo dell'istanza per un ruolo esistente (console)

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, seleziona Ruoli.
3. Seleziona il nome del ruolo al quale desideri aggiungere le autorizzazioni.
4. Scegli la scheda Autorizzazioni.
5. Scegli Aggiungi autorizzazioni, quindi scegli Aggiungi policy inline.
6. Scegli la scheda JSON.
7. Sostituisci il contenuto predefinito della policy con il seguente. Sostituisci *key-name* con l'Amazon Resource Name (ARN) della AWS Key Management Service chiave (AWS KMS key) che desideri utilizzare.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource": "*"
    }
  ]
}
```

```

        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
          "kms:Decrypt"
        ],
        "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-name"
      }
    ]
  }
}

```

Per ulteriori informazioni sull'utilizzo di una chiave KMS per crittografare i dati della sessione, consulta [Attiva la crittografia delle chiavi KMS per i dati delle sessioni \(console\)](#).

Se non intendi utilizzare la AWS KMS crittografia per i dati della sessione, puoi rimuovere i seguenti contenuti dalla policy.

```

{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt"
  ],
  "Resource": "key-name"
}

```

8. Scegli Successivo: Tag.
9. (Facoltativo) Aggiungi i tag scegliendo Aggiungi tag e inserendo i tag preferiti per la policy.
10. Seleziona Next: Revisione.
11. Nella pagina Rivedi policy, per l'opzione Nome specifica un nome per la policy inline, ad esempio **SessionManagerPermissions**.
12. (Facoltativo) In Descrizione, inserisci una descrizione per la policy.

Scegli Crea policy.

Per informazioni sulle operazioni ssmessages, consulta [Referenza: ec2messages, ssmessages e altre operazioni API](#).

Crea un ruolo IAM personalizzato per Session Manager

Puoi creare un ruolo AWS Identity and Access Management (IAM) che conceda Session Manager l'autorizzazione a eseguire azioni sulle tue istanze gestite di Amazon EC2. Puoi anche includere una policy per concedere le autorizzazioni necessarie per l'invio dei log di sessione ad Amazon Simple Storage Service (Amazon S3) e Amazon Logs. CloudWatch

Dopo aver creato il ruolo IAM, per informazioni su come collegare il ruolo a un'istanza, consulta [Allega o sostituisci un profilo di istanza](#) sul AWS re:Post sito web. Per ulteriori informazioni sui profili e i ruoli delle istanze IAM, consulta [Utilizzo di profili di istanze](#) nella Guida per l'utente IAM e [Ruoli IAM per Amazon EC2](#) nella Guida per l'utente di Amazon Elastic Compute Cloud per istanze Linux. Per ulteriori informazioni sulla creazione di un ruolo di servizio IAM per macchine on-premises, consulta [Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud](#).

Argomenti

- [Creazione di un ruolo IAM con un minimo Session Manager autorizzazioni \(console\)](#)
- [Creazione di un ruolo IAM con autorizzazioni per Session Manager e Amazon S3 e CloudWatch Logs \(console\)](#)

Creazione di un ruolo IAM con un minimo Session Manager autorizzazioni (console)

Utilizza la procedura seguente per creare un ruolo IAM personalizzato con una policy che fornisce solo le autorizzazioni per le operazioni del Session Manager sulle tue istanze.

Per creare un profilo di istanza con un minimo Session Manager autorizzazioni (console)

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, scegli Policy e Crea policy. (Se viene visualizzato il pulsante Inizia, sceglierlo, quindi scegli Crea policy).
3. Scegli la scheda JSON.
4. Sostituire il contenuto di default con la seguente policy. Per crittografare i dati della sessione utilizzando AWS Key Management Service (AWS KMS), sostituiscili *key-name* con l'Amazon Resource Name (ARN) AWS KMS key che desideri utilizzare.

 Note

Se l'`ssmmessages:OpenControlChannel` autorizzazione viene rimossa dalle policy allegate al profilo dell'istanza IAM o al ruolo del servizio IAM, SSM Agent sul nodo gestito perde la connettività al servizio Systems Manager nel cloud. Tuttavia, l'interruzione di una connessione può richiedere fino a 1 ora dopo la rimozione dell'autorizzazione. Si tratta dello stesso comportamento di quando il ruolo di istanza IAM o il ruolo del servizio IAM viene eliminato.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:UpdateInstanceInformation",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-name"
    }
  ]
}
```

Per ulteriori informazioni sull'utilizzo di una chiave KMS per crittografare i dati della sessione, consulta [Attiva la crittografia delle chiavi KMS per i dati delle sessioni \(console\)](#).

Se non intendi utilizzare AWS KMS la crittografia per i dati della sessione, puoi rimuovere i seguenti contenuti dalla policy.

```
,
    {
        "Effect": "Allow",
        "Action": [
            "kms:Decrypt"
        ],
        "Resource": "key-name"
    }
}
```

5. Scegli Successivo: Tag.
6. (Facoltativo) Aggiungi i tag scegliendo Aggiungi tag e inserendo i tag preferiti per la policy.
7. Seleziona Next: Revisione.
8. Nella pagina Rivedi policy, per l'opzione Nome specifica un nome per la policy inline, ad esempio **SessionManagerPermissions**.
9. (Facoltativo) In Descrizione, inserisci una descrizione per la policy.
10. Scegli Crea policy.
11. Nel pannello di navigazione, scegli Ruoli e quindi Crea ruolo.
12. Sulla pagina Crea ruolo, scegli AWS servizio, e per Caso d'uso, scegli EC2.
13. Scegli Avanti.
14. Nella pagina Aggiungi autorizzazioni, seleziona la casella di controllo a sinistra del nome della policy appena creata, ad esempio **SessionManagerPermissions**.
15. Scegli Avanti.
16. Nella pagina Rinomina, revisione e creazione, per Nome ruolo immettere un nome per il ruolo IAM, ad esempio **MySessionManagerRole**.
17. (Facoltativo) Per Descrizione ruolo, immetti una descrizione per il profilo dell'istanza.
18. (Facoltativo) Aggiungi i tag scegliendo Aggiungi tag e inserendo i tag preferiti per il ruolo.

Scegliere Crea ruolo.

Per informazioni sulle operazioni di ssmmessages, consulta [Referenza: ec2messages, ssmmessages e altre operazioni API](#).

Creazione di un ruolo IAM con autorizzazioni per Session Manager e Amazon S3 e CloudWatch Logs (console)

Utilizza la procedura seguente per creare un ruolo IAM personalizzato con una policy che fornisce le autorizzazioni per le operazioni del Session Manager sulle tue istanze. La policy fornisce anche le autorizzazioni necessarie per l'archiviazione dei log di sessione nei bucket Amazon Simple Storage Service (Amazon S3) e nei gruppi di log di Amazon CloudWatch Logs.

Important

Per eseguire l'output dei log di sessione su un bucket Amazon S3 appartenente a un Account AWS diverso, devi aggiungere l'autorizzazione `s3:PutObjectAc1` alla policy del ruolo IAM. Inoltre, devi assicurarti che la policy del bucket conceda l'accesso tra più account al ruolo IAM utilizzato dall'account proprietario per concedere le autorizzazioni di Systems Manager per le istanze gestite. Se il bucket utilizza la crittografia Key Management Service (KMS), anche la policy KMS del bucket deve concedere questo accesso multi-account. Per ulteriori informazioni sulla configurazione di autorizzazioni del bucket multi-account in Amazon S3, consulta [Concessione di autorizzazioni del bucket multi-account](#) nella Guida per l'utente di Amazon Simple Storage Service. Se queste autorizzazioni multi-account non vengono aggiunte, l'account proprietario del bucket Amazon S3 non è in grado di accedere ai log di output della sessione.

Per informazioni su come specificare le preferenze di archiviazione per i log delle sessioni, consulta [Abilitazione e disabilitazione della registrazione di sessione](#).

Per creare un ruolo IAM con autorizzazioni per Session Manager e Amazon S3 e CloudWatch Logs (console)

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, scegli Policy e Crea policy. (Se viene visualizzato il pulsante Inizia, sceglierlo, quindi scegli Crea policy).
3. Scegli la scheda JSON.
4. Sostituire il contenuto di default con la seguente policy. Sostituisci ogni *example resource placeholder* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/s3-prefix/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```



```
        "Action": [
            "kms:Decrypt"
        ],
        "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-name"
    },
    {
        "Effect": "Allow",
        "Action": "kms:GenerateDataKey",
        "Resource": "*"
    }
]
```

5. Scegli Successivo: Tag.
6. (Facoltativo) Aggiungi i tag scegliendo Aggiungi tag e inserendo i tag preferiti per la policy.
7. Seleziona Next: Revisione.
8. Nella pagina Rivedi policy, per l'opzione Nome specifica un nome per la policy inline, ad esempio **SessionManagerPermissions**.
9. (Facoltativo) In Descrizione, inserisci una descrizione per la policy.
10. Scegli Crea policy.
11. Nel pannello di navigazione, scegli Ruoli e quindi Crea ruolo.
12. Sulla pagina Crea ruolo, scegli AWS servizio, e per Caso d'uso, scegli EC2.
13. Scegli Avanti.
14. Nella pagina Aggiungi autorizzazioni, seleziona la casella di controllo a sinistra del nome della policy appena creata, ad esempio **SessionManagerPermissions**.
15. Scegli Avanti.
16. Nella pagina Rinomina, revisione e creazione, per Nome ruolo immettere un nome per il ruolo IAM, ad esempio **MySessionManagerRole**.
17. (Facoltativo) In Descrizione del ruolo, immetti una descrizione per il nuovo ruolo.
18. (Facoltativo) Aggiungi i tag scegliendo Aggiungi tag e inserendo i tag preferiti per il ruolo.
19. Scegliere Crea ruolo.

Fase 3: Controlla l'accesso della sessione ai nodi gestiti

Puoi concedere o revocare Session Manager l'accesso ai nodi gestiti utilizzando le policy AWS Identity and Access Management (IAM). È possibile creare una policy e collegarla a un utente o

gruppo IAM che specifichi a quali nodi gestiti l'utente o il gruppo può connettersi. È possibile anche specificare le operazioni API Session Manager che l'utente o i gruppi possono eseguire su tali nodi gestiti.

Per aiutarti a iniziare a usare le policy di autorizzazione IAM per Session Manager, abbiamo creato policy di esempio per un utente finale e un utente amministratore. È possibile utilizzare queste policy solo con modifiche minori. Oppure è possibile usarle come guida per creare policy IAM personalizzate. Per ulteriori informazioni, consulta [Esempi di policy IAM per Session Manager](#). Per informazioni su come creare policy IAM e collegarle a utenti o gruppi, consulta le pagine [Creazione di policy IAM](#) e [Aggiunta e rimozione di policy IAM](#) nella Guida per l'utente di IAM.

Informazioni sui formati ARN degli ID di sessione

Quando crei una policy IAM per l'accesso di Session Manager, specifichi un ID di sessione come parte del nome della risorsa Amazon (ARN). L'ID di sessione include il nome utente come variabile. A scopo illustrativo, ecco il formato di un ARN di Session Manager e un esempio:

```
arn:aws:ssm:region-id:account-id:session/session-id
```

Esempio:

```
arn:aws:ssm:us-east-2:123456789012:session/JohnDoe-1a2b3c4d5eEXAMPLE
```

Per ulteriori informazioni sull'utilizzo delle variabili nelle policy IAM, consulta [Elementi delle policy IAM: variabili](#).

Argomenti

- [Avviare una sessione di shell predefinita specificando il documento di sessione predefinito nelle policy IAM](#)
- [Avviare una sessione con un documento specificando i documenti di sessione nelle policy IAM](#)
- [Esempi di policy IAM per Session Manager](#)
- [Esempi aggiuntivi di policy IAM per Session Manager](#)

Avviare una sessione di shell predefinita specificando il documento di sessione predefinito nelle policy IAM

Quando si configura Session Manager per Account AWS o quando si modificano le preferenze di sessione nella console Systems Manager, il sistema crea un documento di sessione SSM

chiamato `SSM-SessionManagerRunShell`. Questo è il documento di sessione predefinito. Session Manager utilizza questo documento per memorizzare le preferenze di sessione, che includono informazioni come le seguenti:

- Una posizione in cui desideri salvare i dati della sessione, ad esempio un bucket Amazon Simple Storage Service (Amazon S3) o un gruppo di log CloudWatch Amazon Logs.
- Un ID chiave AWS Key Management Service (AWS KMS) per crittografare i dati della sessione.
- Se il supporto Run As è consentito o meno per le sessioni.

Ecco un esempio delle informazioni contenute nel documento sulle preferenze di sessione `SSM-SessionManagerRunShell`.

```
{
  "schemaVersion": "1.0",
  "description": "Document to hold regional settings for Session Manager",
  "sessionType": "Standard_Stream",
  "inputs": {
    "s3BucketName": "amzn-s3-demo-bucket",
    "s3KeyPrefix": "MyS3Prefix",
    "s3EncryptionEnabled": true,
    "cloudWatchLogGroupName": "MyCWLogGroup",
    "cloudWatchEncryptionEnabled": false,
    "kmsKeyId": "1a2b3c4d",
    "runAsEnabled": true,
    "runAsDefaultUser": "RunAsUser"
  }
}
```

Per impostazione predefinita, Session Manager utilizza il documento di sessione predefinito quando un utente avvia una sessione dalla Console di gestione AWS. Questo vale Fleet Manager sia Session Manager per la console Systems Manager che per EC2 Connect nella console Amazon EC2. Session Manager utilizza anche il documento di sessione predefinito quando un utente avvia una sessione utilizzando un AWS CLI comando come nell'esempio seguente:

```
aws ssm start-session \
  --target i-02573cafcfEXAMPLE
```

Per accedere alla sessione di shell predefinita, è necessario specificare il documento di sessione predefinito nella policy IAM, come mostrato nell'esempio seguente.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnableSSMSession",
      "Effect": "Allow",
      "Action": [
        "ssm:StartSession"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/instance-id",
        "arn:aws:ssm:us-east-1:111122223333:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Avviare una sessione con un documento specificando i documenti di sessione nelle policy IAM

Se utilizzi il comando [start-session](#) della AWS CLI utilizzando il documento di sessione predefinito, puoi omettere il nome del documento. Il sistema richiama automaticamente il documento di sessione `SSM-SessionManagerRunShell`.

In tutti gli altri casi, devi specificare un valore per il parametro `document-name`. Quando un utente specifica il nome di un documento di sessione in un comando, i sistemi controllano la policy IAM per verificare che dispongano dell'autorizzazione ad accedere al documento. Se non dispongono dell'autorizzazione, la richiesta di connessione non riesce. Gli esempi seguenti includono il parametro `document-name` con il documento di sessione `AWS-StartPortForwardingSession`.

```
aws ssm start-session \  
  --target i-02573cafcfEXAMPLE \  
  --document-name AWS-StartPortForwardingSession \  
  --parameters '{"portNumber":["80"], "localPortNumber":["56789"]}'
```

Per un esempio di come specificare un documento di sessione Session Manager in una policy IAM, consulta [Politiche Quickstart per gli utenti finali per Session Manager](#).

Note

Per avviare una sessione con SSH, le fasi di configurazione devono essere completate sul nodo gestito di destinazione e sul computer locale dell'utente. Per informazioni, consulta [\(Facoltativo\) Abilitare e controllare le autorizzazioni per le connessioni SSH tramite Session Manager](#).

Esempi di policy IAM per Session Manager

Usa gli esempi in questa sezione per aiutarti a creare policy AWS Identity and Access Management (IAM) che forniscono le autorizzazioni di Session Manager accesso più comunemente necessarie.

Note

Puoi anche utilizzare una AWS KMS key policy per controllare a quali entità IAM (utenti o ruoli) Account AWS viene concesso l'accesso alla tua chiave KMS. Per informazioni, consulta la [panoramica sulla gestione dell'accesso alle AWS KMS risorse](#) e sull'[utilizzo delle politiche chiave AWS KMS](#) nella Guida per gli AWS Key Management Service sviluppatori.

Argomenti

- [Politiche Quickstart per gli utenti finali per Session Manager](#)
- [Politica di amministrazione Quickstart per Session Manager](#)

Politiche Quickstart per gli utenti finali per Session Manager

Utilizzare gli esempi seguenti per creare policy IAM per l'utente finale per Session Manager.

Puoi creare una policy che consenta agli utenti di avviare sessioni solo dalla Session Manager console e AWS Command Line Interface (AWS CLI), solo dalla console Amazon Elastic Compute Cloud (Amazon EC2) o da tutte e tre.

Queste policy offrono agli utenti finali la possibilità di avviare una sessione per un determinato nodo gestito nonché la possibilità di terminare solo le proprie sessioni. Per alcuni esempi di personalizzazioni che potresti applicare alla policy, fai riferimento a [Esempi aggiuntivi di policy IAM per Session Manager](#).

Nei seguenti esempi di policy, sostituisci ciascuna *example resource placeholder* con le tue informazioni.

Fare riferimento alle sezioni seguenti per visualizzare e policy di esempio per l'intervallo di accesso alla sessione che si desidera fornire.

Session Manager and Fleet Manager

Utilizzare questa policy di esempio per fornire agli utenti la possibilità di avviare e riprendere sessioni solo dalle console Session Manager e Fleet Manager.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:StartSession"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/i-02573cafcfEXAMPLE",
        "arn:aws:ssm:us-east-1:111122223333:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Effect": "Allow",
      "Action": ["ssmmessages:OpenDataChannel"],
      "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
    }
  ]
}
```

```

    {
      "Effect": "Allow",
      "Action": [
        "ssm:DescribeSessions",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceProperties",
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:TerminateSession",
        "ssm:ResumeSession"
      ],
      "Resource": [
        "arn:aws:ssm:*:*:session/${aws:userid}-*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-name"
    }
  ]
}

```

Amazon EC2

Utilizzare questa policy di esempio per fornire agli utenti la possibilità di avviare e riprendere sessioni solo dalla console Amazon EC2. Questa policy non fornisce tutte le autorizzazioni necessarie per avviare le sessioni dalla console Session Manager e dall' AWS CLI.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [

```

```

    {
      "Effect": "Allow",
      "Action": [
        "ssm:StartSession",
        "ssm:SendCommand"
      ],
      "Resource": [
        "arn:aws:ec2:us-  
east-1:111122223333:instance/i-02573cafcfEXAMPLE",
        "arn:aws:ssm:us-east-1:111122223333:document/SSM-  
SessionManagerRunShell"
      ]
    },
    {
      "Effect": "Allow",
      "Action": ["ssmmessages:OpenDataChannel"],
      "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:TerminateSession",
        "ssm:ResumeSession"
      ],
      "Resource": [
        "arn:aws:ssm:*:*:session/${aws:username}-*"
      ]
    }
  ]
}

```


AWS CLI

Utilizzare questa policy di esempio per fornire agli utenti la possibilità di avviare e riprendere sessioni solo da AWS CLI.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:StartSession",
        "ssm:SendCommand"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/i-02573cafcfEXAMPLE",
        "arn:aws:ssm:us-east-1:111122223333:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Effect": "Allow",
      "Action": ["ssmmessages:OpenDataChannel"],
      "Resource": ["arn:aws:ssm:*:session/${aws:userid}-*"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:TerminateSession",
        "ssm:ResumeSession"
      ],
      "Resource": [
        "arn:aws:ssm:*:session/${aws:userid}-*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey"
      ],
    }
  ]
}
```

```

    "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-name"
  }
]
}

```

Note

SSM-SessionManagerRunShell è il nome predefinito del documento SSM creato da Session Manager per archiviare le preferenze di configurazione della sessione. Puoi creare un documento di sessione personalizzato e specificarlo in questa policy. Puoi anche specificare il documento AWS-StartSSHSesssion fornito da AWS per gli utenti che avviano le sessioni mediante SSH. Per informazioni sui passi di configurazione necessari per supportare le sessioni utilizzando SSH, consulta [\(Facoltativo\) Permettere e controllare le autorizzazioni per le connessioni SSH tramite Session Manager](#).

L'autorizzazione kms:GenerateDataKey consente la creazione di una chiave di crittografia dei dati che verrà utilizzata per crittografare i dati delle sessioni. Se utilizzi la crittografia AWS Key Management Service (AWS KMS) per i dati della sessione, sostituiscila **key-name** con Amazon Resource Name (ARN) della chiave KMS che desideri utilizzare, nel formato. arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-12345EXAMPLE Se non utilizzi la crittografia delle chiavi KMS per i dati delle sessioni, rimuovi i seguenti contenuti dalla policy:

```

{
    "Effect": "Allow",
    "Action": [
        "kms:GenerateDataKey"
    ],
    "Resource": "key-name"
}

```

Per informazioni sull'utilizzo AWS KMS per la crittografia dei dati della sessione, consulta. [Attiva la crittografia delle chiavi KMS per i dati delle sessioni \(console\)](#)

L'autorizzazione per [SendCommand](#) è necessaria nei casi in cui un utente tenta di avviare una sessione dalla console Amazon EC2, ma bisogna prima aggiornare l'SSM Agent alla versione minima richiesta per Session Manager. Run Command viene utilizzato per inviare un comando all'istanza per aggiornare l'agente.

Politica di amministrazione Quickstart per Session Manager

Utilizzare gli esempi seguenti per creare policy di amministratore IAM per Session Manager.

Queste policy offrono agli amministratori la possibilità di avviare una sessione per i nodi gestiti contrassegnati con il tag `Key=Finance, Value=WebServers`, l'autorizzazione di creare, aggiornare ed eliminare le preferenze nonché l'autorizzazione di terminare solo le proprie sessioni. Per alcuni esempi di personalizzazioni che potresti applicare alla policy, fai riferimento a [Esempi aggiuntivi di policy IAM per Session Manager](#).

È possibile creare una policy che consenta agli amministratori di eseguire queste attività solo dalla Session Manager console e AWS CLI, solo dalla console Amazon EC2, o da tutte e tre.

Nei seguenti esempi di policy, sostituisci ciascuna *example resource placeholder* con le tue informazioni.

Fare riferimento alle sezioni seguenti per visualizzare le policy di esempio per i tre scenari di autorizzazioni.

Session Manager and CLI

Utilizzare questa policy di esempio per fornire agli amministratori del provider la possibilità di eseguire processi correlati alla sessione solo dalla console Session Manager e dall' AWS CLI. Questa policy non fornisce tutte le autorizzazioni necessarie per eseguire processi correlati alla sessione dalla console Amazon EC2.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:StartSession"
      ],
      "Resource": [
        "arn:aws:ec2:*:111122223333:instance/*"
      ],
      "Condition": {
        "StringLike": {
          "ssm:resourceTag/Finance": [
```

```

        "WebServers"
    ]
}
},
{
    "Effect": "Allow",
    "Action": [
        "ssmmessages:OpenDataChannel"
    ],
    "Resource": [
        "arn:aws:ssm:*:*:session/${aws:userid}-*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ssm:DescribeSessions",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceProperties",
        "ec2:DescribeInstances"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ssm:CreateDocument",
        "ssm:UpdateDocument",
        "ssm:GetDocument",
        "ssm:StartSession"
    ],
    "Resource": "arn:aws:ssm:us-east-1:111122223333:document/SSM-SessionManagerRunShell"
},
{
    "Effect": "Allow",
    "Action": [
        "ssmmessages:OpenDataChannel"
    ],
    "Resource": [
        "arn:aws:ssm:*:*:session/${aws:userid}-*"
    ]
},

```

```

    {
      "Effect": "Allow",
      "Action": [
        "ssm:TerminateSession",
        "ssm:ResumeSession"
      ],
      "Resource": [
        "arn:aws:ssm:*:*:session/${aws:userid}-*"
      ]
    }
  ]
}

```

Amazon EC2

Utilizzare questa policy di esempio per fornire agli amministratori del provider la possibilità di eseguire processi correlati alla sessione solo dalla console Amazon EC2. Questa policy non fornisce tutte le autorizzazioni necessarie per eseguire attività correlate alla sessione dalla console Session Manager e dall' AWS CLI.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:StartSession",
        "ssm:SendCommand"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
        "StringLike": {
          "ssm:resourceTag/tag-key": [
            "tag-value"
          ]
        }
      }
    }
  ]
}

```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:StartSession"
      ],
      "Resource": [
        "arn:aws:ssm:us-east-1:111122223333:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Effect": "Allow",
      "Action": ["ssmmessages:OpenDataChannel"],
      "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:TerminateSession",
        "ssm:ResumeSession"
      ],
      "Resource": [
        "arn:aws:ssm:*:*:session/${aws:userid}-*"
      ]
    }
  ]
}

```

Session Manager, CLI, and Amazon EC2

Utilizzare questa policy di esempio per fornire agli amministratori del provider la possibilità di eseguire processi relativi alla sessione dalla console Session Manager, dall' AWS CLI e dalla console Amazon EC2.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:StartSession",
        "ssm:SendCommand"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
        "StringLike": {
          "ssm:resourceTag/tag-key": [
            "tag-value"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": ["ssmmessages:OpenDataChannel"],
      "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:DescribeSessions",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeInstanceProperties",
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:CreateDocument",
        "ssm:UpdateDocument",

```

```

        "ssm:GetDocument",
        "ssm:StartSession"
    ],
    "Resource": "arn:aws:ssm:us-east-1:111122223333:document/SSM-
SessionManagerRunShell"
},
{
    "Effect": "Allow",
    "Action": [
        "ssm:TerminateSession",
        "ssm:ResumeSession"
    ],
    "Resource": [
        "arn:aws:ssm:*:*:session/${aws:userid}-*"
    ]
}
]
}

```

Note

L'autorizzazione per [SendCommand](#) è necessaria nei casi in cui un utente tenta di avviare una sessione dalla console Amazon EC2, ma prima bisogna inviare un comando per aggiornare SSM Agent.

Esempi aggiuntivi di policy IAM per Session Manager

Fai riferimento alle seguenti policy di esempio per creare una policy IAM AWS Identity and Access Management personalizzata per qualunque scenario di accesso utente al Session Manager che desideri supportare.

Argomenti

- [Esempio 1: concedere l'accesso ai documenti nella console](#)
- [Esempio 2: limitare l'accesso a nodi gestiti specifici](#)
- [Esempio 3: limitazione dell'accesso in base ai tag](#)
- [Esempio 4: consentire agli utenti di terminare solo le sessioni da essi avviate](#)
- [Esempio 5: consentire l'accesso \(amministrativo\) completo a tutte le sessioni](#)

Esempio 1: concedere l'accesso ai documenti nella console

Puoi consentire agli utenti di specificare un documento personalizzato quando avviano una sessione utilizzando la console di Session Manager. Nel seguente esempio, la policy IAM concede l'autorizzazione ad accedere ai documenti con nomi che iniziano con **SessionDocument-** nella Regione AWS e nell' Account AWS specificati.

Per utilizzare questa policy, sostituiscile ognuna *example resource placeholder* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetDocument",
        "ssm:ListDocuments"
      ],
      "Resource": [
        "arn:aws:ssm:us-east-1:111122223333:document/SessionDocument-*"
      ]
    }
  ]
}
```

Note

La console di Session Manager supporta solo i documenti di sessione che hanno un `sessionType` di `Standard_Stream` e che vengono utilizzati per definire le preferenze di sessione. Per ulteriori informazioni, consulta [Schema documento di sessione](#).

Esempio 2: limitare l'accesso a nodi gestiti specifici

È possibile creare una policy IAM che definisca a quali nodi gestiti un utente può connettersi utilizzando Session Manager. Ad esempio, la seguente policy concede a un utente il permesso di

avviare, terminare e riprendere le sessioni su tre nodi specifici. La policy impedisce all'utente di connettersi a nodi diversi da quelli specificati.

 Note

Per utenti federati, consulta [Esempio 4: consentire agli utenti di terminare solo le sessioni da essi avviate](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:StartSession"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/i-1234567890EXAMPLE",
        "arn:aws:ec2:us-east-1:111122223333:instance/i-abcdefghijEXAMPLE",
        "arn:aws:ec2:us-east-1:111122223333:instance/i-0e9d8c7b6aEXAMPLE",
        "arn:aws:ssm:us-east-1:111122223333:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Effect": "Allow",
      "Action": ["ssmmessages:OpenDataChannel"],
      "Resource": ["arn:aws:ssm:*:session/${aws:userid}-*"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:TerminateSession",
        "ssm:ResumeSession"
      ],
      "Resource": [
```

```

        "arn:aws:ssm:*:*:session/${aws:userid}-*"
    ],
    },
    {
        "Effect": "Allow",
        "Action": ["ssmmessages:OpenDataChannel"],
        "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
    }
]
}

```

Esempio 3: limitazione dell'accesso in base ai tag

Puoi limitare l'accesso ai nodi gestiti in base a tag specifici. Nell'esempio seguente, l'utente può avviare e riprendere le sessioni (Effect: Allow, Action: ssm:StartSession, ssm:ResumeSession) su qualsiasi nodo gestito (Resource: arn:aws:ec2:*region*:*987654321098*:instance/*) a condizione che il nodo sia un Finance WebServer (ssm:resourceTag/Finance: WebServer). Se l'utente invia un comando a un nodo gestito senza tag o con un tag diverso da Finance: WebServer, il risultato del comando includerà AccessDenied.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:StartSession"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
        "StringLike": {
          "ssm:resourceTag/Finance": [
            "WebServers"
          ]
        }
      }
    }
  ]
}

```

```

    },
    {
      "Effect": "Allow",
      "Action": ["ssmmessages:OpenDataChannel"],
      "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:TerminateSession",
        "ssm:ResumeSession"
      ],
      "Resource": [
        "arn:aws:ssm:*:*:session/${aws:userid}-*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:StartSession"
      ],
      "Resource": [
        "arn:aws:ssm:us-east-1:111122223333:document/SSM-
SessionManagerRunShell"
      ]
    }
  ]
}

```

Puoi creare policy IAM che permettono a un utente di avviare sessioni su nodi gestiti contrassegnati con più tag. La seguente policy consente all'utente di avviare sessioni su nodi gestiti a cui sono applicati entrambi i tag specificati. Se l'utente invia un comando a un nodo gestito non contrassegnato con questi due tag, il risultato del comando includerà `AccessDenied`.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",

```

```

    "Action": [
      "ssm:StartSession"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "ssm:resourceTag/tag-key1": [
          "tag-value1"
        ],
        "ssm:resourceTag/tag-key2": [
          "tag-value2"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": ["ssmmessages:OpenDataChannel"],
    "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
  },
  {
    "Effect": "Allow",
    "Action": [
      "ssm:StartSession"
    ],
    "Resource": [
      "arn:aws:ssm:us-east-1:111122223333:document/SSM-
SessionManagerRunShell"
    ]
  }
]
}

```

Per ulteriori informazioni sulla creazione di policy IAM, consulta la pagina [Policy gestite e policy inline](#) nella Guida per l'utente di IAM. Per ulteriori informazioni sull'applicazione di tag a nodi gestiti, consulta [Applicazione di tag a risorse Amazon EC2](#) nella Guida per l'utente di Amazon EC2 (il contenuto si applica ai nodi gestiti di Windows e Linux). Per ulteriori informazioni su come aumentare la posizione di sicurezza rispetto ai comandi non autorizzati a livello di root nei nodi gestiti, consulta [Limitare l'accesso ai comandi a livello di root tramite SSM Agent](#)

Esempio 4: consentire agli utenti di terminare solo le sessioni da essi avviate

Session Manager fornisce due metodi per controllare le sessioni che un utente Account AWS federato può terminare.

- Utilizza la variabile `{aws:userId}` in una politica di autorizzazioni AWS Identity and Access Management (IAM). Gli utenti federati possono terminare solo le sessioni da essi avviate. Per gli utenti non federati, utilizzare il Metodo 1. Per gli utenti federati, utilizzare il Metodo 2.
- Utilizza i tag forniti dai AWS tag in una policy di autorizzazioni IAM. Nella policy deve essere inclusa una condizione che consenta agli utenti di terminare solo le sessioni contrassegnate con tag specifici forniti da AWS. Questo metodo funziona per tutti gli account, inclusi quelli che utilizzano ID federati per concedere l'accesso a AWS.

Metodo 1: concedi `TerminateSession` i privilegi utilizzando la variabile `{aws:username}`

La policy IAM seguente consente a un utente di visualizzare gli ID di tutte le sessioni dell'account. Tuttavia, gli utenti possono interagire con i nodi gestiti solo attraverso le sessioni da loro avviate. Un utente a cui è assegnata la seguente policy non può terminare o connettersi alle sessioni di altri utenti. A tale scopo, la policy utilizza la variabile `{aws:username}`.

Note

Questo metodo non funziona per gli account che utilizzano ID federati per concedere l'accesso a AWS .

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ssm:DescribeSessions"
      ],
      "Effect": "Allow",
      "Resource": [
        "*"
      ]
    }
  ]
}
```

```
    },
    {
      "Action": [
        "ssm:TerminateSession"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:ssm:*:*:session/${aws:username}-*"
      ]
    }
  ]
}
```

Metodo 2: concedere TerminateSession i privilegi utilizzando i tag forniti da AWS

È possibile controllare le sessioni che un utente può terminare includendo variabili di chiave tag condizionali in una policy IAM. La condizione specifica che l'utente può terminare solo le sessioni che sono contrassegnate con una o entrambe queste specifiche variabili chiave tag e un valore specificato.

Quando un utente del tuo Account AWS avvia una sessione, Session Manager applica due tag di risorse alla sessione. Il primo tag risorsa è `aws:ssmmessages:target-id`, con il quale si specifica l'ID della destinazione che l'utente può terminare. L'altro tag risorsa è `aws:ssmmessages:session-id`, con un valore nel formato di *role-id:caller-specified-role-name*.

Note

Session Manager non supporta i tag personalizzati per questa policy di controllo dell'accesso IAM. È necessario utilizzare i tag di risorsa forniti da AWS, descritti di seguito.

aws:ssmmessages:target-id

Con questa chiave di tag, è possibile includere l'ID del nodo gestito come valore nella policy. Nel seguente blocco della policy, l'istruzione di condizione consente a un utente di terminare solo il nodo `i-02573cafcfEXAMPLE`.

JSON

```
{
```

```

    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "ssm:TerminateSession"
        ],
        "Resource": "*",
        "Condition": {
          "StringLike": {
            "ssm:resourceTag/aws:ssmmessages:target-id": [
              "i-02573cafcfEXAMPLE"
            ]
          }
        }
      }
    ]
  }
}

```

Se l'utente tenta di terminare una sessione per la quale non è stata concessa questa autorizzazione `TerminateSession`, viene visualizzato un errore `AccessDeniedException`.

aws:ssmmessages:session-id

Questa chiave tag include una variabile per l'ID di sessione come valore nella richiesta di avviare una sessione.

Nell'esempio seguente viene illustrata una policy per i casi in cui il tipo di chiamante è `User`. Il valore fornito per `aws:ssmmessages:session-id` è l'ID dell'utente. In questo esempio, `AIDI0DR4TAW7CSEXAMPLE` rappresenta l'ID di un utente nel tuo Account AWS. Per recuperare l'ID di un utente nel tuo Account AWS, usa il comando `IAM,get-user`. Per informazioni, consulta [get-user](#) nella AWS Identity and Access Management sezione della IAM User Guide.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:TerminateSession"
      ]
    }
  ]
}

```



```

    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "ssm:resourceTag/aws:ssmmessages:session-id": [
          "AIDI0DR4TAW7CSEXAMPLE"
        ]
      }
    }
  }
]
}

```

Nell'esempio seguente viene illustrata una policy per i casi in cui il tipo di chiamante è `AssumedRole`. Puoi utilizzare la variabile `{aws:userid}` per il valore da fornire per `aws:ssmmessages:session-id`. In alternativa, è possibile codificare un ID ruolo per il valore specificato per `aws:ssmmessages:session-id`. Se codifichi un ID ruolo, devi specificare il valore nel formato *role-id:caller-specified-role-name*. Ad esempio, `AIDI0DR4TAW7CSEXAMPLE:MyRole`.

Important

Per applicare i tag di sistema, l'ID del ruolo fornito può contenere solo i seguenti caratteri: lettere Unicode, 0-9, spazio, ,, ,, _ , . , , : / = , + e . - @ \

Per recuperare l'ID del ruolo per un ruolo nel tuo Account AWS, usa il comando `get-caller-identity`. Per informazioni, vedi [get-caller-identity](#) nel Command Reference. AWS CLI

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:TerminateSession"
      ],
      "Resource": "*"
    }
  ]
}

```

```

        "Condition": {
            "StringLike": {
                "ssm:resourceTag/aws:ssmmessages:session-id": [
                    "${aws:userid}*"
                ]
            }
        }
    }
}

```

Se un utente tenta di terminare una sessione per la quale non è stata concessa questa autorizzazione `TerminateSession`, viene visualizzato un errore `AccessDeniedException`.

aws:ssmmessages:target-id e aws:ssmmessages:session-id

È inoltre possibile creare policy IAM che permettono a un utente di terminare sessioni contrassegnate con entrambi i tag di sistema, come illustrato in questo esempio.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:TerminateSession"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ssm:resourceTag/aws:ssmmessages:target-id": [
            "i-02573cafcfEXAMPLE"
          ],
          "ssm:resourceTag/aws:ssmmessages:session-id": [
            "${aws:userid}*"
          ]
        }
      }
    }
  ]
}

```

Esempio 5: consentire l'accesso (amministrativo) completo a tutte le sessioni

La seguente policy IAM consente a un utente di interagire con tutti i nodi gestiti e tutte le sessioni create da tutti gli utenti per tutti i nodi. Dovrebbe essere concessa solo a un amministratore che ha bisogno del controllo completo sulle attività del Session Manager della tua organizzazione.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ssm:StartSession",
        "ssm:TerminateSession",
        "ssm:ResumeSession",
        "ssm:DescribeSessions",
        "ssm:GetConnectionStatus"
      ],
      "Effect": "Allow",
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": ["ssmmessages:OpenDataChannel"],
      "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
    }
  ]
}
```

Fase 4: configurazione delle preferenze delle sessioni

Gli utenti a cui sono state concesse le autorizzazioni amministrative nella propria policy AWS Identity and Access Management (IAM) possono configurare le preferenze di sessione, tra cui:

- Attiva il supporto Esegui come per i nodi gestiti Linux. In questo modo è possibile avviare sessioni utilizzando le credenziali di un utente del sistema operativo specificato anziché le credenziali di un `ssm-user` account generato dal sistema che è AWS Systems Manager Session Manager possibile creare su un nodo gestito.
- Configura Session Manager l'utilizzo della AWS KMS key crittografia per fornire una protezione aggiuntiva ai dati trasmessi tra le macchine client e i nodi gestiti.
- Configura Session Manager per creare e inviare i log della cronologia delle sessioni a un bucket Amazon Simple Storage Service (Amazon S3) o a un gruppo di log Amazon Logs. CloudWatch I dati di log archiviati si utilizzano quindi per fornire rapporti sulle connessioni di sessione effettuate ai nodi gestiti e sui comandi eseguiti su di esse durante le sessioni.
- Configura i timeout delle sessioni. È possibile utilizzare questa impostazione per specificare quando terminare una sessione dopo un periodo di inattività.
- Configura Session Manager per utilizzare profili di shell configurabili. Questi profili personalizzabili permettono di definire le preferenze all'interno di sessioni quali le preferenze della shell, le variabili di ambiente, le directory di lavoro ed eseguire più comandi all'avvio di una sessione.

Per ulteriori informazioni sulle autorizzazioni necessarie per configurare le preferenze di Session Manager, consulta [the section called “Concedere o negare a un utente le autorizzazioni per aggiornare le preferenze del Session Manager”](#).

Argomenti

- [Concedere o negare a un utente le autorizzazioni per aggiornare le preferenze del Session Manager](#)
- [Specificare un valore di timeout della sessione di inattività](#)
- [Specifica la durata massima della sessione](#)
- [Consenti profili shell configurabili](#)
- [Attiva il supporto Run As per Linux and macOS nodi gestiti](#)
- [Attiva la crittografia delle chiavi KMS per i dati delle sessioni \(console\)](#)
- [Creare un documento di preferenze di Session Manager \(riga di comando\)](#)
- [Aggiornamento delle preferenze Session Manager \(riga di comando\)](#)

Per informazioni sull'utilizzo della console di Systems Manager per configurare le opzioni per la registrazione dei dati di sessione, consulta i seguenti argomenti.

- [Registrazione dei dati delle sessioni mediante Amazon S3 \(console\)](#)
- [Streaming dei dati delle sessioni tramite Amazon CloudWatch Logs \(console\)](#)
- [Registrazione dei dati della sessione tramite Amazon CloudWatch Logs \(console\)](#)

Concedere o negare a un utente le autorizzazioni per aggiornare le preferenze del Session Manager

Le preferenze dell'account vengono archiviate come documenti AWS Systems Manager (SSM) per ciascuno Regione AWS di essi. Prima che un utente possa aggiornare le preferenze dell'account per le sessioni nel tuo account, deve disporre delle autorizzazioni necessarie per accedere al tipo di documento SSM in cui sono archiviate tali preferenze. Queste autorizzazioni vengono concesse tramite una policy AWS Identity and Access Management (IAM).

Policy di amministratore per consentire la creazione e l'aggiornamento delle preferenze

Un amministratore può disporre della seguente policy per creare e aggiornare le preferenze in qualsiasi momento. La seguente policy concede l'autorizzazione per accedere e aggiornare il documento SSM-SessionManagerRunShell nell'account us-east-2 123456789012.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ssm:CreateDocument",
        "ssm:GetDocument",
        "ssm:UpdateDocument",
        "ssm>DeleteDocument"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:ssm:us-east-1:111122223333:document/SSM-SessionManagerRunShell"
      ]
    }
  ]
}
```

Policy utente per impedire che le preferenze vengano aggiornate

Utilizza la seguente policy per impedire agli utenti finali nel tuo account di aggiornare o sostituire le preferenze del Session Manager.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ssm:CreateDocument",
        "ssm:GetDocument",
        "ssm:UpdateDocument",
        "ssm>DeleteDocument"
      ],
      "Effect": "Deny",
      "Resource": [
        "arn:aws:ssm:us-east-1:111122223333:document/SSM-SessionManagerRunShell"
      ]
    }
  ]
}
```

Specificare un valore di timeout della sessione di inattività

Con Session Manager, è possibile specificare il periodo di tempo per consentire a un utente di rimanere inattivo prima che il sistema termini una sessione. Per impostazione predefinita, le sessioni scadono dopo 20 minuti di inattività. È possibile modificare questa impostazione per specificare il timeout di una sessione tra 1 e 60 minuti di inattività. Alcune agenzie di sicurezza informatica professionali consigliano di impostare i timeout delle sessioni inattive su un massimo di 15 minuti.

Comprendere il comportamento del timeout di inattività

Il timer di timeout della sessione inattiva si azzerà quando riceve input dal lato client. Session Manager Questi input includono, a titolo esemplificativo ma non esaustivo:

- Inserimento da tastiera nel terminale

- Eventi di ridimensionamento della finestra del terminale o del browser
- Riconnessione della sessione (ResumeSession), che può verificarsi a causa di interruzioni della rete, gestione delle schede del browser o disconnessioni WebSocket

Poiché questi eventi azzerano il timer di inattività, una sessione potrebbe rimanere attiva più a lungo del periodo di timeout configurato anche senza comandi diretti da terminale.

Applicazione di limiti di sessione rigorosi

Se i tuoi requisiti di sicurezza impongono limiti rigorosi di durata della sessione indipendentemente dall'attività, utilizza l'impostazione Durata massima della sessione in aggiunta al timeout di inattività. Per ulteriori informazioni, consulta [the section called “Specifica la durata massima della sessione”](#).

Per consentire il timeout della sessione inattiva (console)

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Session Manager.
3. Scegli la scheda Preferenze, quindi seleziona Modifica.
4. Specificare il periodo di tempo necessario per consentire a un utente di rimanere inattivo prima che una sessione finisca nel campo minuti in tempo di inattività della sessione.
5. Scegli Save (Salva).

Specifica la durata massima della sessione

Con Session Manager, è possibile specificare la durata massima di una sessione prima che termini. Per impostazione predefinita, le sessioni non hanno una durata massima. Il valore specificato per la durata massima della sessione deve essere compreso tra 1 e 1.440 minuti.

Per specificare la durata massima della sessione (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Session Manager.
3. Scegli la scheda Preferenze, quindi seleziona Modifica.
4. Selezionare la casella di controllo accanto ad Abilita la durata massima della sessione.

5. Specificare la durata massima della sessione prima che finisca nel campo minuti sotto Durata massima sessione.
6. Scegli Save (Salva).

Consenti profili shell configurabili

Per impostazione predefinita, le sessioni sulle istanze EC2 per Linux iniziano utilizzando la shell Bourne (sh). Tuttavia, potresti usare un'altra shell come bash. Consentendo i profili di shell configurabili, è possibile personalizzare le preferenze all'interno di sessioni quali le preferenze della shell, le variabili di ambiente, le directory di lavoro ed eseguire più comandi all'avvio di una sessione.

Important

Systems Manager non controlla i comandi o gli script nel profilo della shell per vedere quali modifiche apporterebbero a un'istanza prima dell'esecuzione. Per limitare la capacità di un utente di modificare i comandi o gli script immessi nel profilo della shell, si consiglia quanto segue:

- Crea un Session-type documento personalizzato per i tuoi utenti e ruoli AWS Identity and Access Management (IAM). Quindi modifica la policy IAM per questi utenti e ruoli in modo che l'operazione StartSession API possa utilizzare solo il Session-type documento che hai creato per loro. Per informazioni, consulta [Creare un documento di preferenze di Session Manager \(riga di comando\)](#) e [Politiche Quickstart per gli utenti finali per Session Manager](#).
- Modifica la policy IAM per i tuoi utenti e ruoli IAM per negare l'accesso all'operazione UpdateDocument API per la risorsa Session-type documentale che crei. Ciò consente agli utenti e ai ruoli di utilizzare il documento creato per le preferenze di sessione senza consentire loro di modificare alcuna delle impostazioni.

Per attivare i profili di shell configurabili

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Session Manager.
3. Scegli la scheda Preferenze, quindi seleziona Modifica.

4. Specifica le variabili di ambiente, le preferenze della shell o i comandi che si desidera eseguire all'avvio della sessione nei campi relativi ai sistemi operativi applicabili.
5. Scegli Save (Salva).

Di seguito sono riportati alcuni comandi di esempio che possono essere aggiunti al profilo della shell.

Passa alla shell bash e passa alla directory /usr sulle istanze Linux.

```
exec /bin/bash
cd /usr
```

Invia un timestamp e un messaggio di benvenuto all'avvio di una sessione.

Linux & macOS

```
timestamp=$(date '+%Y-%m-%dT%H:%M:%SZ')
user=$(whoami)
echo $timestamp && echo "Welcome $user"!!'
echo "You have logged in to a production instance. Note that all session activity is
being logged."
```

Windows

```
$timestamp = (Get-Date).ToString("yyyy-MM-ddTH:mm:ssZ")
$splitName = (whoami).Split("\")
$user = $splitName[1]
Write-Host $timestamp
Write-Host "Welcome $user!"
Write-Host "You have logged in to a production instance. Note that all session
activity is being logged."
```

Visualizzare l'attività dinamica del sistema all'avvio di una sessione.

Linux & macOS

```
top
```

Windows

```
while ($true) { Get-Process | Sort-Object -Descending CPU | Select-Object -First 30;
,
Start-Sleep -Seconds 2; cls
Write-Host "Handles    NPM(K)      PM(K)          WS(K) VM(M)      CPU(s)      Id ProcessName";
Write-Host "-----    -"}
```

Attiva il supporto Run As per Linux and macOS nodi gestiti

Per impostazione predefinita, Session Manager autentica le connessioni utilizzando le credenziali di un account `ssm-user` generato dal sistema che viene creato su un nodo gestito. Su Linux e macOS macchine, questo account viene aggiunto a `/etc/sudoers/`. È invece possibile autenticare le sessioni utilizzando le credenziali di un account utente del sistema operativo o di un utente di dominio per le istanze aggiunte ad Active Directory. In questo caso, Session Manager verifica che l'account del sistema operativo esista nel nodo o nel dominio prima di iniziare la sessione. Se l'account del sistema operativo non esiste nel nodo o nel dominio, la connessione non riesce.

Note

Session Manager non supporta l'utilizzo di un account utente `root` del sistema operativo per autenticare le connessioni. Per le sessioni autenticate tramite un account utente del sistema operativo, le politiche del nodo OS-level e della directory, come le restrizioni di accesso o le restrizioni sull'utilizzo delle risorse di sistema, potrebbero non essere applicabili.

Come funziona

Se attivi il supporto Esegui come per le sessioni, il sistema controlla le autorizzazioni di accesso come segue:

1. Per l'utente che avvia la sessione, all'entità IAM (utente o ruolo) è stato assegnato il tag `SSMSessionRunAs = os user account name`?

Se Sì, il nome utente dell'OS esiste sul nodo gestito? In tal caso, avviare la sessione. In caso negativo, non consentire l'avvio di una sessione.

Se l'entità IAM non è stata contrassegnata con `SSMSessionRunAs = os user account name`, continua con il passaggio 2.

2. Se l'entità IAM non è stata contrassegnata con `SSMSessionRunAs = os user account name`, è stato specificato un nome utente Account AWS del sistema operativo nelle Session Manager preferenze?

Se Sì, il nome utente dell'OS esiste sul nodo gestito? In tal caso, avviare la sessione. In caso negativo, non consentire l'avvio di una sessione.

Note

Quando attivi il supporto Esegui come, esso impedisce a Session Manager di avviare sessioni utilizzando l'account `ssm-user` su un nodo gestito. Ciò significa che se Session Manager non riesce a connettersi utilizzando l'account utente del sistema operativo specificato, non ricorre alla connessione utilizzando il metodo predefinito.

Se attivi Esegui come senza specificare un account del sistema operativo o assegnare tag a un'entità IAM e non hai specificato un account del sistema operativo nelle preferenze di Session Manager, i tentativi di connessione alla sessione falliranno.

Per attivare il supporto Run As per Linux and macOS nodi gestiti

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Session Manager.
3. Scegli la scheda Preferenze, quindi seleziona Modifica.
4. Seleziona la casella di controllo accanto a Abilita supporto Esegui come per le istanze Linux.
5. Esegui una delle seguenti operazioni:
 - Opzione 1: nel campo Nome utente del sistema operativo, inserisci il nome dell'account utente del sistema operativo che desideri utilizzare per avviare le sessioni. Utilizzando questa opzione, tutte le sessioni vengono eseguite dallo stesso utente del sistema operativo per tutti gli utenti del tuo Account AWS che si connettono utilizzando Session Manager.
 - Opzione 2 (consigliata): scegli il collegamento Apri la console IAM. Nel riquadro di navigazione, scegli Utenti o Ruoli. Scegliere l'entità (utente o ruolo) cui aggiungere tag e quindi selezionare la scheda Tags (Tag). Inserire `SSMSessionRunAs` per il nome chiave. Inserisci il nome di un account utente del sistema operativo per il valore della chiave. Scegli Salva modifiche.

Utilizzando questa opzione, è possibile specificare utenti univoci dell'OS per diverse entità IAM, se lo desideri. Per ulteriori informazioni sull'applicazione di tag alle entità IAM (utenti o ruoli), consulta la pagina [Applicazione di tag alle risorse IAM](#) nella Guida per l'utente IAM.

Di seguito è riportato un esempio di :

Tags for 

Key	Value (optional)	Remove
<input type="text" value="SSMSessionRunAs"/>	<input type="text" value="My-OS-User-Name"/>	
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 49 more tags.

6. Scegli Save (Salva).

Attiva la crittografia delle chiavi KMS per i dati delle sessioni (console)

Usa AWS Key Management Service (AWS KMS) per creare e gestire le chiavi di crittografia. Con AWS KMS, puoi controllare l'uso della crittografia in un'ampia gamma di Servizi AWS e nelle tue applicazioni. È possibile specificare che i dati di sessione trasmessi tra i nodi gestiti e i computer locali degli utenti in uso siano crittografati utilizzando la Account AWS crittografia delle chiavi KMS. (Questo è in aggiunta al TLS 1.2/1.3 crittografia AWS già fornita per impostazione predefinita.) Per crittografare i dati Session Manager della sessione, crea una chiave KMS simmetrica utilizzando AWS KMS

AWS KMS la crittografia è disponibile per e tipi di Standard_Stream sessioneInteractiveCommands. NonInteractiveCommands Per utilizzare l'opzione per crittografare i dati della sessione utilizzando una chiave creata in AWS KMS, è AWS Systems Manager SSM Agent necessario installare la versione 2.3.539.0 o successiva nel nodo gestito.

 Note

È necessario consentire AWS KMS la crittografia per reimpostare le password sui nodi gestiti dalla console. AWS Systems Manager Per ulteriori informazioni, consulta [Reimpostazione di una password su un nodo gestito](#).

Puoi usare una chiave che hai creato nel tuo Account AWS. Inoltre, è possibile utilizzare una chiave che è stata creata in un account Account AWS diverso. Il creatore della chiave in un'altra Account AWS deve fornirti le autorizzazioni necessarie per utilizzare la chiave.

Dopo aver abilitato la crittografia delle chiavi KMS per i dati delle sessioni, gli utenti che avviano le sessioni e i nodi gestiti a cui si connettono devono entrambi disporre dell'autorizzazione per utilizzare la chiave. Fornisci l'autorizzazione per utilizzare la chiave KMS con politiche Session Manager Through AWS Identity and Access Management (IAM). Per informazioni, consultare gli argomenti seguenti:

- Aggiungi AWS KMS le autorizzazioni per gli utenti del tuo account: [Esempi di policy IAM per Session Manager](#)
- Aggiungi AWS KMS le autorizzazioni per i nodi gestiti nel tuo account: [Fase 2: Verifica o aggiungi le autorizzazioni delle istanze per Session Manager](#)

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

Per informazioni sull'utilizzo di AWS CLI per attivare la crittografia con chiave KMS dei dati di sessione nel tuo account, consulta [Creare un documento di preferenze di Session Manager \(riga di comando\)](#) o [Aggiornamento delle preferenze Session Manager \(riga di comando\)](#)

 Note

C'è un addebito per l'utilizzo delle chiavi KMS. Per informazioni, consulta [Prezzi di AWS Key Management Service](#).

Attivare la crittografia delle chiavi KMS per i dati delle sessioni (console)

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Session Manager.
3. Scegli la scheda Preferenze, quindi seleziona Modifica.
4. Selezionare la casella di controllo accanto ad Abilita la crittografia KMS.
5. Esegui una delle seguenti operazioni:
 - Scegliere il pulsante accanto a Seleziona una chiave KMS nel mio account corrente, quindi seleziona una chiave dall'elenco.

oppure

Scegliere il pulsante accanto a Enter a KMS key alias or KMS key ARN (Immetti un alias della chiave o un ARN della chiave KMS). Immettere manualmente un alias della chiave KMS per una chiave creata nell'account corrente o immettere l'Amazon Resource Name (ARN) della chiave per una chiave in un altro account. Di seguito vengono mostrati gli esempi:

- Alias della chiave: `alias/my-kms-key-alias`
- ARN della chiave: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-12345EXAMPLE`

oppure

Scegli Crea nuova chiave per creare una nuova KMS nel tuo account. Una volta creata la nuova chiave, torna alla scheda Preferenze e seleziona la chiave per crittografare i dati della sessione nel tuo account.

Per ulteriori informazioni sulla condivisione delle chiavi, consulta [Consentire l'accesso Account AWS a una chiave da parte di un esterno](#) nella Guida per gli AWS Key Management Service sviluppatori.

6. Scegli Save (Salva).

Creare un documento di preferenze di Session Manager (riga di comando)

Utilizza la seguente procedura per creare documenti SSM che definiscono le tue preferenze per le sessioni. AWS Systems Manager Session Manager Puoi utilizzare il documento per configurare

le opzioni della sessione, tra cui la crittografia dei dati, la durata della sessione e la registrazione. Ad esempio, puoi specificare se archiviare i dati di log della sessione in un bucket Amazon Simple Storage Service (Amazon S3) o in un gruppo di log Amazon CloudWatch Logs. Puoi creare documenti che definiscono le preferenze generali per tutte le sessioni per un Account AWS and Regione AWS o che definiscono le preferenze per le singole sessioni.

Note

Puoi inoltre configurare le preferenze generali di sessione utilizzando la console di Session Manager.

I documenti utilizzati per impostare le preferenze di Session Manager devono avere un `sessionType` di `Standard_Stream`. Per ulteriori informazioni sui documenti di sessione, consulta [the section called “Schema documento di sessione”](#).

Per informazioni sull'utilizzo della riga di comando per aggiornare le preferenze Session Manager esistenti, consulta [Aggiornamento delle preferenze Session Manager \(riga di comando\)](#).

Per un esempio di come creare preferenze di sessione utilizzando CloudFormation, vedere [Create a Systems Manager document for Session Manager preferences](#) nella Guida per l'AWS CloudFormation utente.

Note

Questa procedura descrive come creare documenti per impostare Session Manager le preferenze a Account AWS livello. Per creare documenti che verranno utilizzati per impostare le preferenze a livello di sessione, specifica un valore diverso da `SSM-SessionManagerRunShell` per il nome file relativo agli input dei comandi. Per utilizzare il documento per impostare le preferenze per le sessioni avviate dalla AWS Command Line Interface (AWS CLI), fornisci il nome del documento come valore del parametro `--document-name`. Per impostare le preferenze per le sessioni avviate dalla console di Session Manager, puoi digitare o selezionare il nome del documento da un elenco.

Per creare preferenze Session Manager (riga di comando)

1. Sul proprio computer locale creare un file JSON denominato ad esempio `SessionManagerRunShell.json`, quindi incollarvi i seguenti contenuti:

```
{
  "schemaVersion": "1.0",
  "description": "Document to hold regional settings for Session Manager",
  "sessionType": "Standard_Stream",
  "inputs": {
    "s3BucketName": "",
    "s3KeyPrefix": "",
    "s3EncryptionEnabled": true,
    "cloudWatchLogGroupName": "",
    "cloudWatchEncryptionEnabled": true,
    "cloudWatchStreamingEnabled": false,
    "kmsKeyId": "",
    "runAsEnabled": false,
    "runAsDefaultUser": "",
    "idleSessionTimeout": "",
    "maxSessionDuration": "",
    "shellProfile": {
      "windows": "date",
      "linux": "pwd;ls"
    }
  }
}
```

Puoi anche passare i valori alle preferenze delle sessioni utilizzando i parametri invece di codificare i valori come illustrato nell'esempio seguente.

```
{
  "schemaVersion": "1.0",
  "description": "Session Document Parameter Example JSON Template",
  "sessionType": "Standard_Stream",
  "parameters": {
    "s3BucketName": {
      "type": "String",
      "default": ""
    },
    "s3KeyPrefix": {
      "type": "String",
      "default": ""
    },
    "s3EncryptionEnabled": {
      "type": "Boolean",
      "default": "false"
    }
  }
}
```



```

    },
    "cloudWatchLogGroupName":{
      "type":"String",
      "default":""
    },
    "cloudWatchEncryptionEnabled":{
      "type":"Boolean",
      "default":"false"
    }
  },
  "inputs":{
    "s3BucketName":"{{s3BucketName}}",
    "s3KeyPrefix":"{{s3KeyPrefix}}",
    "s3EncryptionEnabled":"{{s3EncryptionEnabled}}",
    "cloudWatchLogGroupName":"{{cloudWatchLogGroupName}}",
    "cloudWatchEncryptionEnabled":"{{cloudWatchEncryptionEnabled}}",
    "kmsKeyId":""
  }
}

```

2. Specificare dove inviare i dati delle sessioni. È possibile specificare un nome di bucket S3 (con un prefisso opzionale) o un nome di gruppo di CloudWatch log Logs. Per crittografare ulteriormente i dati tra client locale e i nodi gestiti, fornisci la chiave KMS da utilizzare per la crittografia. Di seguito è riportato un esempio di :

```

{
  "schemaVersion": "1.0",
  "description": "Document to hold regional settings for Session Manager",
  "sessionType": "Standard_Stream",
  "inputs": {
    "s3BucketName": "amzn-s3-demo-bucket",
    "s3KeyPrefix": "MyS3Prefix",
    "s3EncryptionEnabled": true,
    "cloudWatchLogGroupName": "MyLogGroupName",
    "cloudWatchEncryptionEnabled": true,
    "cloudWatchStreamingEnabled": false,
    "kmsKeyId": "MyKMSKeyID",
    "runAsEnabled": true,
    "runAsDefaultUser": "MyDefaultRunAsUser",
    "idleSessionTimeout": "20",
    "maxSessionDuration": "60",
    "shellProfile": {
      "windows": "MyCommands",

```

```
    "linux": "MyCommands"  
  }  
}  
}
```

Note

Se non si desidera crittografare i dati di log della sessione, modifica `true` in `false` per `s3EncryptionEnabled`.

Se non invii log a un bucket Amazon S3 o a CloudWatch un gruppo di log Logs, non desideri crittografare i dati delle sessioni attive o non desideri attivare il supporto RunAs per le sessioni del tuo account, puoi eliminare le righe relative a tali opzioni. Assicurarsi che l'ultima riga nella sezione `inputs` non termini con una virgola.

Se si aggiunge un ID della chiave KMS per crittografare i dati della sessione, gli utenti che avviano le sessioni e i nodi gestiti a cui si collegano devono entrambi disporre dell'autorizzazione per utilizzare la chiave. Fornire l'autorizzazione a utilizzare la chiave KMS con il Session Manager tramite le policy IAM. Per informazioni, consultare gli argomenti seguenti:

- Aggiungi le AWS KMS autorizzazioni per gli utenti del tuo account: [Esempi di policy IAM per Session Manager](#)
- Aggiungi AWS KMS le autorizzazioni per i nodi gestiti nel tuo account: [Fase 2: Verifica o aggiungi le autorizzazioni delle istanze per Session Manager](#)

3. Salvare il file.
4. Nella directory in cui è stato creato il file JSON, eseguire il comando seguente.

Linux & macOS

```
aws ssm create-document \  
  --name SSM-SessionManagerRunShell \  
  --content "file:///SessionManagerRunShell.json" \  
  --document-type "Session" \  
  --document-format JSON
```

Windows

```
aws ssm create-document ^  
  --name SSM-SessionManagerRunShell ^
```

```
--content "file://SessionManagerRunShell.json" ^  
--document-type "Session" ^  
--document-format JSON
```

PowerShell

```
New-SSMDocument `   
-Name "SSM-SessionManagerRunShell" `   
-Content (Get-Content -Raw SessionManagerRunShell.json) `   
-DocumentType "Session" `   
-DocumentFormat JSON
```

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente:

```
{  
  "DocumentDescription": {  
    "Status": "Creating",  
    "Hash": "ce4fd0a2ab9b0fae759004ba603174c3ec2231f21a81db8690a33eb66EXAMPLE",  
    "Name": "SSM-SessionManagerRunShell",  
    "Tags": [],  
    "DocumentType": "Session",  
    "PlatformTypes": [  
      "Windows",  
      "Linux"  
    ],  
    "DocumentVersion": "1",  
    "HashType": "Sha256",  
    "CreateDate": 1547750660.918,  
    "Owner": "111122223333",  
    "SchemaVersion": "1.0",  
    "DefaultVersion": "1",  
    "DocumentFormat": "JSON",  
    "LatestVersion": "1"  
  }  
}
```

Aggiornamento delle preferenze Session Manager (riga di comando)

La procedura seguente descrive come utilizzare lo strumento da riga di comando preferito per apportare modifiche alle AWS Systems Manager Session Manager preferenze del gruppo selezionato

Regione AWS. Account AWS Utilizza Session Manager le preferenze per specificare le opzioni per la registrazione dei dati della sessione in un bucket Amazon Simple Storage Service (Amazon S3) o in un gruppo di log Amazon Logs. CloudWatch Puoi anche utilizzare le preferenze del Session Manager per crittografare i dati delle sessioni.

Per aggiornare le preferenze Session Manager (riga di comando)

1. Sul proprio computer locale creare un file JSON denominato ad esempio `SessionManagerRunShell.json`, quindi incollarvi i seguenti contenuti.

```
{
  "schemaVersion": "1.0",
  "description": "Document to hold regional settings for Session Manager",
  "sessionType": "Standard_Stream",
  "inputs": {
    "s3BucketName": "",
    "s3KeyPrefix": "",
    "s3EncryptionEnabled": true,
    "cloudWatchLogGroupName": "",
    "cloudWatchEncryptionEnabled": true,
    "cloudWatchStreamingEnabled": false,
    "kmsKeyId": "",
    "runAsEnabled": true,
    "runAsDefaultUser": "",
    "idleSessionTimeout": "",
    "maxSessionDuration": "",
    "shellProfile": {
      "windows": "date",
      "linux": "pwd;ls"
    }
  }
}
```

2. Specificare dove inviare i dati delle sessioni. Puoi specificare un nome di bucket S3 (con un prefisso opzionale) o un nome di gruppo di log Logs. CloudWatch Se desideri crittografare ulteriormente i dati tra client locale e nodi gestiti, fornisci il codice da utilizzare per la AWS KMS key crittografia. Di seguito è riportato un esempio di :

```
{
  "schemaVersion": "1.0",
  "description": "Document to hold regional settings for Session Manager",
  "sessionType": "Standard_Stream",
```

```
"inputs": {
  "s3BucketName": "amzn-s3-demo-bucket",
  "s3KeyPrefix": "MyS3Prefix",
  "s3EncryptionEnabled": true,
  "cloudWatchLogGroupName": "MyLogGroupName",
  "cloudWatchEncryptionEnabled": true,
  "cloudWatchStreamingEnabled": false,
  "kmsKeyId": "MyKMSKeyID",
  "runAsEnabled": true,
  "runAsDefaultUser": "MyDefaultRunAsUser",
  "idleSessionTimeout": "20",
  "maxSessionDuration": "60",
  "shellProfile": {
    "windows": "MyCommands",
    "linux": "MyCommands"
  }
}
```

Note

Se non si desidera crittografare i dati di log della sessione, modifica `true` in `false` per `s3EncryptionEnabled`.

Se non invii log a un bucket Amazon S3 o a CloudWatch un gruppo di log Logs, non desideri crittografare i dati delle sessioni attive o non desideri attivare il supporto RunAs per le sessioni del tuo account, puoi eliminare le righe relative a tali opzioni. Assicurarsi che l'ultima riga nella sezione `inputs` non termini con una virgola.

Se si aggiunge un ID della chiave KMS per crittografare i dati della sessione, gli utenti che avviano le sessioni e i nodi gestiti a cui si collegano devono entrambi disporre dell'autorizzazione per utilizzare la chiave. Fornisci l'autorizzazione a utilizzare la chiave KMS tramite policy (IAM). Session Manager AWS Identity and Access Management Per informazioni, consultare gli argomenti seguenti:

- Aggiungi AWS KMS le autorizzazioni per gli utenti del tuo account: [Esempi di policy IAM per Session Manager](#)
- Aggiungi AWS KMS le autorizzazioni per i nodi gestiti nel tuo account: [Fase 2: Verifica o aggiungi le autorizzazioni delle istanze per Session Manager](#)

3. Salvare il file.

4. Nella directory in cui è stato creato il file JSON, eseguire il comando seguente.

Linux & macOS

```
aws ssm update-document \  
  --name "SSM-SessionManagerRunShell" \  
  --content "file:///SessionManagerRunShell.json" \  
  --document-version "$LATEST"
```

Windows

```
aws ssm update-document ^  
  --name "SSM-SessionManagerRunShell" ^  
  --content "file:///SessionManagerRunShell.json" ^  
  --document-version "$LATEST"
```

PowerShell

```
Update-SSMDocument `   
  -Name "SSM-SessionManagerRunShell" `   
  -Content (Get-Content -Raw SessionManagerRunShell.json) `   
  -DocumentVersion '$LATEST'
```

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente:

```
{  
  "DocumentDescription": {  
    "Status": "Updating",  
    "Hash": "ce4fd0a2ab9b0fae759004ba603174c3ec2231f21a81db8690a33eb66EXAMPLE",  
    "Name": "SSM-SessionManagerRunShell",  
    "Tags": [],  
    "DocumentType": "Session",  
    "PlatformTypes": [  
      "Windows",  
      "Linux"  
    ],  
    "DocumentVersion": "2",  
    "HashType": "Sha256",  
    "CreateDate": 1537206341.565,  
    "Owner": "111122223333",  
    "SchemaVersion": "1.0",
```

```
    "DefaultVersion": "1",  
    "DocumentFormat": "JSON",  
    "LatestVersion": "2"  
  }  
}
```

Fase 5: (facoltativo) limitazione dell'accesso ai comandi in una sessione

È possibile limitare i comandi che un utente può eseguire in una AWS Systems Manager Session Manager sessione utilizzando un documento Session di tipo personalizzato AWS Systems Manager (SSM). Nel documento, puoi definire il comando che viene eseguito quando l'utente avvia una sessione e i parametri che l'utente può fornire al comando. Il documento Session schemaVersion deve essere 1.0 e il sessionType del documento deve essere InteractiveCommands. Puoi quindi creare policy AWS Identity and Access Management (IAM) che consentano agli utenti di accedere solo ai documenti Session definiti. Per ulteriori informazioni sull'utilizzo delle policy IAM per limitare l'accesso ai comandi in una sessione, consulta [Esempi di policy IAM per comandi interattivi](#).

I documenti con sessionType of InteractiveCommands sono supportati solo per le sessioni iniziate da AWS Command Line Interface (AWS CLI). L'utente fornisce il nome del documento personalizzato come valore del parametro `--document-name` e specifica tutti i valori dei parametri del comando utilizzando l'opzione `--parameters`. Per ulteriori informazioni sull'esecuzione di comandi interattivi, consulta [Avvio di una sessione \(comandi interattivi e non interattivi\)](#).

Utilizza la procedura seguente per creare un documento SSM di tipo Session personalizzato che definisce il comando che un utente può eseguire.

Limitare l'accesso ai comandi in una sessione (console)

Per limitare i comandi che un utente può eseguire in una sessione Session Manager (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Documenti.
3. Scegli Crea comando o sessione.
4. Per Nome, inserisci un nome descrittivo per il documento.
5. Per Tipo di documento, scegli Documento di sessione.

6. Immettere il contenuto del documento che definisce il comando che un utente può eseguire in una sessione Session Manager utilizzando JSON o YAML, come illustrato nell'esempio seguente.

YAML

```
---
schemaVersion: '1.0'
description: Document to view a log file on a Linux instance
sessionType: InteractiveCommands
parameters:
  logpath:
    type: String
    description: The log file path to read.
    default: "/var/log/amazon/ssm/amazon-ssm-agent.log"
    allowedPattern: "^[a-zA-Z0-9-_/]+(.log)$"
properties:
  linux:
    commands: "tail -f {{ logpath }}"
    runAsElevated: true
```

JSON

```
{
  "schemaVersion": "1.0",
  "description": "Document to view a log file on a Linux instance",
  "sessionType": "InteractiveCommands",
  "parameters": {
    "logpath": {
      "type": "String",
      "description": "The log file path to read.",
      "default": "/var/log/amazon/ssm/amazon-ssm-agent.log",
      "allowedPattern": "^[a-zA-Z0-9-_/]+(.log)$"
    }
  },
  "properties": {
    "linux": {
      "commands": "tail -f {{ logpath }}",
      "runAsElevated": true
    }
  }
}
```


7. Scegli Crea documento.

Limitare l'accesso ai comandi in una sessione (riga di comando)

Prima di iniziare

Se non l'hai già fatto, installa e configura AWS Command Line Interface (AWS CLI) o AWS Strumenti per PowerShell. Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

Per limitare i comandi che un utente può eseguire in una sessione Session Manager (riga di comando)

1. Creare un file JSON o YAML per il contenuto del documento che definisce il comando che un utente può eseguire in una sessione Session Manager, come illustrato nell'esempio seguente.

YAML

```
---
schemaVersion: '1.0'
description: Document to view a log file on a Linux instance
sessionType: InteractiveCommands
parameters:
  logpath:
    type: String
    description: The log file path to read.
    default: "/var/log/amazon/ssm/amazon-ssm-agent.log"
    allowedPattern: "^[a-zA-Z0-9-_/]+(.log)$"
properties:
  linux:
    commands: "tail -f {{ logpath }}"
    runAsElevated: true
```

JSON

```
{
  "schemaVersion": "1.0",
  "description": "Document to view a log file on a Linux instance",
  "sessionType": "InteractiveCommands",
  "parameters": {
    "logpath": {
      "type": "String",
```

```

        "description": "The log file path to read.",
        "default": "/var/log/amazon/ssm/amazon-ssm-agent.log",
        "allowedPattern": "^[a-zA-Z0-9-_]+(.log)$"
    },
    "properties": {
        "linux": {
            "commands": "tail -f {{ logpath }}",
            "runAsElevated": true
        }
    }
}

```

2. Eseguire i comandi seguenti per creare un documento SSM utilizzando il contenuto che definisce il comando che un utente può eseguire in una sessione Session Manager.

Linux & macOS

```

aws ssm create-document \
  --content file://path/to/file/documentContent.json \
  --name "exampleAllowedSessionDocument" \
  --document-type "Session"

```

Windows

```

aws ssm create-document ^
  --content file://C:\path\to\file\documentContent.json ^
  --name "exampleAllowedSessionDocument" ^
  --document-type "Session"

```

PowerShell

```

$json = Get-Content -Path "C:\path\to\file\documentContent.json" | Out-String
New-SSMDocument `
  -Content $json `
  -Name "exampleAllowedSessionDocument" `
  -DocumentType "Session"

```

Parametri di comando interattivi e AWS CLI

È possibile fornire parametri di comando interattivi quando si utilizza la AWS CLI. A seconda del sistema operativo (OS) del computer client utilizzato per la connessione ai nodi gestiti con AWS CLI, la sintassi fornita per i comandi che contengono caratteri speciali o di escape potrebbe essere diversa. Gli esempi seguenti mostrano alcuni dei diversi modi in cui è possibile fornire i parametri di comando quando si AWS CLI utilizza e come gestire caratteri speciali o di escape.

Parameter Store È possibile fare riferimento ai parametri memorizzati in nei parametri del AWS CLI comando, come illustrato nell'esempio seguente.

Linux & macOS

```
aws ssm start-session \  
  --target instance-id \  
  --document-name MyInteractiveCommandDocument \  
  --parameters '{"command":["{{ssm:mycommand}}"]}'
```

Windows

```
aws ssm start-session ^  
  --target instance-id ^  
  --document-name MyInteractiveCommandDocument ^  
  --parameters '{"command":["{{ssm:mycommand}}"]}'
```

L'esempio seguente mostra come puoi utilizzare una sintassi abbreviata con la AWS CLI per passare i parametri.

Linux & macOS

```
aws ssm start-session \  
  --target instance-id \  
  --document-name MyInteractiveCommandDocument \  
  --parameters command="ifconfig"
```

Windows

```
aws ssm start-session ^  
  --target instance-id ^  
  --document-name MyInteractiveCommandDocument ^
```

```
--parameters command="ipconfig"
```

Puoi anche fornire parametri facoltativi in JSON , come mostrato nel seguente esempio.

Linux & macOS

```
aws ssm start-session \  
  --target instance-id \  
  --document-name MyInteractiveCommandDocument \  
  --parameters '{"command":["ifconfig"]}'
```

Windows

```
aws ssm start-session ^  
  --target instance-id ^  
  --document-name MyInteractiveCommandDocument ^  
  --parameters '{"command":["ipconfig"]}'
```

I parametri possono anche essere memorizzati in un file JSON e forniti AWS CLI come illustrato nell'esempio seguente. Per ulteriori informazioni sull'utilizzo di parametri AWS CLI da un file, consulta [Caricamento di parametri AWS CLI da un file](#) nella Guida per l'utente di AWS Command Line Interface .

```
{  
  "command": [  
    "my command"  
  ]  
}
```

Linux & macOS

```
aws ssm start-session \  
  --target instance-id \  
  --document-name MyInteractiveCommandDocument \  
  --parameters file://complete/path/to/file/parameters.json
```

Windows

```
aws ssm start-session ^
```

```
--target instance-id ^
--document-name MyInteractiveCommandDocument ^
--parameters file://complete/path/to/file/parameters.json
```

È inoltre possibile generare AWS CLI uno scheletro da un file di input JSON, come illustrato nell'esempio seguente. Per ulteriori informazioni sulla generazione di AWS CLI scheletri da file di input JSON, consulta [Generazione di AWS CLI scheletri e parametri di input da un file di input JSON o YAML](#) nella Guida per l'utente AWS Command Line Interface

```
{
  "Target": "instance-id",
  "DocumentName": "MyInteractiveCommandDocument",
  "Parameters": {
    "command": [
      "my command"
    ]
  }
}
```

Linux & macOS

```
aws ssm start-session \
  --cli-input-json file://complete/path/to/file/parameters.json
```

Windows

```
aws ssm start-session ^
  --cli-input-json file://complete/path/to/file/parameters.json
```

Per eseguire l'escape dei caratteri all'interno delle virgolette, è necessario aggiungere ulteriori barre rovesciate ai caratteri di escape, come illustrato nell'esempio seguente.

Linux & macOS

```
aws ssm start-session \
  --target instance-id \
  --document-name MyInteractiveCommandDocument \
  --parameters '{"command":["printf \"abc\\\\\\\\tdef\\\""]}'
```

Windows

```
aws ssm start-session ^  
  --target instance-id ^  
  --document-name MyInteractiveCommandDocument ^  
  --parameters '{"command":["printf \\\"abc\\\\\\\\\\tdef\\\""]}'
```

Per ulteriori informazioni sulla citazione con parametri di comando nella AWS CLI, consulta [Utilizzo di virgolette con stringhe nella AWS CLI](#) nella Guida per l'utente della AWS Command Line Interface .

Esempi di policy IAM per comandi interattivi

Puoi creare policy IAM che consentono agli utenti di accedere solo ai documenti Session definiti. Ciò limita i comandi che un utente può eseguire in una sessione Session Manager ai soli comandi definiti nei documenti SSM di tipo Session personalizzati.

Consentire a un utente di eseguire un comando interattivo su un singolo nodo

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "ssm:StartSession",  
      "Resource": [  
        "arn:aws:ec2:us-east-1:444455556666:instance/i-02573cafcfEXAMPLE",  
        "arn:aws:ssm:us-east-1:444455556666:document/allowed-session-  
document"  
      ]  
    },  
    {  
      "Effect": "Allow",  
      "Action": ["ssmmessages:OpenDataChannel"],  
      "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]  
    }  
  ]  
}
```

Consentire a un utente di eseguire un comando interattivo su tutti i nodi gestiti

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ssm:StartSession",
      "Resource": [
        "arn:aws:ec2:us-east-1:444455556666:instance/*",
        "arn:aws:ssm:us-east-1:444455556666:document/allowed-session-  
document"
      ]
    },
    {
      "Effect": "Allow",
      "Action": ["ssmmessages:OpenDataChannel"],
      "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
    }
  ]
}
```

Consentire a un utente di eseguire più comandi interattivi su tutti i nodi gestiti

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ssm:StartSession",
      "Resource": [
        "arn:aws:ec2:us-east-1:444455556666:instance/*",
        "arn:aws:ssm:us-east-1:444455556666:document/allowed-session-  
document",
        "arn:aws:ssm:us-east-1:444455556666:document/allowed-session-  
document-2"
      ]
    },
    {
      "Effect": "Allow",
```

```
    "Action": ["ssmmessages:OpenDataChannel"],
    "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
  }
]
```

Fase 6: (Facoltativo) Uso AWS PrivateLink per configurare un endpoint VPC per Session Manager

È possibile migliorare ulteriormente la posizione di sicurezza dei tuoi nodi gestiti configurando AWS Systems Manager in modo che utilizzi un endpoint di interfaccia di cloud privato virtuale (VPC) (VPC). Gli endpoint di interfaccia sono alimentati da AWS PrivateLink, una tecnologia che consente di accedere privatamente alle API Amazon Elastic Compute Cloud (Amazon EC2) e Systems Manager utilizzando indirizzi IP privati.

AWS PrivateLink limita tutto il traffico di rete tra i nodi gestiti, Systems Manager e Amazon EC2 alla rete Amazon. (I nodi gestiti non hanno accesso a Internet.) Inoltre, non hai bisogno di un gateway Internet, di un dispositivo NAT o di un gateway privato virtuale.

Per informazioni su come creare un endpoint VPC, consulta [Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager](#).

L'alternativa all'utilizzo di un endpoint VPC è l'abilitazione dell'accesso a Internet in uscita sui nodi gestiti. In questo caso, i nodi gestiti devono permettere anche il traffico in uscita HTTPS (porta 443) verso i seguenti endpoint:

- `ec2messages.region.amazonaws.com`
- `ssm.region.amazonaws.com`
- `ssmmessages.region.amazonaws.com`

Systems Manager utilizza l'ultimo di questi endpoint, `ssmmessages.region.amazonaws.com` per effettuare chiamate da SSM Agent al servizio Session Manager nel cloud.

Per utilizzare funzionalità opzionali come la crittografia AWS Key Management Service (AWS KMS), lo streaming di CloudWatch log su Amazon Logs (CloudWatch Logs) e l'invio di log ad Amazon Simple Storage Service (Amazon S3), devi consentire il traffico in uscita HTTPS (porta 443) verso i seguenti endpoint:

- `kms.region.amazonaws.com`

- `logs.region.amazonaws.com`
- `s3.region.amazonaws.com`

Per ulteriori informazioni sugli endpoint richiesti per Systems Manager, consultare [Referenza: ec2messages, ssmmessages e altre operazioni API](#).

Fase 7 (facoltativo): abilitazione o disabilitazione delle autorizzazioni amministrative dell'account ssm-account

A partire dalla versione 2.3.50.0 di AWS Systems Manager SSM Agent, l'agente crea un account utente locale chiamato `ssm-user` e lo aggiunge a `/etc/sudoers` (Linux e macOS) o al gruppo Administrators (). Windows Nelle versioni dell'agente precedenti alla 2.3.612.0, l'account viene creato la prima volta che SSM Agent viene avviato o riavviato dopo l'installazione. Nella versione 2.3.612.0 e successive, l'account `ssm-user` viene creato la prima volta che una sessione viene avviata su un nodo. Si `ssm-user` tratta dell'utente predefinito del sistema operativo (OS) all'avvio di una AWS Systems Manager Session Manager sessione. SSM Agent la versione 2.3.612.0 è stata rilasciata l'8 maggio 2019.

Se desideri impedire agli utenti Session Manager di eseguire comandi amministrativi su un nodo, puoi aggiornare le autorizzazioni dell'account `ssm-user`. Puoi anche ripristinare queste autorizzazioni dopo che sono state rimosse.

Argomenti

- [Gestione delle autorizzazioni sudo per l'account ssm-user su Linux e macOS](#)
- [Gestione delle autorizzazioni di amministratore per l'account ssm-user su Windows Server](#)

Gestione delle autorizzazioni sudo per l'account ssm-user su Linux e macOS

Utilizza una delle seguenti procedure per abilitare o disabilitare le autorizzazioni sudo per l'account `ssm-user` sui nodi gestiti Linux e macOS.

Utilizza Run Command per modificare le autorizzazioni sudo di `ssm-user` (console)

- Utilizza la procedura descritta in [Esecuzione di comandi dalla console](#) con i seguenti valori:
 - Per Documenti di comando, scegli `AWS-RunShellScript`.
 - Per rimuovere l'accesso sudo, nell'area Parametri di comando, incolla quanto segue nella casella Comandi.

```
cd /etc/sudoers.d
echo "#User rules for ssm-user" > ssm-agent-users
```

oppure

Per ripristinare l'accesso sudo, nell'area Parametri di comando, incolla quanto segue nella casella Comandi.

```
cd /etc/sudoers.d
echo "ssm-user ALL=(ALL) NOPASSWD:ALL" > ssm-agent-users
```

Utilizza la riga di comando per modificare le autorizzazioni sudo di ssm-user (AWS CLI)

1. Connettersi al nodo master ed eseguire il comando seguente.

```
sudo -s
```

2. Cambiare la directory di lavoro utilizzando il comando seguente.

```
cd /etc/sudoers.d
```

3. Aprire il file denominato `ssm-agent-users` per la modifica.
4. Per rimuovere l'accesso sudo, eliminare la riga seguente.

```
ssm-user ALL=(ALL) NOPASSWD:ALL
```

oppure

Per ripristinare l'accesso sudo, aggiungere la riga seguente.

```
ssm-user ALL=(ALL) NOPASSWD:ALL
```

5. Salvare il file.

Gestione delle autorizzazioni di amministratore per l'account ssm-user su Windows Server

Utilizza una delle seguenti procedure per abilitare o disabilitare le autorizzazioni di amministratore per l'account ssm-user sui nodi gestiti Windows Server:

Utilizza Run Command per modificare le autorizzazioni di amministratore (console)

- Utilizza la procedura descritta in [Esecuzione di comandi dalla console](#) con i seguenti valori:

Per Documenti di comando, scegli `AWS-RunPowerShellScript`.

Per rimuovere l'accesso amministrativo, nell'area Parametri di comando, incolla quanto segue nella casella Comandi.

```
net localgroup "Administrators" "ssm-user" /delete
```

oppure

Per ripristinare l'accesso amministrativo, nell'area Parametri di comando, incolla quanto segue nella casella Comandi.

```
net localgroup "Administrators" "ssm-user" /add
```

Utilizza PowerShell o la finestra del prompt dei comandi per modificare le autorizzazioni di amministratore

- Connettiti al nodo gestito e apri PowerShell o la finestra del prompt dei comandi.
- Per rimuovere l'accesso amministrativo, eseguire il comando riportato di seguito.

```
net localgroup "Administrators" "ssm-user" /delete
```

oppure

Per ripristinare l'accesso amministrativo, eseguire il comando riportato di seguito.

```
net localgroup "Administrators" "ssm-user" /add
```

Utilizza la console Windows per modificare le autorizzazioni di amministratore

- Connettiti al nodo gestito e apri PowerShell o la finestra del prompt dei comandi.
- Dalla riga di comando, esegui `lusrmgr.msc` per aprire la console Utenti e gruppi locali.
- Apri la directory Utenti, quindi apri `ssm-user`.

4. Nella scheda **Membro di**, esegui una delle seguenti operazioni:

- Per rimuovere l'accesso amministrativo, seleziona **Amministratori**, quindi scegli **Rimuovi**.

oppure

Per ripristinare l'accesso amministrativo, inserire **Administrators** nella casella di testo, quindi scegli **Aggiungi**.

5. Scegli **OK**.

Passaggio 8: (Facoltativo) Consenti e controlla le autorizzazioni per le connessioni SSH tramite Session Manager

Puoi consentire agli utenti del tuo account Account AWS di utilizzare AWS Command Line Interface (AWS CLI) per stabilire connessioni Secure Shell (SSH) ai nodi gestiti utilizzando AWS Systems Manager Session Manager. Gli utenti che si connettono utilizzando SSH possono anche copiare i file tra i loro computer locali e gli nodi gestiti usando SCP (Secure Copy Protocol). È possibile usare questa funzionalità per connetterti ai nodi gestiti senza aprire porte in entrata o gestire host bastion.

Quando si stabiliscono connessioni SSH tramite Session Manager, AWS CLI e si SSM Agent creano WebSocket connessioni sicure tramite TLS agli endpoint. Session Manager La sessione SSH viene eseguita all'interno di questo tunnel crittografato, fornendo un ulteriore livello di sicurezza senza richiedere l'apertura delle porte in entrata sui nodi gestiti.

Dopo aver consentito le connessioni SSH, puoi utilizzare le policy AWS Identity and Access Management (IAM) per consentire o negare esplicitamente a utenti, gruppi o ruoli di effettuare connessioni SSH utilizzando Session Manager.

Note

La registrazione non è disponibile per sessioni Session Manager che si connettono tramite inoltro porta o SSH. Questo perché SSH crittografa tutti i dati della sessione all'interno della connessione TLS sicura stabilita tra gli Session Manager endpoint AWS CLI e funge Session Manager solo da tunnel per le connessioni SSH.

Argomenti

- [Consentire connessioni SSH per Session Manager](#)
- [Controllo delle autorizzazioni utente per le connessioni SSH tramite Session Manager](#)

Consentire connessioni SSH per Session Manager

Attenersi alla seguente procedura per abilitare le connessioni SSH tramite Session Manager su un nodo gestito.

Per consentire connessioni SSH per Session Manager

1. Nel nodo gestito per cui si desidera permettere le connessioni SSH, procedere nel modo seguente:
 - Assicurati che SSH sia in esecuzione sul nodo gestito. (È possibile chiudere le porte in entrata sul nodo.)
 - Assicurati che la SSM Agent versione 2.3.672.0 o successiva sia installata sul nodo gestito.

Per informazioni su come installare e aggiornare SSM Agent su un nodo gestito, consulta i seguenti argomenti:

- [Installazione e disinstallazione manuali Agente SSM su istanze EC2 per Windows Server](#).
 - [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#)
 - [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per macOS](#)
 - [Come installare SSM Agent su nodi Windows ibridi](#)
 - [Come installare SSM Agent su nodi Linux ibridi](#)
2. Sul computer locale da cui si desidera connettersi a un nodo gestito tramite SSH, procedi nel modo seguente:
 - Assicurati che sia installata la versione 1.1.23.0 o successiva del plugin. Session Manager

Per informazioni sull'installazione del plugin Session Manager, consulta [Installa il Session Manager plugin per AWS CLI](#).

- Aggiornare il file di configurazione SSH per permettere l'esecuzione di un comando proxy che avvia una sessione Session Manager e trasferire tutti i dati tramite la connessione.

Linux e macOS

Tip

Il file di configurazione SSH si trova in genere nel percorso `~/.ssh/config`.

Aggiungere quanto segue al file di configurazione sul computer locale.

```
# SSH over Session Manager
Host i-* mi-*
    ProxyCommand sh -c "aws ssm start-session --target %h --document-name AWS-StartSSHSession --parameters 'portNumber=%p'"
    User ec2-user
```

Windows

Tip

Il file di configurazione SSH si trova in genere nel percorso C:\Users\<username>\.ssh\config.

Aggiungere quanto segue al file di configurazione sul computer locale.

```
# SSH over Session Manager
Host i-* mi-*
    ProxyCommand C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe "aws ssm start-session --target %h --document-name AWS-StartSSHSession --parameters portNumber=%p"
```

- Creare o verificare di disporre di un certificato Privacy Enhanced Mail Certificate (un file PEM) o almeno una chiave pubblica, da utilizzare quando si stabiliscono connessioni a nodi gestiti. Questa deve essere una chiave già associata al nodo gestito. Le autorizzazioni del file di chiavi private devono essere impostate in modo che tu sia l'unico a poterlo leggere. È possibile utilizzare il seguente comando per impostare le autorizzazioni del file di chiavi private in modo che tu sia l'unico a poterlo leggere.

```
chmod 400 <my-key-pair>.pem
```

Ad esempio, per un'istanza Amazon Elastic Compute Cloud (Amazon EC2), il file della coppia di chiavi creata o selezionata al momento della creazione dell'istanza. (Specificare il percorso al certificato o alla chiave come parte del comando per avviare una sessione. Per informazioni sull'avvio di una sessione tramite SSH, consultare) [Avvio di una sessione \(SSH\).](#))

Controllo delle autorizzazioni utente per le connessioni SSH tramite Session Manager

Dopo aver abilitato le connessioni SSH tramite Session Manager su un nodo gestito, è possibile utilizzare le policy IAM per consentire o impedire a utenti, gruppi o ruoli la possibilità di effettuare connessioni SSH tramite Session Manager.

Utilizzare una policy IAM per consentire le connessioni SSH tramite Session Manager

- Utilizza una delle opzioni seguenti:
 - Opzione 1: aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.

Nel riquadro di navigazione, scegli Policy e quindi aggiorna le policy di autorizzazioni per l'utente o il ruolo che desideri possa avviare le connessioni SSH tramite Session Manager.

Ad esempio, aggiungi il seguente elemento alla policy di avvio rapido creata in [Politiche Quickstart per gli utenti finali per Session Manager](#). Sostituisci ogni *example resource placeholder* con le tue informazioni.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ssm:StartSession",
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/instance-id",
        "arn:aws:ssm:*:*:document/AWS-StartSSHSession"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ssmmessages:OpenDataChannel",
      "Resource": "arn:aws:ssm:*:*:session/${aws:userid}-*"
    }
  ]
}
```

- Opzione 2: allega una policy in linea a una policy utente utilizzando Console di gestione AWS, AWS CLI, o l'AWS API.

Utilizzando il metodo prescelto, allega la dichiarazione politica nell'opzione 1 alla politica per un AWS utente, un gruppo o un ruolo.

Per informazioni, consulta [Aggiunta e rimozione di autorizzazioni per identità IAM](#) nella Guida per l'utente di IAM.

Per utilizzare una policy IAM per negare le connessioni SSH tramite Session Manager

- Utilizza una delle opzioni seguenti:
- Opzione 1: aprire la console IAM all'indirizzo. <https://console.aws.amazon.com/iam/> Nel riquadro di navigazione, scegli Policy e quindi aggiorna le policy di autorizzazione per l'utente o il ruolo per bloccare l'avvio delle sessioni Session Manager.

Ad esempio, aggiungi il seguente elemento alla policy di avvio rapido creata in [Politiche Quickstart per gli utenti finali per Session Manager](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ssm:StartSession",
      "Resource": "arn:aws:ssm:*:*:document/AWS-StartSSHSession"
    },
    {
      "Effect": "Allow",
      "Action": "ssmmessages:OpenDataChannel",
      "Resource": "arn:aws:ssm:*:*:session/${aws:userid}-*"
    }
  ]
}
```

- Opzione 2: allega una policy in linea a una policy utente utilizzando Console di gestione AWS, AWS CLI, o l'AWS API.

Utilizzando il metodo prescelto, allega la dichiarazione politica nell'opzione 1 alla politica per un AWS utente, un gruppo o un ruolo.

Per informazioni, consulta [Aggiunta e rimozione di autorizzazioni per identità IAM](#) nella Guida per l'utente di IAM.

Utilizzo di Session Manager

Puoi utilizzare la AWS Systems Manager console, la console Amazon Elastic Compute Cloud (Amazon EC2) o AWS CLI() per avviare sessioni che ti connettono ai nodi gestiti a cui AWS Command Line Interface l'amministratore di sistema ti ha concesso l'accesso utilizzando le policy (IAM). AWS Identity and Access Management A seconda delle autorizzazioni, puoi anche visualizzare le informazioni sulle sessioni, riprendere le sessioni inattive non ancora scadute e terminare le sessioni. Una volta stabilita, la sessione non è influenzata dalla durata della sessione del ruolo IAM. Per informazioni sulla limitazione della durata della sessione con Session Manager, consulta le sezioni [Specificare un valore di timeout della sessione di inattività](#) e [Specifica la durata massima della sessione](#).

Per ulteriori informazioni sulle sessioni, consulta [Che cos'è una sessione?](#)

Argomenti

- [Installa il Session Manager plugin per AWS CLI](#)
- [Avvio di una sessione](#)
- [Terminare una sessione](#)
- [Visualizzazione della cronologia delle sessioni](#)

Installa il Session Manager plugin per AWS CLI

 È richiesta una versione minima del plugin

Aggiorna il tuo Session Manager plugin alla versione 1.2.764.0 o successiva. Session Manager presto smetterà di supportare le versioni precedenti e le tue operazioni potrebbero non avere successo. Per verificare la versione installata, esegui il comando seguente.

```
session-manager-plugin --version
```

Per avviare sessioni di Session Manager con i nodi gestiti utilizzando la AWS Command Line Interface (AWS CLI), è necessario installare il plugin di Session Manager sul computer locale. È

possibile installare il plug-in su versioni supportate di Microsoft Windows Server, macOS, Linux e Ubuntu Server.

Note

Per utilizzare il Session Manager plugin, è necessario che la AWS CLI versione 1.16.12 o successiva sia installata sul computer locale. Per ulteriori informazioni, consulta [Installare o aggiornare la versione più recente della AWS Command Line Interface](#).

Argomenti

- [Session Manager ultima versione e cronologia delle versioni del plugin](#)
- [Installa il Session Manager plugin attivo Windows](#)
- [Installa il plugin Session Manager su macOS](#)
- [Installa il plug-in di Session Manager su Linux](#)
- [Verificare l'installazione del plugin Session Manager](#)
- [Plugin di Session Manager su GitHub](#)
- [\(Facoltativo\) Attivare la registrazione del plug-in Session Manager](#)

Session Manager ultima versione e cronologia delle versioni del plugin

Il computer locale deve eseguire una versione supportata del plug-in Session Manager. L'attuale versione minima supportata è 1.2.764.0. Se esegui una versione precedente, le operazioni del plug-in Session Manager potrebbero non andare a buon fine.

Per vedere se hai la versione più recente, esegui il comando riportato di seguito in AWS CLI.

Note

Il comando restituisce risultati solo se il plug-in si trova nella directory di installazione di default per il tuo tipo di sistema operativo. È possibile anche controllare la versione nel contenuto del file VERSION nella directory in cui è stato installato il plugin.

```
session-manager-plugin --version
```

La tabella seguente elenca tutte le release del plug-in Session Manager, nonché le funzionalità e i miglioramenti inclusi in ciascuna versione.

⚠ Important

Consigliamo di eseguire sempre la versione più recente. L'ultima versione include miglioramenti che migliorano l'esperienza di utilizzo del plug-in.

Versione	Data di rilascio	Informazioni
1.2.835.0	17 giugno 2026	Miglioramento: aggiungi sequenze di SSH-style escape alle sessioni di shell (~. per terminare, ~? per chiedere aiuto). Correzione di bug: risolve il problema delle sessioni di port forwarding che si interrompono silenziosamente dopo la riconnessione. WebSocket
1.2.814.0	23 aprile 2026	Correzione di bug: sposta la configurazione dell'endpoint SSM dalla AWS configurazione globale al livello di client SSM.
1.2.804.0	2 aprile 2026	Miglioramento: passa al pacchetto aws-sdk-go-v2. Correzione di bug: aggiorna lo script di installazione di Windows. Correzione bug: aggiorna la versione predefinita del plugin per la build locale.
1.2.792.0	17 marzo 2026	Correzione di bug: aggiunto il supporto internazionale per la tastiera per Windows.
1.2.779.0	12 febbraio 2026	Miglioramento: aggiorna la versione Go alla 1.25 in Dockerfile. Correzione di bug: aggiungere linee shebang agli script di pacchettizzazione di Debian.
1.2.764.0	19 novembre 2025	Miglioramento: aggiunto il supporto per la richiesta di firma OpenDataChannel .

Versione	Data di rilascio	Informazioni
		Correzione di bug: risolve i problemi di checkstyle per supportare la versione Go più recente.
1.2.707.0	6 febbraio 2025	Miglioramento: aggiornamento della versione Go alla 1.23 nel Dockerfile. Aggiornamento della fase di configurazione della versione nel README.
1,2,694,0	20 novembre 2024	Correzione bug: annullata la modifica che aggiungeva credenziali alle richieste. OpenDataChannel
1.2.688.0	6 novembre 2024	Questa versione è stata dichiarata obsoleta il /2024. 11/20 Miglioramenti: <ul style="list-style-type: none"> • Credenziali aggiunte alle OpenDataChannel richieste. • Sono stati aggiornati i pacchetti dipendenti testify e objx.
1.2.677.0	10 ottobre 2024	Miglioramento: aggiunto il supporto per il passaggio della versione del plugin con le richieste. OpenDataChannel
1.2.650.0	2 luglio 2024	Miglioramento: aws-sdk-go aggiornato alla versione 1.54.10. Correzione di bug: riformati commenti per gofmt check.
1,2.6330	30 maggio 2024	Miglioramento: è stato aggiornato il Dockerfile per utilizzare un'immagine Amazon Elastic Container Registry (Amazon ECR).
1,2,553.0	10 gennaio 2024	Miglioramento: pacchetti aws-sdk-go e Golang dipendenti aggiornati.
1,2,536,0	04 dicembre 2023	Miglioramento: aggiunto il supporto per il passaggio di una risposta StartSession API come variabile di ambiente a session-manager-plugin.
1.2.497.0	1° agosto 2023	Miglioramento: Go SDK aggiornato alla versione 1.44.302.

Versione	Data di rilascio	Informazioni
1,2,463,0	15 marzo 2023	Miglioramento: aggiunto il supporto Mac with Apple silicon per Apple Mac (M1) nel programma di installazione del bundle macOS e nel programma di installazione firmato.
1,2,398,0	14 ottobre 2022	Miglioramento: supporto per la versione go lang 1.17. Aggiorna il runner del plug-in di gestione delle sessioni predefinito per macOS in modo da usare python3. Aggiorna il percorso di importazione da SSMCLI a session-manager-plugin.
1,2,339,0	16 giugno 2022	Correzione di bug: correzione del timeout della sessione inattiva per le sessioni di porta.
1,2,331.0	27 maggio 2022	Correzione di bug: correzione della chiusura prematura delle sessioni della porta quando il server locale non si connette prima del timeout.
1,2.323,0	19 maggio 2022	Correzione di bug: disabilita smux keep alive per utilizzare la funzione di timeout della sessione inattiva.
1,2.312,0	31 marzo 2022	Miglioramento: supporta più tipi di payload dei messaggi di output.
1,2,295,0	12 gennaio 2022	Correzione di bug: sessioni sospese causate dal client che invia nuovamente i dati del flusso quando l'agente diventa inattivo e i log errati per i messaggi di <code>start_publication</code> e <code>pause_publication</code> .
1,2,279,0	27 ottobre 2021	Miglioramento: packaging in formato zip per la piattaforma Windows.
1,2,245.0	19 agosto 2021	Miglioramento: Aggiornamento di <code>aws-sdk-go</code> alla versione più recente (v1.40.17) per supportare Centro identità AWS IAM.
1,2,234.0	26 luglio 2021	Risoluzione dei bug: Gestione dello scenario di una sessione terminata improvvisamente nel tipo di sessione interattiva.

Versione	Data di rilascio	Informazioni
1,2,205.0	10 giugno 2021	Miglioramento: è stato aggiunto il supporto per il programma di installazione firmato macOS.
1,2.54,0	29 gennaio 2021	Miglioramento: aggiunto il supporto per l'esecuzione di sessioni in modalità di esecuzione. NonInteractiveCommands
1.2.30.0	24 novembre 2020	Miglioramento: (solo le sessioni di inoltro delle porte) Miglioramento delle prestazioni complessive.
1.2.7.0	15 ottobre 2020	Miglioramento: (solo le sessioni di inoltro delle porte) latenza ridotta e prestazioni complessive migliorate.
1.1.61.0	17 aprile 2020	Miglioramento: aggiunto il supporto ARM per Linux e Ubuntu Server.
1.1.54.0	6 gennaio 2020	Correzione di bug: gestione dello scenario di race condition dei pacchetti che vengono rilasciati quando il plug-in Session Manager non è pronto.
1.1.50.0	19 novembre 2019	Miglioramento: Aggiunto il supporto per l'inoltro di una porta a un socket unix locale.
1.1.35.0	7 novembre 2019	Miglioramento: (solo sessioni di port forwarding) Invia un TerminateSession comando a SSM Agent quando l'utente locale preme. <code>Ctrl+C</code>
1.1.33.0	26 settembre 2019	Miglioramento: (solo sessioni di inoltro alla porta) invia un segnale di disconnessione al server quando il client rimuove la connessione TCP.
1.1.31.0	6 settembre 2019	Miglioramento: aggiorna per mantenere aperta la sessione di inoltro alla porta finché il server remoto non chiude la connessione.
1.1.26.0	30 luglio 2019	Miglioramento: aggiornamento per limitare la velocità di trasferimento dei dati durante una sessione.

Versione	Data di rilascio	Informazioni
1.1.23.0	09 luglio 2019	Miglioramento: aggiunta del supporto per l'esecuzione di sessioni SSH utilizzando Session Manager.
1.1.17.0	4 aprile 2019	Miglioramento: aggiunta del supporto per ulteriore crittografia dei dati delle sessioni utilizzando AWS Key Management Service (AWS KMS).
1.0.37.0	20 settembre 2018	Miglioramento: correzione di bug per la versione Windows.
1.0.0.0	11 settembre 2018	Versione iniziale del plug-in Session Manager.

Installa il Session Manager plugin attivo Windows

È possibile installare il Session Manager plug-in a 64 bit Windows 10 o versioni successive Windows Server 2016 oppure in versioni successive utilizzando il programma di installazione autonomo.

Quando vengono rilasciati gli aggiornamenti, è necessario ripetere il processo di installazione per ottenere la versione più recente del plug-in Session Manager.

Note

Osservare le seguenti informazioni.

- Il programma di installazione del plugin di Session Manager necessita dei diritti di amministratore per installare il plug-in.
- Per ottenere risultati ottimali, ti consigliamo di avviare sessioni sui client Windows utilizzando Windows PowerShell versione 5 o successiva. In alternativa, puoi utilizzare la shell Command in Windows 10. Il Session Manager plugin supporta solo la PowerShell shell di comando. Third-party gli strumenti da riga di comando potrebbero non essere compatibili con il plugin.

Per installare il Session Manager plugin che utilizza il programma di installazione EXE

1. Scaricare il programma di installazione utilizzando l'URL seguente.

```
https://s3.amazonaws.com/session-manager-downloads/plugin/latest/windows/SessionManagerPluginSetup.exe
```

In alternativa, è possibile scaricare una versione compressa del programma di installazione utilizzando il seguente URL.

```
https://s3.amazonaws.com/session-manager-downloads/plugin/latest/windows/SessionManagerPlugin.zip
```

2. Esegui il programma di installazione scaricato e segui le istruzioni sullo schermo. Se hai scaricato la versione compressa del programma di installazione, devi prima decomprimere il programma di installazione.

Lasciare vuota la casella del percorso di installazione per installare il plug-in nella directory di default.

- %PROGRAMFILES%\Amazon\SessionManagerPlugin\bin\

3. Verificare che l'installazione sia stata effettuata correttamente. Per informazioni, consulta [Verificare l'installazione del plugin Session Manager](#).

Note

Se Windows non è in grado di trovare l'eseguibile, potrebbe essere necessario aprire nuovamente il prompt dei comandi o aggiungere manualmente la directory di installazione alla variabile di ambiente PATH. Per ulteriori informazioni relative alla risoluzione di problemi, consultare [Il plug-in di Session Manager non viene aggiunto automaticamente al percorso della riga di comando \(Windows\)](#).

Installa il plugin Session Manager su macOS

Scegli uno dei seguenti argomenti per installare il plug-in di Session Manager su macOS.

 Note

Il programma di installazione firmato è un file `.pkg` firmato. Il programma di installazione in bundle utilizza un file `.zip`. Una volta decompresso il file, puoi installare il plug-in utilizzando il file binario.

Installazione di plug-in Session Manager su macOS con il programma di installazione firmato

Questa sezione descrive come installare il plugin di Session Manager su macOS utilizzando il programma di installazione firmato.

Per installare il plug-in Session Manager utilizzando il programma di installazione firmato (macOS)

1. Scaricare il programma di installazione firmato.

x86_64

```
curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/mac/session-manager-plugin.pkg" -o "session-manager-plugin.pkg"
```

Mac con processore Apple

```
curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/mac_arm64/session-manager-plugin.pkg" -o "session-manager-plugin.pkg"
```

2. Esegui i comandi di installazione. Se il comando fa errore, verifica che la cartella `/usr/local/bin` esista. In caso contrario, creala ed esegui nuovamente il comando.

```
sudo installer -pkg session-manager-plugin.pkg -target /  
sudo ln -s /usr/local/sessionmanagerplugin/bin/session-manager-plugin /usr/local/bin/session-manager-plugin
```

3. Verificare che l'installazione sia stata effettuata correttamente. Per informazioni, consulta [Verificare l'installazione del plugin Session Manager](#).

Installa il plugin Session Manager su macOS

Questa sezione descrive come installare il plugin di Session Manager su macOS utilizzando il programma di installazione in bundle.

 Important

Prendi nota delle seguenti informazioni importanti.

- Per impostazione predefinita, il programma di installazione richiede l'accesso sudo per l'esecuzione, poiché lo script installa il plug-in nella directory di sistema di `/usr/local/sessionmanagerplugin`. Se non vuoi installare il plugin usando sudo, aggiorna manualmente lo script di installazione per installare il plugin in una directory che non richiede l'accesso sudo.
- Non supporta l'installazione in percorsi che contengono spazi.

Per installare il plug-in Session Manager mediante il programma di installazione in bundle (macOS)

1. Scarica il programma di installazione in bundle.

x86_64

```
curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/mac/sessionmanager-bundle.zip" -o "sessionmanager-bundle.zip"
```

Mac con processore Apple

```
curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/mac_arm64/sessionmanager-bundle.zip" -o "sessionmanager-bundle.zip"
```

2. Decomprimi il pacchetto.

```
unzip sessionmanager-bundle.zip
```

3. Eseguire il comando di installazione.

```
sudo ./sessionmanager-bundle/install -i /usr/local/sessionmanagerplugin -b /usr/local/bin/session-manager-plugin
```

 Note

Il plugin richiede Python 3.10 o successivo. Per default, lo script di installazione viene eseguito con la versione di Python di default del sistema. Se è installata una versione

alternativa di Python e si intende utilizzare questa per installare il Session Manager, eseguire lo script del programma di installazione con tale versione dal percorso assoluto dell'eseguibile di Python. Di seguito è riportato un esempio di :

```
sudo /usr/local/bin/python3.11 sessionmanager-bundle/install -i /usr/local/sessionmanagerplugin -b /usr/local/bin/session-manager-plugin
```

Il programma di installazione installa il Session Manager in `/usr/local/sessionmanagerplugin` e crea il collegamento simbolico `session-manager-plugin` nella directory `/usr/local/bin`. Ciò elimina la necessità di specificare la directory di installazione nella variabile `$PATH` dell'utente.

Per vedere una spiegazione delle opzioni `-i` e `-b`, usa l'opzione `-h`.

```
./sessionmanager-bundle/install -h
```

4. Verificare che l'installazione sia stata effettuata correttamente. Per informazioni, consulta [Verificare l'installazione del plugin Session Manager](#).

Note

Per disinstallare il plugin, esegui i due comandi riportati di seguito nell'ordine visualizzato.

```
sudo rm -rf /usr/local/sessionmanagerplugin
```

```
sudo rm /usr/local/bin/session-manager-plugin
```

Installa il plug-in di Session Manager su Linux

Questa sezione include informazioni sulla verifica della firma del pacchetto del programma di installazione del plug-in di Session Manager e sull'installazione del plug-in nelle seguenti distribuzioni Linux:

- Amazon Linux 2
- AL2023

- RHEL
- Debian Server
- Ubuntu Server

Argomenti

- [Verifica la firma del Session Manager plugin](#)
- [Installa il plug-in di Session Manager su Amazon Linux 2, Amazon Linux 2023 e distribuzioni Red Hat Enterprise Linux](#)
- [Installazione del plug-in Session Manager su Debian Server e Ubuntu Server](#)

Verifica la firma del Session Manager plugin

I pacchetti del programma di installazione RPM e Debian del plug-in di Session Manager per le istanze Linux sono firmati crittograficamente. È possibile utilizzare una chiave pubblica per verificare che il plug-in binario e il pacchetto siano originali e non modificati. Se i file sono in qualche modo danneggiati o alterati, la verifica non va a buon fine. È possibile verificare la firma del programma di installazione tramite lo strumento GNU Privacy Guard (GPG). Le seguenti informazioni sono relative alle versioni 1.2.707.0 o successive del plug-in di Session Manager.

Completa i seguenti passaggi, per verificare la firma del pacchetto del programma di installazione del plug-in di Session Manager.

Argomenti

- [Passaggio 1: scarica il Session Manager pacchetto di installazione del plugin](#)
- [Passaggio 2: scarica il file di firma associato](#)
- [Passaggio 3: installa lo strumento GPG](#)
- [Fase 4: Verifica Session Manager pacchetto di installazione del plug-in su un server Linux](#)

Passaggio 1: scarica il Session Manager pacchetto di installazione del plugin

Scarica il pacchetto del programma di installazione del plug-in di Session Manager che desideri verificare.

Amazon Linux 2, AL2023 e pacchetti RPM RHEL

x86_64

```
curl -o "session-manager-plugin.rpm" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_64bit/session-manager-plugin.rpm"
```

ARM64

```
curl -o "session-manager-plugin.rpm" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_arm64/session-manager-plugin.rpm"
```

Pacchetti Debian Server e Deb Ubuntu Server

x86_64

```
curl -o "session-manager-plugin.deb" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_64bit/session-manager-plugin.deb"
```

ARM64

```
curl -o "session-manager-plugin.deb" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_arm64/session-manager-plugin.deb"
```

Passaggio 2: scarica il file di firma associato

Dopo aver scaricato il pacchetto del programma di installazione, scarica il file di firma associato per la verifica del pacchetto. Per fornire un ulteriore livello di protezione contro la copia o l'utilizzo non autorizzati del file binario session-manager-plugin all'interno del pacchetto, offriamo anche firme binarie da utilizzare per convalidare singoli file binari. Puoi scegliere di utilizzare queste firme binarie in base alle tue esigenze di sicurezza.

Amazon Linux 2, AL2023 e pacchetti di firma RHEL

x86_64

Pacchetto:

```
curl -o "session-manager-plugin.rpm.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_64bit/session-manager-plugin.rpm.sig"
```

File binario:

```
curl -o "session-manager-plugin.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_64bit/session-manager-plugin.sig"
```

ARM64

Pacchetto:

```
curl -o "session-manager-plugin.rpm.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_arm64/session-manager-plugin.rpm.sig"
```

File binario:

```
curl -o "session-manager-plugin.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_arm64/session-manager-plugin.sig"
```

Debian Server e pacchetti di firma Deb Ubuntu Server

x86_64

Pacchetto:

```
curl -o "session-manager-plugin.deb.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_64bit/session-manager-plugin.deb.sig"
```

File binario:

```
curl -o "session-manager-plugin.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_64bit/session-manager-plugin.sig"
```

ARM64

Pacchetto:

```
curl -o "session-manager-plugin.deb.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_arm64/session-manager-plugin.deb.sig"
```

File binario:

```
curl -o "session-manager-plugin.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_arm64/session-manager-plugin.sig"
```

Passaggio 3: installa lo strumento GPG

Per verificare la firma del plug-in di Session Manager, è necessario che sul sistema sia installato lo strumento GNU Privacy Guard (GPG). Il processo di verifica richiede la versione 2.1 o successiva di GPG. Puoi verificare la tua versione GPG eseguendo il comando seguente:

```
gpg --version
```

Se la tua versione di GPG è precedente alla 2.1, aggiornala prima di continuare con il processo di verifica. Per la maggior parte dei sistemi, puoi aggiornare lo strumento GPG usando il tuo gestore di pacchetti. Ad esempio, su versioni di Amazon e RHEL supportate, puoi utilizzare i seguenti comandi:

```
sudo yum update
sudo yum install gnupg2
```

Sui sistemi Ubuntu Server e Debian Server supportati, puoi utilizzare i seguenti comandi:

```
sudo apt-get update
sudo apt-get install gnupg2
```

Assicurati di avere la versione GPG richiesta prima di continuare con il processo di verifica.

Fase 4: Verifica Session Manager pacchetto di installazione del plug-in su un server Linux

Utilizza la procedura seguente per verificare il pacchetto del programma di installazione del plug-in di Session Manager in un server Linux.

Note

Amazon Linux 2 non supporta la versione 2.1 o successiva dello strumento GPG. Se la seguente procedura non funziona sulle tue istanze Amazon Linux 2, verifica la firma su una piattaforma diversa prima di installarla sulle tue istanze Amazon Linux 2.

1. Copia la seguente chiave pubblica e salvala in un file denominato session-manager-plugin.gpg.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mFIEZ5ERQxMIKoZIZj0DAQcCAwQjuZy+IjFoYg57sLTGhF3aZLBaGpzB+gY6j7Ix
P7NqbpXyjVj8a+dy79gSd640EaMxUb7vw/jug+CfRXwVGRMNtIBBV1MgU1NNIFNl
c3Npb24gTWFuYWdlciA8c2Vzc2lubi1tYW5hZ2VYLXBsdWdpbi1zaWduZXJAYW1h
em9uLmNvbT4gKEFXUyBTExN0ZW1zIE1hbmFnZXIgaU2Vzc2lubiBNYW5hZ2VYIFBs
dWdpbiBMaW5leCBTaWduZXIgaS2V5KYkBAQQQEwgAqAUCZ5ERQ4EcQVdTIFNTTSBT
ZXNzaW9uIE1hbmFnZXIgaPHNlc3Npb24tbWFnYUdlci1wbHVnaW4tc2lnbmVyQGft
YXpvi5jb20+IChBV1MgU3lzdGVtcyBNYW5hZ2VYIFNlc3Npb24gTWFuYWdlciBQ
bHVnaW4gTGludXggU2lnbmVyIEtleSkWIQR5WWNxJM4J0tUB1HosTUr/b2dX7gIe
AwIbAwIVCAAKCRAsTUr/b2dX7r01AQCa1kig3lQ78W/QHGU76uHx3XAYv0tftpE9U
oQBCIwFLSgEA3PDHt3lZ+s6m9JLGJsy+Cp5ZFzpiF6RgluR/2gA861M=
=2DQm
-----END PGP PUBLIC KEY BLOCK-----
```

2. Importa la chiave pubblica nel tuo keyring. Il valore della chiave restituito dovrebbe essere 2C4D4AFF6F6757EE.

```
$ gpg --import session-manager-plugin.gpg
gpg: key 2C4D4AFF6F6757EE: public key "AWS SSM Session Manager <session-manager-
plugin-signer@amazon.com> (AWS Systems Manager Session Manager Plugin Linux Signer
Key)" imported
gpg: Total number processed: 1
gpg:             imported: 1
```

3. Per verificare l'impronta digitale, esegui il seguente comando.

```
gpg --fingerprint 2C4D4AFF6F6757EE
```

L'impronta digitale per l'output dell'impronta digitale deve corrispondere a quanto riportato di seguito.

```
7959 6371 24CE 093A D501 D47A 2C4D 4AFF 6F67 57EE
```

```
pub  nistp256 2025-01-22 [SC]
      7959 6371 24CE 093A D501 D47A 2C4D 4AFF 6F67 57EE
uid  [ unknown] AWS SSM Session Manager <session-manager-plugin-
signer@amazon.com> (AWS Systems Manager Session Manager Plugin Linux Signer Key)
```

Se l'impronta digitale non corrisponde, non installare il plug-in. Contatto Supporto AWS.

4. Verificare la firma del pacchetto di installazione. Sostituisci *signature-filename* e *downloaded-plugin-filename* con i valori specificati durante il download del file di firma e del session-manager-plugin, come elencato nella tabella precedente in questo argomento.

```
gpg --verify signature-filename downloaded-plugin-filename
```

Ad esempio, per l'architettura x86_64 in Amazon Linux 2, il comando è il seguente:

```
gpg --verify session-manager-plugin.rpm.sig session-manager-plugin.rpm
```

Questo comando restituisce un output simile al seguente.

```
gpg: Signature made Mon Feb 3 20:08:32 2025 UTC gpg: using ECDSA key
    2C4D4AFF6F6757EE
gpg: Good signature from "AWS Systems Manager Session Manager <session-manager-
plugin-signer@amazon.com> (AWS Systems Manager Session Manager Plugin Linux Signer
Key)" [unknown]
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: 7959 6371 24CE 093A D501 D47A 2C4D 4AFF 6F67 57EE
```

Se l'output include la frase `BAD signature`, controllare di avere eseguito la procedura correttamente. Se continui a ricevere questa risposta, contatta Supporto AWS e non installare il pacchetto. Il messaggio di avviso relativo all'attendibilità non indica che la firma non sia valida, ma soltanto che la chiave pubblica non è stata verificata. Una chiave è considerata attendibile solo se è stata firmata dall'utente o da un firmatario fidato. Se l'output include la frase `Can't check signature: No public key`, verifica di aver scaricato il plug-in di Session Manager con la versione 1.2.707.0 o successiva.

Installa il plug-in di Session Manager su Amazon Linux 2, Amazon Linux 2023 e distribuzioni Red Hat Enterprise Linux

Utilizza la seguente procedura per installare il plug-in di Session Manager su Amazon Linux 2, Amazon Linux 2023 (AL2023) e distribuzioni RHEL.

1. Scarica e installa il pacchetto RPM del plugin Session Manager.

x86_64

Su Amazon Linux 2 e RHEL 7 eseguire il seguente comando:

```
sudo yum install -y https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_64bit/session-manager-plugin.rpm
```

Su AL2023 e RHEL 8 e 9 eseguire il seguente comando:

```
sudo dnf install -y https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_64bit/session-manager-plugin.rpm
```

ARM64

Su Amazon Linux 2 e RHEL 7 eseguire il seguente comando:

```
sudo yum install -y https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_arm64/session-manager-plugin.rpm
```

Su AL2023 e RHEL 8 e 9 eseguire il seguente comando:

```
sudo dnf install -y https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_arm64/session-manager-plugin.rpm
```

2. Verificare che l'installazione sia stata effettuata correttamente. Per informazioni, consulta [Verificare l'installazione del plugin Session Manager](#).

Note

Se desideri disinstallare il plugin, esegui `sudo yum erase session-manager-plugin -y`

Installazione del plug-in Session Manager su Debian Server e Ubuntu Server

1. Scaricare il pacchetto deb del plug-in Session Manager:

x86_64

```
curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_64bit/session-manager-plugin.deb" -o "session-manager-plugin.deb"
```

ARM64

```
curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_arm64/session-manager-plugin.deb" -o "session-manager-plugin.deb"
```

2. Eseguire il comando di installazione.

```
sudo dpkg -i session-manager-plugin.deb
```

3. Verificare che l'installazione sia stata effettuata correttamente. Per informazioni, consulta [Verificare l'installazione del plugin Session Manager](#).

Note

Se si desidera disinstallare il plugin, eseguire `sudo dpkg -r session-manager-plugin`

Verificare l'installazione del plugin Session Manager

Per verificare che il plug-in Session Manager sia stato installato, esegui il comando riportato di seguito.

```
session-manager-plugin
```

Se l'installazione è stata completata, viene restituito il seguente messaggio.

```
The Session Manager plugin is installed successfully. Use the AWS CLI to start a session.
```

È anche possibile testare l'installazione eseguendo il comando [start-session](#) riportato di seguito in [AWS Command Line Interface](#) (AWS CLI). Nel comando seguente, sostituisci *instance-id* con le tue informazioni.

```
aws ssm start-session --target instance-id
```

Questo comando funzionerà solo se hai installato e configurato e se l' AWS CLI Session Manager amministratore ti ha concesso le autorizzazioni IAM necessarie per accedere al nodo gestito di destinazione utilizzando Session Manager.

Plugin di Session Manager su GitHub

Il codice sorgente per il plug-in di Session Manager è disponibile su [GitHub](#) in modo da adattare il plug-in per soddisfare le proprie esigenze. Ti consigliamo di inviare le [richieste pull](#) per le modifiche da includere. Tuttavia, Amazon Web Services attualmente non fornisce il supporto per eseguire copie modificate di questo software.

(Facoltativo) Attivare la registrazione del plug-in Session Manager

Il plug-in Session Manager include un'opzione per abilitare la registrazione per le sessioni che esegui. Per impostazione predefinita, la registrazione è disattivata.

Se abiliti la registrazione, il plug-in Session Manager crea un file di log sia per le attività dell'applicazione (`session-manager-plugin.log`) sia per gli errori (`errors.log`) sul tuo computer locale.

Argomenti

- [Attivare la registrazione per il plug-in Session Manager \(Windows\)](#)
- [Abilitazione della registrazione per il plug-in Session Manager \(Linux e macOS\)](#)

Attivare la registrazione per il plug-in Session Manager (Windows)

1. Individuare il file `seelog.xml.template` per il plugin.

Il percorso predefinito è `C:\Program Files\Amazon\SessionManagerPlugin\seelog.xml.template`.

2. Modificare il nome del file in `seelog.xml`.
3. Aprire il file e modificare `minlevel="off"` in `minlevel="info"` o `minlevel="debug"`.

 Note

Per impostazione predefinita, le voci di log relative all'apertura di un canale di dati e alla riconnessione delle sessioni sono registrate nel livello INFO. Le voci del flusso di dati (pacchetti e relativa conferma) sono registrate nel livello DEBUG.

4. Modificare altre opzioni di configurazione in base alle proprie esigenze. Le opzioni che è possibile modificare includono:
 - Livello di debug: è possibile modificare il livello di debug da `formatid="fmtinfo"` a `formatid="fmtdebug"`.
 - Opzioni relative ai file di log: è possibile modificare le opzioni relative ai file di log, inclusa la posizione in cui vengono archiviati i log, ad eccezione dei nomi dei file.

 Important

Non modificare i nomi dei file, altrimenti la registrazione non funzionerà correttamente.

```
<rollingfile type="size" filename="C:\Program Files\Amazon\SessionManagerPlugin
\Log\session-manager-plugin.log" maxsize="30000000" maxrolls="5"/>
<filter levels="error,critical" formatid="fmterror">
<rollingfile type="size" filename="C:\Program Files\Amazon\SessionManagerPlugin
\Log\errors.log" maxsize="10000000" maxrolls="5"/>
```

5. Salvare il file.

Abilitazione della registrazione per il plug-in Session Manager (Linux e macOS)

1. Individuare il file `seelog.xml.template` per il plugin.

Il percorso predefinito è `/usr/local/sessionmanagerplugin/seelog.xml.template`.

2. Modificare il nome del file in `seelog.xml`.
3. Aprire il file e modificare `minlevel="off"` in `minlevel="info"` o `minlevel="debug"`.

 Note

Per impostazione predefinita, le voci di log relative all'apertura di canali di dati e alla riconnessione delle sessioni sono registrate nel livello INFO. Le voci del flusso di dati (pacchetti e relativa conferma) sono registrate nel livello DEBUG.

4. Modificare altre opzioni di configurazione in base alle proprie esigenze. Le opzioni che è possibile modificare includono:

- Livello di debug: è possibile modificare il livello di debug da `formatid="fmtinfo"` a `outputs formatid="fmtdebug"`.
- Opzioni relative ai file di log: è possibile modificare le opzioni relative ai file di log, inclusa la posizione in cui vengono archiviati i log, ad eccezione dei nomi dei file.

 Important

Non modificare i nomi dei file, altrimenti la registrazione non funzionerà correttamente.

```
<rollingfile type="size" filename="/usr/local/sessionmanagerplugin/logs/session-  
manager-plugin.log" maxsize="300000000" maxrolls="5"/>  
<filter levels="error,critical" formatid="fmterror">  
<rollingfile type="size" filename="/usr/local/sessionmanagerplugin/logs/  
errors.log" maxsize="100000000" maxrolls="5"/>
```

 Important

Se si utilizza la directory di default specificata per l'archiviazione dei log, è necessario eseguire i comandi di sessione utilizzando `sudo` o fornire l'accesso completo in lettura e scrittura alla directory in cui è installato il plugin. Per by-passare queste limitazioni, modifica il percorso in cui vengono archiviati i log.

5. Salvare il file.

Avvio di una sessione

Puoi utilizzare la AWS Systems Manager console, la console Amazon Elastic Compute Cloud (Amazon EC2), AWS Command Line Interface il AWS CLI() o SSH per avviare una sessione.

Argomenti

- [Avvio di una sessione \(console Systems Manager\)](#)
- [Avvio di una sessione \(console Amazon EC2 \)](#)
- [Avvio di una sessione \(AWS CLI\)](#)
- [Avvio di una sessione \(SSH\)](#)
- [Avvio di una sessione \(inoltro alla porta\)](#)
- [Avvio di una sessione \(inoltro alla porta a un host remoto\)](#)
- [Avvio di una sessione \(comandi interattivi e non interattivi\)](#)

Avvio di una sessione (console Systems Manager)

Puoi utilizzare la AWS Systems Manager console per avviare una sessione con un nodo gestito nel tuo account.

Note

Prima di avviare una sessione, assicurati di aver completato la procedura di configurazione per Session Manager. Per informazioni, consulta [Configurazione di Session Manager](#).

Per avviare una sessione (console Systems Manager)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Session Manager.
3. Scegliere Start session (Avvia sessione).
4. (Facoltativo) Inserisci una descrizione della sessione nel campo Motivo della sessione.
5. Per Istanze di destinazione, scegli il pulsante di opzione a sinistra del nodo gestito a cui desideri connetterti.

Se il nodo che desideri non è presente nell'elenco o se selezioni un nodo e ricevi un errore di configurazione, consulta [Nodo gestito non disponibile o non configurato per Session Manager](#) per la procedura di risoluzione dei problemi.

6. Scegli Avvia sessione per avviare immediatamente la sessione.

oppure

Scegli Avanti per le opzioni di sessione.

7. (Facoltativo) Per Documento di sessione, seleziona il documento che desideri eseguire all'inizio della sessione. Se il documento supporta i parametri di runtime, è possibile inserire uno o più valori separati da virgole in ogni campo dei parametri.
8. Scegli Next (Successivo).
9. Scegliere Start session (Avvia sessione).

Una volta creata la connessione, è possibile eseguire i comandi bash (Linux e macOS) o i comandi PowerShell (Windows) come per qualsiasi altro tipo di connessione.

Important

Se desideri consentire agli utenti di specificare un documento all'avvio delle sessioni nella console di Session Manager, tieni presente quanto segue:

- Devi concedere agli utenti le autorizzazioni `ssm:GetDocument` e `ssm:ListDocuments` nella loro policy IAM. Per ulteriori informazioni, consulta [Concedere l'accesso ai documenti di sessione personalizzati nella console](#).
- La console supporta solo i documenti di sessione il cui `sessionType` è definito come `Standard_Stream`. Per ulteriori informazioni, consulta [Schema documento di sessione](#).

Avvio di una sessione (console Amazon EC2)

È possibile utilizzare la console Amazon Elastic Compute Cloud (Amazon EC2) per avviare una sessione con un'istanza nel tuo account.

 Note

Se ricevi un errore che indica che non sei autorizzato a eseguire una o più operazioni Systems Manager (`ssm: command-name`), devi contattare il tuo amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso. Chiedere a tale persona di aggiornare le policy per consentire l'avvio delle sessioni dalla console Amazon EC2. Se sei un amministratore, consulta [Esempi di policy IAM per Session Manager](#) per ulteriori informazioni.

Avvio di una sessione (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 Connection Method (Metodo di connessione), scegliere Session Manager.
5. Scegli Connetti.

Una volta creata la connessione, è possibile eseguire i comandi bash (Linux e macOS) o i comandi PowerShell (Windows) come per qualsiasi altro tipo di connessione.

Avvio di una sessione (AWS CLI)

Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

Prima di avviare una sessione, assicurati di aver completato la procedura di configurazione per Session Manager. Per informazioni, consulta [Configurazione di Session Manager](#).

Per utilizzare i comandi AWS CLI to run session, il Session Manager plugin deve essere installato anche sul computer locale. Per informazioni, consulta [Installa il Session Manager plugin per AWS CLI](#).

Per avviare una sessione utilizzando il AWS CLI, esegui il comando seguente sostituendolo *instance-id* con le tue informazioni.

```
aws ssm start-session \  
  --target instance-id
```

Per informazioni sulle altre opzioni utilizzabili con il start-session comando, [start-session](#)consultate la AWS Systems Manager sezione del AWS CLI Command Reference.

Avvio di una sessione (SSH)

Per avviare una sessione SSH Session Manager, la versione 2.3.672.0 o successiva di SSM Agent deve essere installata sul nodo gestito.

Requisiti di connessione SSH

Prendi nota dei seguenti requisiti e limitazioni per le connessioni di sessione che utilizzano SSH tramite Session Manager:

- Il tuo nodo gestito di destinazione deve essere configurato per supportare le connessioni SSH. Per ulteriori informazioni, consulta [\(Facoltativo\) Abilitare e controllare le autorizzazioni per le connessioni SSH tramite Session Manager](#).
- È necessario connettere l'utente sull'account del nodo gestito associato al certificato PEM (Privacy Enhanced Mail), non l'account ssm-user utilizzato per altri tipi di connessioni di sessione. Ad esempio, nelle istanze EC2 per Linux e macOS, l'utente predefinito è ec2-user. Per informazioni sull'identificazione dell'utente di default per ogni tipo di istanza, consulta [Ottenere informazioni sull'istanza](#) nella Guida per l'utente di Amazon EC2.
- La registrazione non è disponibile per sessioni Session Manager che si connettono tramite inoltro porta o SSH. Questo perché SSH crittografa tutti i dati della sessione all'interno della connessione TLS sicura stabilita tra gli Session Manager endpoint AWS CLI e funge Session Manager solo da tunnel per le connessioni SSH.

Note

Prima di avviare una sessione, assicurati di aver completato la procedura di configurazione per Session Manager. Per informazioni, consulta [Configurazione di Session Manager](#).

Per avviare una sessione tramite SSH, esegui il comando riportato di seguito. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
ssh -i /path/my-key-pair.pem username@instance-id
```

Tip

Quando avvii una sessione tramite SSH, è possibile copiare i file locali nel nodo gestito di destinazione usando il formato di comando seguente.

```
scp -i /path/my-key-pair.pem /path/ExampleFile.txt username@instance-id:~
```

Per informazioni sulle altre opzioni che è possibile utilizzare con il start-session comando, vedere la AWS Systems Manager sezione del Command [start-session](#)Reference. AWS CLI

Avvio di una sessione (inoltro alla porta)

Per avviare una sessione di inoltro porta Session Manager, la versione 2.3.672.0 o successiva di SSM Agent deve essere installata sul nodo gestito.

Note

Prima di avviare una sessione, assicurati di aver completato la procedura di configurazione per Session Manager. Per informazioni, consulta [Configurazione di Session Manager](#). Per utilizzare i comandi AWS CLI per eseguire la sessione, è necessario installare il Session Manager plug-in sul computer locale. Per informazioni, consulta [Installa il Session Manager plugin per AWS CLI](#).

A seconda del sistema operativo e dello strumento da riga di comando, il posizionamento delle virgolette può variare e potrebbero essere necessari caratteri di escape.

Per avviare una sessione di inoltro alla porta, esegui il comando seguente dalla CLI: Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux & macOS

```
aws ssm start-session \  
  --target instance-id \  
  --document-name AWS-StartPortForwardingSession \  
  --parameters '{"portNumber":["80"], "localPortNumber":["56789"]}'
```

Windows

```
aws ssm start-session ^  
  --target instance-id ^  
  --document-name AWS-StartPortForwardingSession ^  
  --parameters portNumber="3389",localPortNumber="56789"
```

`portNumber` rappresenta la porta remota sul nodo gestito a cui desideri reindirizzare il traffico della sessione. Ad esempio, è possibile specificare la porta 3389 per connetterti a un nodo Windows utilizzando il protocollo RDP (Remote Desktop Protocol). Se non specifichi il parametro `portNumber`, Session Manager utilizza 80 come valore predefinito.

`localPortNumber` è la porta del computer locale da cui inizia il traffico, ad esempio 56789. Questo valore è ciò che immetti quando ti connetti a un nodo gestito utilizzando un client. Ad esempio, **localhost:56789**.

Per informazioni sulle altre opzioni utilizzabili con il `start-session` comando, [start-session](#) consultate la AWS Systems Manager sezione del AWS CLI Command Reference.

Per ulteriori informazioni sulle sessioni di inoltro delle porte, consulta [Inoltro della porta tramite AWS Systems Manager Session Manager](#) nel Blog di notizie AWS .

Avvio di una sessione (inoltro alla porta a un host remoto)

Per avviare una sessione di inoltro alla porta Session Manager a un host remoto, sul nodo gestito deve essere installata la versione 3.1.1374.0 o successiva di SSM Agent. Non è necessario che l'host remoto sia gestito da Systems Manager.

Note

Prima di avviare una sessione, assicurati di aver completato la procedura di configurazione per Session Manager. Per informazioni, consulta [Configurazione di Session Manager](#). Per utilizzare i comandi AWS CLI per eseguire la sessione, è necessario installare il Session Manager plug-in sul computer locale. Per informazioni, consulta [Installa il Session Manager plugin per AWS CLI](#).

A seconda del sistema operativo e dello strumento da riga di comando, il posizionamento delle virgolette può variare e potrebbero essere necessari caratteri di escape.

Per avviare una sessione di inoltro alla porta, esegui il comando seguente dalla AWS CLI: Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux & macOS

```
aws ssm start-session \
  --target instance-id \
  --document-name AWS-StartPortForwardingSessionToRemoteHost \
  --parameters '{"host":["mydb.example.us-east-2.rds.amazonaws.com"],"portNumber":
["3306"], "localPortNumber":["3306"]}'
```

Windows

```
aws ssm start-session ^
  --target instance-id ^
  --document-name AWS-StartPortForwardingSessionToRemoteHost ^
  --parameters host="mydb.example.us-
east-2.rds.amazonaws.com",portNumber="3306",localPortNumber="3306"
```

Il valore `host` rappresenta il nome host o l'indirizzo IP dell'host remoto a cui vuoi connetterti. I requisiti generali di connettività e risoluzione dei nomi tra il nodo gestito e l'host remoto continuano a essere validi.

`portNumber` rappresenta la porta remota sul nodo gestito a cui desideri reindirizzare il traffico della sessione. Ad esempio, è possibile specificare la porta 3389 per connetterti a un nodo Windows utilizzando il protocollo RDP (Remote Desktop Protocol). Se non specifichi il parametro `portNumber`, Session Manager utilizza 80 come valore predefinito.

`localPortNumber` è la porta del computer locale da cui inizia il traffico, ad esempio 56789. Questo valore è ciò che immetti quando ti connetti a un nodo gestito utilizzando un client. Ad esempio, **localhost:56789**.

Per informazioni sulle altre opzioni utilizzabili con il `start-session` comando, [start-session](#)consultate la AWS Systems Manager sezione del AWS CLI Command Reference.

Avvio di una sessione con un'attività Amazon ECS

Session Manager supporta l'avvio di una sessione di inoltro della porta con un'attività all'interno di un cluster Amazon Elastic Container Service (Amazon ECS). Per farlo, abilita ECS Exec. Per ulteriori

informazioni, consulta [Monitoraggio dei container del servizio Amazon Elastic Container con ECS Exec](#) nella Guida per gli sviluppatori del servizio Amazon Elastic Container.

A tale scopo, è necessario aggiornare il ruolo dell'attività in IAM per includere le seguenti autorizzazioni:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource": "*"
    }
  ]
}
```

Per avviare una sessione di inoltro alla porta con un'attività Amazon ECS, esegui il comando seguente dalla AWS CLI. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Note

Rimuovi i simboli < e > dal parametro target. Questi simboli vengono forniti solo a scopo di chiarimento per il lettore.

Linux & macOS

```
aws ssm start-session \
  --target ecs:<ECS_cluster_name>_<ECS_container_ID>_<container_runtime_ID> \
  --document-name AWS-StartPortForwardingSessionToRemoteHost \
```

```
--parameters '{"host":["URL"],"portNumber":["port_number"], "localPortNumber":  
["port_number"]}'
```

Windows

```
aws ssm start-session ^  
--target ecs:<ECS_cluster_name>_<ECS_container_ID>_<container_runtime_ID> ^  
--document-name AWS-StartPortForwardingSessionToRemoteHost ^  
--parameters host="URL",portNumber="port_number",localPortNumber="port_number"
```

Avvio di una sessione (comandi interattivi e non interattivi)

Prima di avviare una sessione, assicurati di aver completato la procedura di configurazione per Session Manager. Per informazioni, consulta [Configurazione di Session Manager](#).

Per utilizzare i comandi AWS CLI per eseguire la sessione, il Session Manager plug-in deve essere installato anche sul computer locale. Per informazioni, consulta [Installa il Session Manager plugin per AWS CLI](#).

Per avviare una sessione di comando interattivo, esegui il comando seguente: Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux & macOS

```
aws ssm start-session \  
--target instance-id \  
--document-name CustomCommandSessionDocument \  
--parameters '{"logpath":["/var/log/amazon/ssm/amazon-ssm-agent.log"]}'
```

Windows

```
aws ssm start-session ^  
--target instance-id ^  
--document-name CustomCommandSessionDocument ^  
--parameters logpath="/var/log/amazon/ssm/amazon-ssm-agent.log"
```

Per informazioni sulle altre opzioni utilizzabili con il start-session comando, [start-session](#)consultate la AWS Systems Manager sezione del AWS CLI Command Reference.

Ulteriori informazioni

- [Usa l'inoltro della porta in AWS Systems Manager Session Manager per connetterti a host remoti](#)
- [Inoltro delle porte delle istanze Amazon EC2 con AWS Systems Manager](#)
- [Gestisci le risorse Microsoft AD AWS gestite con il Session Manager port forwarding](#)
- [Inoltro porta utilizzando AWS Systems ManagerSession Manager](#) sul Blog di notizie AWS .

Terminare una sessione

È possibile terminare una sessione avviata nel proprio account utilizzando la AWS Systems Manager console o il pulsante AWS Command Line Interface (AWS CLI). Quando scegli il pulsante Termina sessione per una sessione nella console o richiami l'azione [TerminateSession](#) API utilizzando il AWS CLI, termina Session Manager definitivamente la sessione e chiude la connessione dati tra il Session Manager client e SSM Agent il nodo gestito. Non è possibile riprendere una sessione terminata.

Se non vi è alcuna attività utente in una sessione aperta per 20 minuti, lo stato di inattività attiva un timeout. Session Manager non richiama `TerminateSession`, ma chiude il canale sottostante. Non è possibile riprendere una sessione chiusa a causa di un timeout di inattività.

Consigliamo sempre di terminare una sessione in modo esplicito utilizzando il `terminate-session` comando, quando si utilizza il AWS CLI, o il pulsante Termina sessione quando si utilizza la console. (I pulsanti per terminare la sessione si trovano sia nella finestra della sessione che nella pagina principale Session Manager della console). Se chiudi solo un browser o una finestra di comando, la sessione rimane nell'elenco come Attiva nella console per 30 giorni. Quando non si termina esplicitamente una sessione o quando una sessione scade, tutti i processi in esecuzione sul nodo gestito in quel momento continueranno a essere eseguiti.

Argomenti

- [Per terminare una sessione \(console\)](#)
- [Terminare una sessione \(AWS CLI\)](#)

Per terminare una sessione (console)

Puoi utilizzare la AWS Systems Manager console per terminare una sessione nel tuo account.

Per terminare una sessione (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Session Manager.
3. Per Sessions (Sessioni), scegliere il pulsante di opzione a sinistra della sessione da terminare.
4. Scegli Termina sessione.

Terminare una sessione (AWS CLI)

Per terminare una sessione utilizzando il AWS CLI, esegui il comando seguente. Sostituiscilo *session-id* con le tue informazioni.

```
aws ssm terminate-session \  
  --session-id session-id
```

Per ulteriori informazioni sul terminate-session comando, vedere [terminate-session](#) la AWS Systems Manager sezione del AWS CLI Command Reference.

Visualizzazione della cronologia delle sessioni

È possibile utilizzare la AWS Systems Manager console o il AWS Command Line Interface (AWS CLI) per visualizzare le informazioni sulle sessioni nel proprio account. Nella console, puoi visualizzare i dettagli della sessione come i seguenti:

- L'ID della sessione
- Quale utente si è connesso a un nodo gestito attraverso una sessione
- L'ID del nodo gestito
- Quando è iniziata e terminata la sessione
- Lo stato della sessione
- Il percorso specificato per l'archiviazione dei log delle sessioni (se abilitata)

Utilizzando AWS CLI, puoi visualizzare un elenco di sessioni nel tuo account, ma non i dettagli aggiuntivi disponibili nella console.

Per informazioni sul controllo e delle informazioni relative alla cronologia della sessione, consulta [Abilitazione e disabilitazione della registrazione di sessione](#).

Argomenti

- [Visualizzazione della cronologia delle sessioni \(console\)](#)
- [Visualizzazione della cronologia delle sessioni \(AWS CLI\)](#)

Visualizzazione della cronologia delle sessioni (console)

Puoi utilizzare la AWS Systems Manager console per visualizzare i dettagli sulle sessioni del tuo account.

Visualizzazione della cronologia delle sessioni (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Session Manager.
3. Scegli la scheda Cronologia delle sessioni.

oppure

Se la home page si apre per prima Session Manager, scegli Configura preferenze, quindi scegli la scheda Cronologia delle sessioni.

Visualizzazione della cronologia delle sessioni (AWS CLI)

Per visualizzare un elenco di sessioni nel tuo account utilizzando il AWS CLI, esegui il comando seguente.

```
aws ssm describe-sessions \  
  --state History
```

Note

Questo comando restituisce solo i risultati per le connessioni alle destinazioni avviate utilizzando Session Manager. Non elenca le connessioni effettuate tramite altri mezzi, ad esempio Remote Desktop Protocol (RDP) o Secure Shell Protocol (SSH).

Per informazioni sulle altre opzioni che è possibile utilizzare con il describe-sessions comando, vedere [describe-sessions](#) la AWS Systems Manager sezione della Guida ai AWS CLI comandi.

Attività di registrazione delle sessioni

Oltre a fornire informazioni sulle sessioni correnti e completate nella console Systems Manager, Session Manager fornisce le opzioni per la verifica e la registrazione dell'attività delle sessioni nell'Account AWS tramite AWS CloudTrail.

CloudTrail acquisisce le chiamate API di sessione tramite la console Systems Manager, AWS Command Line Interface (AWS CLI) e Systems Manager SDK. Puoi visualizzare le informazioni sulla CloudTrail console o archivarle in un bucket Amazon Simple Storage Service (Amazon S3) specificato. Un bucket Amazon S3 viene utilizzato per tutti i CloudTrail log del tuo account. Per ulteriori informazioni, consulta [Registrazione dei log AWS Systems Manager Chiamate API con AWS CloudTrail](#).

Note

[Per un'analisi ricorrente, storica e analitica dei tuoi file di registro, prendi in considerazione la possibilità di interrogare i CloudTrail log utilizzando CloudTrail Lake o una tabella gestita da te.](#) Per ulteriori informazioni, consulta [Interrogare i AWS CloudTrail log](#) nella Guida per l'utente.AWS CloudTrail

Monitoraggio dell'attività della sessione tramite Amazon EventBridge (console)

Con EventBridge, puoi configurare regole per rilevare quando avvengono modifiche alle AWS risorse. È possibile creare una regola per rilevare quando un utente della tua organizzazione avvia o termina una sessione e quindi, ad esempio, ricevere una notifica sull'evento tramite Amazon SNS.

EventBridge il supporto per Session Manager si basa sui record delle operazioni API che sono stati registrati da CloudTrail. (È possibile utilizzare l' CloudTrail integrazione con EventBridge per rispondere alla maggior parte AWS Systems Manager degli eventi.) Le azioni eseguite all'interno di una sessione, ad esempio un `exit` comando, che non effettuano una chiamata API non vengono rilevate da EventBridge.

La procedura seguente illustra come avviare le notifiche tramite Amazon Simple Notification Service (Amazon SNS) quando si verifica un evento API Session Manager, ad esempio `StartSession`.

Per monitorare l'attività della sessione utilizzando Amazon EventBridge (console)

1. Creare un argomento Amazon SNS da utilizzare per l'invio di notifiche quando si verifica l'evento del Session Manager che si desidera monitorare.

Per ulteriori informazioni, consulta la pagina [Creazione di un argomento](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service.

2. Crea una EventBridge regola per richiamare il target Amazon SNS per il tipo Session Manager di evento che desideri monitorare.

Per informazioni su come creare la regola, consulta la sezione [Creazione di EventBridge regole Amazon che reagiscono agli eventi](#) nella Amazon EventBridge User Guide.

Durante la procedura per la creazione della regola, effettuare le selezioni seguenti:

- Per AWS , scegli Systems Manager.
- Per il tipo di evento, scegli AWS API Call through CloudTrail.
- Scegli Operazioni specifiche, quindi immetti i comandi del Session Manager (uno alla volta) per cui si desidera ricevere le notifiche. Puoi scegliere StartSessionResumeSession, eTerminateSession. (EventBridge non supporta Get* List* i Describe* comandi e.)
- Per Seleziona una destinazione, scegli Argomento SNS. Per Argomento, scegli il nome dell'argomento Amazon SNS creato nella Fase 1.

Per ulteriori informazioni, consulta la [Amazon EventBridge User Guide](#) e la [Amazon Simple Notification Service Getting Started Guide](#).

Abilitazione e disabilitazione della registrazione di sessione

La registrazione di sessione registra le informazioni sulle sessioni correnti e completate nella console di Systems Manager. È inoltre possibile registrare nell' Account AWS i dettagli sui comandi eseguiti durante le sessioni. La registrazione della sessione consente di effettuare le seguenti operazioni:

- Creare e memorizzare i log delle sessioni a scopo di archiviazione.
- Generare un report che mostra i dettagli di ogni connessione effettuata ai tuoi nodi gestiti tramite il Session Manager negli ultimi 30 giorni.
- Genera notifiche per l'accesso alla sessione Account AWS, ad esempio le notifiche di Amazon Simple Notification Service (Amazon SNS).
- Avvia automaticamente un'altra azione su una AWS risorsa a seguito di azioni eseguite durante una sessione, come l'esecuzione di una AWS Lambda funzione, l'avvio di una AWS CodePipeline pipeline o l'esecuzione di un documento. AWS Systems Manager Run Command

Important

Tieni presenti i seguenti requisiti e limitazioni su Session Manager:

- Session Manager registra i comandi immessi e il loro output durante una sessione a seconda delle preferenze di sessione. Per evitare che i dati sensibili, ad esempio le password, vengano visualizzati nei log di sessione, è consigliabile utilizzare i seguenti comandi quando si immettono dati sensibili durante una sessione.

Linux & macOS

```
stty -echo; read passwd; stty echo;
```

Windows

```
$Passwd = Read-Host -AsSecureString
```

- Se utilizzi Windows Server 2012 o le versioni precedenti, i dati nei log potrebbero non essere formattati in modo ottimale. Ti consigliamo di usare Windows Server 2012 R2 o le versioni successive per ottimizzare il formato dei log.
- Se utilizzi Linux o macOS gestisci nodi, assicurati che l'utilità screen sia installata. In caso contrario, i dati di log potrebbero essere troncati. Su Amazon Linux 2, AL2023 e Ubuntu Server, l'utilità dello schermo è installata per impostazione predefinita. Per installare lo schermo manualmente, a seconda della versione di Linux, esegui `sudo yum install screen` o `sudo apt-get install screen`.
- La registrazione non è disponibile per sessioni Session Manager che si connettono tramite inoltro porta o SSH. Questo perché SSH crittografa tutti i dati della sessione all'interno della connessione TLS sicura stabilita tra gli Session Manager endpoint AWS CLI e funge Session Manager solo da tunnel per le connessioni SSH.

Per ulteriori informazioni sulle autorizzazioni necessarie per utilizzare Amazon S3 o Amazon CloudWatch Logs per la registrazione dei dati delle sessioni, consulta [Creazione di un ruolo IAM con autorizzazioni per Session Manager e Amazon S3 e CloudWatch Logs \(console\)](#)

Per ulteriori informazioni sulle opzioni di registrazione di Session Manager, consulta i seguenti argomenti.

Argomenti

- [Streaming dei dati delle sessioni tramite Amazon CloudWatch Logs \(console\)](#)
- [Registrazione dei dati delle sessioni mediante Amazon S3 \(console\)](#)
- [Registrazione dei dati della sessione tramite Amazon CloudWatch Logs \(console\)](#)
- [Configurazione della registrazione di sessione su disco](#)
- [Regolazione della durata del Session Manager il file di registro temporaneo è memorizzato su disco](#)
- [Disabilitazione Session Manager accesso a CloudWatch Logs e Amazon S3](#)

Streaming dei dati delle sessioni tramite Amazon CloudWatch Logs (console)

Puoi inviare un flusso continuo di registri dei dati delle sessioni ad Amazon CloudWatch Logs. I dettagli essenziali, come i comandi eseguiti da un utente in una sessione, l'ID dell'utente che ha eseguito i comandi e i timestamp relativi alla trasmissione dei dati della sessione ai CloudWatch log, sono inclusi nello streaming dei dati delle sessioni. Durante lo streaming dei dati delle sessioni, i log servono JSON-formatted ad aiutarti a integrarti con le tue soluzioni di registrazione esistenti. I dati della sessione di streaming non sono supportati per i comandi interattivi.

Note

Per trasmettere i dati di sessione da nodi gestiti Windows Server, è necessario disporre di PowerShell 5.1 o versione successiva installata. Per impostazione predefinita, Windows Server 2016 e versioni successive hanno installato la versione di PowerShell richiesta. Tuttavia, Windows Server 2012 e 2012 R2 non hanno la versione di PowerShell richiesta installata per impostazione predefinita. Se PowerShell non è stato ancora aggiornato nei nodi gestiti Windows Server 2012 o 2012 R2, è possibile farlo utilizzando Run Command. Per informazioni sull'aggiornamento di PowerShell utilizzando Run Command, consulta [Aggiornamento tramite PowerShell Run Command](#).

Important

Se hai configurato l'impostazione dei criteri di PowerShell trascrizione nei nodi Windows Server gestiti, non sarai in grado di eseguire lo streaming dei dati delle sessioni.

Per trasmettere i dati delle sessioni utilizzando Amazon CloudWatch Logs (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Session Manager.
3. Scegli la scheda Preferenze, quindi seleziona Modifica.
4. Seleziona la casella di controllo accanto a **Abilita in CloudWatch registrazione**.
5. Seleziona l'opzione Log delle sessioni di streaming.
6. (Consigliato) Seleziona la casella di controllo accanto a **Consenti solo gruppi di CloudWatch log crittografati**. Se questa opzione è attivata, i dati di log vengono crittografati utilizzando la chiave di crittografia lato server specificata per il gruppo di log. Se non desideri crittografare i dati di registro inviati a CloudWatch Logs, deseleziona la casella di controllo. È inoltre necessario deselezionare la casella di controllo se la crittografia non è abilitata nel gruppo di log.
7. Per CloudWatch i log, per specificare il gruppo di CloudWatch log Logs esistente nel quale Account AWS caricare i log delle sessioni, seleziona una delle seguenti opzioni:
 - Immetti il nome di un gruppo di log nella casella di testo che è già stato creato nell'account per archiviare i dati di log della sessione.
 - Esplora gruppi di log: seleziona un gruppo di log che è già stato creato nel tuo account per archiviare i dati di log della sessione.
8. Scegli Save (Salva).

Registrazione dei dati delle sessioni mediante Amazon S3 (console)

Puoi scegliere di archiviare i dati di log delle sessioni in un bucket Amazon Simple Storage Service (Amazon S3) di tua scelta a scopi di debug e risoluzione dei problemi. L'opzione predefinita comporta l'invio dei log a un bucket Amazon S3 crittografato. La crittografia viene eseguita utilizzando la chiave specificata per il bucket, una AWS KMS key o una chiave Amazon S3 Server-Side Encryption (SSE) (). AES-256

Important

Quando si utilizzano bucket in stile hosting virtuale con Secure Sockets Layer (SSL), il certificato jolly SSL confronta solo i bucket che non contengono punti. Per risolvere questo problema, utilizzare HTTP o scrivere una logica di verifica del certificato personalizzata.

Consigliamo di non utilizzare punti (".") nei nomi dei bucket quando si utilizzano bucket in stile hosting virtuale.

Crittografia bucket Amazon S3

Per inviare i log al tuo bucket Amazon S3 con crittografia, la crittografia deve essere consentita nel bucket. Per ulteriori informazioni sulla crittografia del bucket Amazon S3, consulta [Crittografia di default di Amazon S3 per bucket S3](#).

Chiave gestita dal cliente

Se utilizzi una chiave KMS da te gestita per crittografare il tuo bucket, il profilo dell'istanza IAM collegato alle tue istanze deve disporre di autorizzazioni esplicite per leggere la chiave. Se usi una Chiave gestita da AWS, l'istanza non richiede questa autorizzazione esplicita. Per ulteriori informazioni su come fornire al profilo dell'istanza l'accesso a utilizzare la chiave, consulta [Consenti agli utenti della chiave di utilizzare la chiave](#) nella Guida per sviluppatori AWS Key Management Service .

Segui questa procedura per configurare il Session Manager per archiviare i registri delle sessioni in un bucket Amazon S3.

Note

Puoi anche utilizzarlo AWS CLI per specificare o modificare il bucket Amazon S3 a cui vengono inviati i dati della sessione. Per informazioni, consulta [Aggiornamento delle preferenze Session Manager \(riga di comando\)](#).

Per registrare i dati delle sessioni mediante Amazon S3 (console)

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Session Manager.
3. Scegli la scheda Preferenze, quindi seleziona Modifica.
4. Seleziona la casella di controllo accanto ad Abilitazione sotto Registrazione S3.
5. (Opzione consigliata) Selezionare la casella di controllo accanto a Consenti solo bucket S3 crittografati. Se questa opzione è attivata, i dati di log vengono crittografati utilizzando la chiave

di crittografia lato server specificata per il bucket. Se non si desidera crittografare i dati di log inviati a Amazon S3, deselezionare la casella di controllo. Se la crittografia non è abilitata nel bucket S3, è necessario anche deselezionare la casella di controllo.

6. Per Nome bucket S3, seleziona una delle opzioni seguenti:

 Note

Consigliamo di non utilizzare punti (".") nei nomi dei bucket quando si utilizzano bucket in stile hosting virtuale. Per ulteriori informazioni su come formattare i nomi dei bucket Amazon S3, consulta [Restrizioni e limitazioni dei bucket](#) nella Guida per gli utenti di Amazon Simple Storage Service.

- Scegli un bucket nell'elenco: seleziona un bucket Amazon S3 che è già stato creato nel proprio account per archiviare i dati di log delle sessioni.
 - Immetti un nome di bucket nella casella di testo: immetti il nome del bucket Amazon S3 che è già stato creato nell'account per archiviare i dati di log delle sessioni.
7. (Facoltativo) Per Prefisso della chiave S3, immetti il nome di una cartella nuova o esistente per archiviare i log nel bucket selezionato.
8. Scegli Salva.

Per ulteriori informazioni su Simple Storage Service (Amazon S3) e i bucket Amazon S3, consulta [Guida per l'utente di Amazon Simple Storage Service](#) e [Guida per l'utente di Amazon Simple Storage Service](#).

Registrazione dei dati della sessione tramite Amazon CloudWatch Logs (console)

Con Amazon CloudWatch Logs, puoi monitorare, archiviare e accedere a file di registro da diversi Servizi AWS file. Puoi inviare i dati dei log di sessione a un gruppo di log CloudWatch Logs per scopi di debug e risoluzione dei problemi. L'opzione predefinita comporta l'invio dei dati di log con la crittografia utilizzando la chiave KMS, ma puoi trasmettere i dati al gruppo di log con o senza crittografia.

Segui questi passaggi per configurare AWS Systems Manager Session Manager l'invio dei dati del registro di sessione a un gruppo di log di CloudWatch Logs al termine delle sessioni.

 Note

È inoltre possibile utilizzare il AWS CLI per specificare o modificare il gruppo di log CloudWatch Logs a cui vengono inviati i dati della sessione. Per informazioni, consulta [Aggiornamento delle preferenze Session Manager \(riga di comando\)](#).

Per registrare i dati della sessione utilizzando Amazon CloudWatch Logs (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Session Manager.
3. Scegli la scheda Preferenze, quindi seleziona Modifica.
4. Seleziona la casella di controllo accanto a Abilita nella sezione CloudWatch Registrazione.
5. Seleziona l'opzione Carica log della sessione.
6. (Consigliato) Seleziona la casella di controllo accanto a Consenti solo gruppi di CloudWatch log crittografati. Se questa opzione è attivata, i dati di log vengono crittografati utilizzando la chiave di crittografia lato server specificata per il gruppo di log. Se non desideri crittografare i dati di registro inviati ai CloudWatch registri, deselecta la casella di controllo. È inoltre necessario deselectare la casella di controllo se la crittografia non è abilitata nel gruppo di log.
7. Per CloudWatch i log, per specificare il gruppo di log CloudWatch Logs esistente nel gruppo in cui Account AWS caricare i log delle sessioni, seleziona una delle seguenti opzioni:
 - Scegli un gruppo di log nell'elenco: seleziona un gruppo di log che è già stato creato nel tuo account per archiviare i dati di log della sessione.
 - Immetti un nome di bucket nella casella di testo: immetti il nome di un gruppo di log che è già stato creato nell'account per archiviare i dati di log della sessione.
8. Scegli Save (Salva).

Per ulteriori informazioni sull'utilizzo dei CloudWatch log, consulta la [Amazon CloudWatch Logs User Guide](#).

Configurazione della registrazione di sessione su disco

Dopo aver abilitato Session Manager la registrazione su Amazon S3, tutti i comandi eseguiti durante una sessione (e l'output risultante da tali comandi) vengono registrati in un file temporaneo sul disco dell'istanza di destinazione. CloudWatch Il file temporaneo è denominato `ipcTempFile.log`.

`ipcTempFile.log` è controllato dal parametro `SessionLogsDestination` nel file di configurazione dell'SSM Agent. Questo parametro accetta i seguenti valori:

- `disco`: se specifichi questo parametro e la registrazione della sessione su Amazon S3 è abilitataSSM Agent, crea `ipcTempFile.log` il file di registro temporaneo e registra i comandi e l'output della sessione su disco. CloudWatch Session Managercarica questo registro su S3 o durante CloudWatch o dopo la sessione, a seconda della configurazione di registrazione. Il log viene quindi eliminato in base alla durata specificata per il parametro di configurazione `SessionLogsRetentionDurationHours` di SSM Agent.

Se specifichi questo parametro e la registrazione della sessione su Amazon S3 è disabilitataSSM Agent, registra comunque la cronologia dei comandi e l'output nel file. CloudWatch `ipcTempFile.log` Il file verrà eliminato in base alla durata specificata per il parametro di configurazione `SessionLogsRetentionDurationHours` di SSM Agent.

- `none`: se specifichi questo parametro e la registrazione della sessione su Amazon S3 è abilitata, la registrazione su disco funziona esattamente come se avessi specificato il parametro. CloudWatch `disk` SSM Agentrichiede il file temporaneo quando la registrazione della sessione su Amazon S3 CloudWatch o Amazon S3 è abilitata.

Se specifichi questo parametro e la registrazione della sessione su Amazon S3 è disabilitataSSM Agent, non crea `ipcTempFile.log` il file. CloudWatch

Utilizza la seguente procedura per abilitare o disabilitare la creazione del file di log `ipcTempFile.log` temporaneo su disco all'avvio di una sessione.

Per abilitare o disabilitare la creazione del file di log temporaneo di Session Manager su disco

1. Installa l'SSM Agent sull'istanza o esegui l'aggiornamento alla versione 3.2.2086 o successiva. Per informazioni su come verificare il numero della versione dell'agente, consulta [Verifica del Agente SSM numero di versione](#). Per informazioni su come installare manualmente l'agente, individua la procedura per il sistema operativo nelle seguenti sezioni:
 - [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#)

- [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per macOS](#)
 - [Installazione e disinstallazione manuali Agente SSM su istanze EC2 per Windows Server](#)
2. Connettiti all'istanza e individua il file `amazon-ssm-agent.json` nella seguente posizione.
 - Linux://ssm/ etc/amazon
 - macOS://ssm/ opt/aws
 - Windows Server: C:\Program Files\Amazon\SSM

Se il file `amazon-ssm-agent.json` non esiste, copia i contenuti di `amazon-ssm-agent.json.template` in un nuovo file nella stessa directory. Assegna un nome al nuovo file `amazon-ssm-agent.json`.

3. Specifica tra `none` or `disk` per il parametro `SessionLogsDestination`. Salvare le modifiche.
4. [Riavviare](#) SSM Agent.

Se si specifica `disk` per il parametro `SessionLogsDestination`, è possibile verificare che l'SSM Agent crei il file di log temporaneo avviando una nuova sessione, per poi posizionare `ipcTempFile.log` nella seguente posizione:

- Linux:///var/lib/amazon/ssm`target ID`.log session/orchestration `session ID` Standard_Stream/ ipcTempFile
- macOS:/opt/aws/ssm/data//`target ID`session/orchestration`session ID`.log Standard_Stream/ ipcTempFile
- Windows Server: C:\ProgramData\Amazon\SSM\InstanceData\`target ID` sessione\ orchestrazione\\ ipc `session ID` Standard_Stream TempFile.log

Note

Per impostazione predefinita, il file di log temporaneo viene salvato sull'istanza per 14 giorni.

Per aggiornare il parametro `SessionLogsDestination` su più istanze, è consigliato creare un documento SSM che specifichi la nuova configurazione. È quindi possibile utilizzare Systems Manager Run Command per implementare la modifica sulle istanze. Per ulteriori informazioni,

consulta [Scrivere i propri AWS Systems Manager documenti \(blog\)](#) e [Esecuzione di comandi su nodi gestiti](#)

Regolazione della durata del Session Manager il file di registro temporaneo è memorizzato su disco

Dopo aver abilitato la Session Manager registrazione su Amazon S3, tutti i comandi eseguiti durante una sessione (e l'output risultante da tali comandi) vengono registrati in un file temporaneo sul disco dell'istanza di destinazione. CloudWatch Il file temporaneo è denominato `ipcTempFile.log`. Durante una sessione, o al termine, Session Manager carica questo registro temporaneo su uno o su S3. CloudWatch Il log temporaneo viene quindi eliminato in base alla durata specificata per il parametro di configurazione SSM Agent `SessionLogsRetentionDurationHours`. Per impostazione predefinita, il file di log temporaneo viene salvato sull'istanza per 14 giorni nella seguente posizione:

- Linux: `//var/lib/amazon/ssm/target ID/session/orchestration/.log session ID Standard_Stream/ ipcTempFile`
- macOS: `//opt/aws/ssm/data/target ID/session/orchestrationsession ID/.log Standard_Stream/ ipcTempFile`
- Windows Server: `C:\ProgramData\Amazon\SSM\InstanceData\target ID\ sessione\ orchestrazione\\ ipc session ID Standard_Stream TempFile.log`

Utilizza la procedura seguente per modificare la durata di archiviazione del file di log temporaneo di Session Manager su disco.

Per regolare la durata di archiviazione del TempFile.log **file** ipc su disco

1. Connettiti all'istanza e individua il file `amazon-ssm-agent.json` nella seguente posizione.

- Linux: `//ssm/ etc/amazon`
- macOS: `//ssm/ opt/aws`
- Windows Server: `C:\Program Files\Amazon\SSM`

Se il file `amazon-ssm-agent.json` non esiste, copia i contenuti di `amazon-ssm-agent.json.template` in un nuovo file nella stessa directory. Assegna un nome al nuovo file `amazon-ssm-agent.json`.

2. Modifica il valore di `SessionLogsRetentionDurationHours` nel numero di ore desiderato. Se `SessionLogsRetentionDurationHours` è impostato su 0, il file di log temporaneo viene

creato durante la sessione ed eliminato al termine della stessa. Questa impostazione dovrebbe garantire che il file di registro non persista dopo la fine della sessione.

3. Salvare le modifiche.
4. [Riavviare](#) SSM Agent.

Disabilitazione Session Manager accesso a CloudWatch Logs e Amazon S3

Puoi utilizzare la console Systems Manager o AWS CLI disabilitare la registrazione delle sessioni nel tuo account.

Per disabilitare la registrazione di sessione (console)

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Session Manager.
3. Scegli la scheda Preferenze, quindi seleziona Modifica.
4. Per disabilitare la CloudWatch registrazione, nella sezione CloudWatch registrazione, deseleziona la casella di controllo Abilita.
5. Per disabilitare la registrazione di S3, nella sezione Registrazione di S3, deseleziona la casella di controllo Abilita.
6. Selezionare Salva.

Per disattivare la registrazione della sessione (AWS CLI)

Per disabilitare la registrazione della sessione utilizzando il AWS CLI, segui le istruzioni in. [Aggiornamento delle preferenze Session Manager \(riga di comando\)](#)

Nel tuo file JSON, assicurati che gli `c1oudWatchLogGroupName` input `s3BucketName` e non contengano valori. Ad esempio:

```
"inputs": {
  "s3BucketName": "",
  ...
  "c1oudWatchLogGroupName": "",
  ...
}
```

In alternativa, per disabilitare la registrazione, è possibile rimuovere tutti gli input `S3*` e `cloudWatch*` dal file JSON.

Note

A seconda della configurazione, dopo aver disabilitato CloudWatch o S3, potrebbe ancora essere generato su disco un file di registro temporaneo da SSM Agent. Per informazioni su come disabilitare la registrazione su disco, consulta [Configurazione della registrazione di sessione su disco](#).

Schema documento di sessione

Le seguenti informazioni descrivono gli elementi dello schema di un documento di sessione. AWS Systems Manager Session Manager utilizza i documenti di sessione per determinare il tipo di sessione da avviare, ad esempio una sessione standard, una sessione di port forwarding o una sessione per eseguire un comando interattivo.

[schemaVersion](#)

Versione dello schema del documento di sessione. I documenti delle sessioni supportano solo la versione 1.0.

Tipo: stringa

Obbligatorio: sì

[description](#)

Descrizione specificata per il documento di sessione. Ad esempio, «Documento per avviare la sessione di inoltro della porta con Session Manager».

■ Tipo: stringa

Obbligatorio: no

[sessionType](#)

Il tipo di sessione che il documento di sessione viene utilizzato per stabilire.

Tipo: stringa

Obbligatorio: sì

Valori validi: `InteractiveCommands`| `NonInteractiveCommands`| `Port`| `Standard_Stream`
[inputs](#)

Preferenze di sessione da utilizzare per le sessioni stabilite utilizzando questo documento di sessione. Questo elemento è necessario per i documenti di sessione utilizzati per creare sessioni `Standard_Stream`.

Tipo: `StringMap`

Obbligatorio: no

[s3BucketName](#)

Il bucket Amazon Simple Storage Service (Amazon S3) a cui desideri inviare i log delle sessioni al termine delle sessioni.

Tipo: `string`

Obbligatorio: no

[s3KeyPrefix](#)

Il prefisso da utilizzare quando si inviano i log al bucket Amazon S3 specificato nell'input `s3BucketName`. Per ulteriori informazioni sull'utilizzo di un prefisso condiviso con gli oggetti archiviati in Amazon S3, consulta [Come si utilizzano le cartelle in un bucket S3?](#) nella Guida per l'utente di Amazon Simple Storage Service.

■Tipo: `stringa`

Obbligatorio: no

[s3EncryptionEnabled](#)

Se impostato su `true`, il bucket Amazon S3 specificato nell'input `s3BucketName` deve essere crittografato.

Tipo: `Booleano`

Obbligatorio: sì

[cloudWatchLogGroupName](#)

Il nome del gruppo Amazon CloudWatch Logs (CloudWatch Logs) a cui desideri inviare i log di sessione al termine delle sessioni.

■Tipo: stringa

Obbligatorio: no

[cloudWatchEncryptionEnabled](#)

Se impostato su `true`, il gruppo di log specificato nell'input `cloudWatchLogGroupName` deve essere crittografato.

Tipo: Booleano

Obbligatorio: sì

[cloudWatchStreamingEnabled](#)

Se impostato su `true`, un flusso continuo di log di dati delle sessioni viene inviato al gruppo di log specificato nell'input `cloudWatchLogGroupName`. Se impostati su `false`, i log delle sessioni vengono inviati al gruppo di log specificato nell'input di `cloudWatchLogGroupName` alla fine delle sessioni.

Tipo: Booleano

Obbligatorio: sì

[kmsKeyId](#)

L'ID che AWS KMS key desideri utilizzare per crittografare ulteriormente i dati tra i computer client locali e i nodi gestiti da Amazon Elastic Compute Cloud (Amazon EC2) a cui ti connetti.

■Tipo: stringa

Obbligatorio: no

[runAsEnabled](#)

Se impostato su `true`, devi specificare un account utente presente nei nodi gestiti a cui ti stai connettendo nell'input `runAsDefaultUser`. In caso contrario, le sessioni non verranno avviate. Per impostazione predefinita, le sessioni vengono avviate utilizzando `ssm-user` creato dall'account AWS Systems Manager SSM Agent. La funzionalità Esegui come è supportata solo per la connessione con Linux ai nodi gestiti da macOS.

Tipo: Booleano

Obbligatorio: sì

runAsDefaultUser

Il nome dell'account utente per avviare le sessioni con i nodi gestiti da Linux e macOS, quando l'input `runAsEnabled` è impostato su `true`. L'account utente specificato per questo input deve esistere nei nodi gestiti a cui ci si connette; in caso contrario, le sessioni non verranno avviate. Nel determinare quale account utente del sistema operativo utilizzare, Session Manager controlla nel seguente ordine: il `SSMSessionRunAs` tag sui tag di sessione dell'utente IAM, quindi il `SSMSessionRunAs` tag sul ruolo IAM assunto e infine questo `runAsDefaultUser` valore nelle preferenze di sessione. Per ulteriori informazioni, consulta [Attiva il supporto Run As per Linux and macOS nodi gestiti](#).

─Tipo: stringa

Obbligatorio: no

idleSessionTimeout

La quantità di tempo di inattività che si desidera consentire prima del termine di una sessione. Questo input viene misurato in minuti.

Tipo: stringa

Valori validi: 1-60

Obbligatorio: no

maxSessionDuration

La quantità di tempo che si desidera permettere prima del termine di una sessione. Questo input viene misurato in minuti.

Tipo: stringa

Valori validi: 1-1440

Obbligatorio: no

shellProfile

Le preferenze specificate per il sistema operativo da applicare alle sessioni quali le preferenze della shell, le variabili di ambiente, le directory di lavoro e l'esecuzione di più comandi all'avvio di una sessione.

Tipo: StringMap

Obbligatorio: no

[windows](#)

Le preferenze della shell, le variabili di ambiente, le directory di lavoro e i comandi specificati per le sessioni sui nodi gestiti Windows Server.

─Tipo: stringa

Obbligatorio: no

[linux](#)

Le preferenze della shell, le variabili di ambiente, le directory di esecuzione e i comandi specificati per le sessioni sui nodi gestiti da Linux e macOS.

Tipo: stringa

Obbligatorio: no

[parameters](#)

Una struttura che definisce i parametri accettati dal documento. Per ulteriori informazioni su come specificare i parametri del documento, consulta Parametri di definizione del processo nella [Top-level elementi di dati](#). Per i parametri a cui fai spesso riferimento, è consigliabile archiviare questi parametri in Systems Manager Parameter Store e farvi riferimento. Puoi fare riferimento ai parametri String, StringList e Parameter Store in questa sezione di un documento. Puoi fare riferimento ai parametri Parameter Store SecureString in questa sezione di un documento. È possibile fare riferimento a un parametro Parameter Store utilizzando il seguente formato.

```
{{ssm:parameter-name}}
```

Per ulteriori informazioni su Parameter Store, consultare [AWS Systems Manager Parameter Store](#).

Tipo: StringMap

Obbligatorio: no

[properties](#)

Un oggetto i cui valori specificati vengono utilizzati nell' operazione API `StartSession`.

Per i documenti di sessione utilizzati per sessioni `InteractiveCommands`, l'oggetto proprietà include i comandi da eseguire nei sistemi operativi specificati. Puoi inoltre determinare se i comandi vengono eseguiti come `root` utilizzando la proprietà booleana `runAsElevated`. Per ulteriori informazioni consulta [Limitare l'accesso ai comandi in una sessione](#).

Per i documenti di sessione utilizzati per sessioni `Port`, l'oggetto proprietà contiene il numero di porta verso cui deve essere reindirizzato il traffico. Per un esempio, consulta il documento di Sessione tipo `Port` più avanti in questo argomento.

Tipo: `StringMap`

Obbligatorio: no

Esempio di documento di sessione tipo `Standard_Stream`

YAML

```
---
schemaVersion: '1.0'
description: Document to hold regional settings for Session Manager
sessionType: Standard_Stream
inputs:
  s3BucketName: ''
  s3KeyPrefix: ''
  s3EncryptionEnabled: true
  cloudWatchLogGroupName: ''
  cloudWatchEncryptionEnabled: true
  cloudWatchStreamingEnabled: true
  kmsKeyId: ''
  runAsEnabled: true
  runAsDefaultUser: ''
  idleSessionTimeout: '20'
  maxSessionDuration: '60'
  shellProfile:
    windows: ''
    linux: ''
```

JSON

```
{
  "schemaVersion": "1.0",
  "description": "Document to hold regional settings for Session Manager",
```

```

"sessionType": "Standard_Stream",
"inputs": {
  "s3BucketName": "",
  "s3KeyPrefix": "",
  "s3EncryptionEnabled": true,
  "cloudWatchLogGroupName": "",
  "cloudWatchEncryptionEnabled": true,
  "cloudWatchStreamingEnabled": true,
  "kmsKeyId": "",
  "runAsEnabled": true,
  "runAsDefaultUser": "",
  "idleSessionTimeout": "20",
  "maxSessionDuration": "60",
  "shellProfile": {
    "windows": "date",
    "linux": "pwd;ls"
  }
}
}

```

Esempio di documento di sessione tipo InteractiveCommands

YAML

```

---
schemaVersion: '1.0'
description: Document to view a log file on a Linux instance
sessionType: InteractiveCommands
parameters:
  logpath:
    type: String
    description: The log file path to read.
    default: "/var/log/amazon/ssm/amazon-ssm-agent.log"
    allowedPattern: "^[a-zA-Z0-9-_/]+(.log)$"
properties:
  linux:
    commands: "tail -f {{ logpath }}"
    runAsElevated: true

```

JSON

```
{
```

```

"schemaVersion": "1.0",
"description": "Document to view a log file on a Linux instance",
"sessionType": "InteractiveCommands",
"parameters": {
  "logpath": {
    "type": "String",
    "description": "The log file path to read.",
    "default": "/var/log/amazon/ssm/amazon-ssm-agent.log",
    "allowedPattern": "^[a-zA-Z0-9-_/]+(.log)$"
  }
},
"properties": {
  "linux": {
    "commands": "tail -f {{ logpath }}",
    "runAsElevated": true
  }
}
}

```

Esempio di documento di sessione tipo Port

YAML

```

---
schemaVersion: '1.0'
description: Document to open given port connection over Session Manager
sessionType: Port
parameters:
  paramExample:
    type: string
    description: document parameter
properties:
  portNumber: anyPortNumber

```

JSON

```

{
  "schemaVersion": "1.0",
  "description": "Document to open given port connection over Session Manager",
  "sessionType": "Port",
  "parameters": {
    "paramExample": {

```

```
        "type": "string",
        "description": "document parameter"
      }
    },
    "properties": {
      "portNumber": "anyPortNumber"
    }
  }
}
```

Esempio di documento di sessione con caratteri speciali

YAML

```
---
schemaVersion: '1.0'
description: Example document with quotation marks
sessionType: InteractiveCommands
parameters:
  Test:
    type: String
    description: Test Input
    maxChars: 32
properties:
  windows:
    commands: |
      $Test = '{{ Test }}'
      $myVariable = "\"Computer name is $env:COMPUTERNAME\""
      Write-Host "Test variable: $myVariable`. `nInput parameter: $Test"
    runAsElevated: false
```

JSON

```
{
  "schemaVersion": "1.0",
  "description": "Test document with quotation marks",
  "sessionType": "InteractiveCommands",
  "parameters": {
    "Test": {
      "type": "String",
      "description": "Test Input",
      "maxChars": 32
    }
  }
}
```

```
    },
    "properties":{
      "windows":{
        "commands":[
          "$Test = '{{ Test }}'",
          "$myVariable = \\\\"Computer name is $env:COMPUTERNAME\\\\""",
          "Write-Host \\"Test variable: $myVariable`.\\nInput parameter: $Test\\"
        ],
        "runAsElevated":false
      }
    }
  }
}
```

Risoluzione dei problemi relativi a Session Manager

Utilizza le informazioni seguenti per risolvere i problemi relativi a AWS Systems Manager Session Manager.

Argomenti

- [AccessDeniedException quando si chiama l' TerminateSession operazione](#)
- [Il processo documentale è fallito improvvisamente: l'operatore documentale è scaduto](#)
- [Session Manager non si connette dalla console Amazon EC2](#)
- [Nessuna autorizzazione ad avviare una sessione](#)
- [SSM Agent non online](#)
- [Nessuna autorizzazione a modificare le preferenze delle sessioni](#)
- [Nodo gestito non disponibile o non configurato per Session Manager](#)
- [Plug-in Session Manager non trovato](#)
- [Il plug-in di Session Manager non viene aggiunto automaticamente al percorso della riga di comando \(Windows\)](#)
- [Il plug-in Session Manager non risponde](#)
- [TargetNotConnected](#)
- [Dopo l'avvio di una sessione viene visualizzata una schermata vuota](#)
- [Il nodo gestito non risponde durante le sessioni di esecuzione prolungata](#)
- [Si è verificato un errore \(InvalidDocument\) durante la chiamata dell'operazione StartSession](#)

AccessDeniedException quando si chiama l' TerminateSession operazione

Problema: quando si tenta di terminare una sessione, Systems Manager restituisce il seguente errore:

```
An error occurred (AccessDeniedException) when calling the TerminateSession operation:
User: <user_arn> is not authorized to perform: ssm:TerminateSession on resource:
<ssm_session_arn> because no identity-based policy allows the ssm:TerminateSession
action.
```

Soluzione A: verifica che la [versione più recente del Session Manager plugin](#) sia installata sul nodo

Immetti il seguente comando nel terminale e premi Invio.

```
session-manager-plugin --version
```

Soluzione B: installa o reinstalla l'ultima versione del plug-in

Per ulteriori informazioni, consulta [Installa il Session Manager plugin per AWS CLI](#).

Soluzione C: tentativo di ristabilire una connessione al nodo

Verifica che il nodo risponda alle richieste. Prova a ristabilire la sessione. Oppure, se necessario, apri la console Amazon EC2 e verifica lo stato dell'istanza è in esecuzione.

Il processo documentale è fallito improvvisamente: l'operatore documentale è scaduto

Problema: quando si avvia una sessione su un host Linux, Systems Manager restituisce il seguente errore:

```
document process failed unexpectedly: document worker timed out,
check [ssm-document-worker]/[ssm-session-worker] log for crash reason
```

Se è stata configurata la registrazione dell'SSM Agent, come descritto in [Visualizzazione Agente SSM log](#), è possibile visualizzare maggiori dettagli nel log di debug. Per questo problema, Session Manager mostra la seguente voce di log:

```
failed to create channel: too many open files
```

Questo errore indica in genere che ci sono troppi processi di lavoro Session Manager in esecuzione e che il sistema operativo sottostante ha raggiunto un limite. Sono disponibili due opzioni per la risoluzione di questo problema.

Soluzione A: aumenta il limite di notifica dei file del sistema operativo

È possibile aumentare il limite eseguendo il comando seguente da un host Linux separato. Questo comando utilizza Systems Manager Run Command. Il valore specificato fa aumentare `max_user_instances` fino a 8192. Questo valore è notevolmente superiore al valore predefinito di 128, ma non affaticherà le risorse dell'host:

```
aws ssm send-command --document-name AWS-RunShellScript \  
--instance-id i-02573cafcfEXAMPLE --parameters \  
"commands=sudo sysctl fs.inotify.max_user_instances=8192"
```

Soluzione B: diminuire le notifiche relative ai file utilizzate da Session Manager nell'host di destinazione

Esegui il comando seguente da un host Linux separato per elencare le sessioni in esecuzione sull'host di destinazione:

```
aws ssm describe-sessions --state Active --filters key=Target,value=i-02573cafcfEXAMPLE
```

Esamina l'output del comando per identificare le sessioni che non sono più necessarie. È possibile terminare tali sessioni eseguendo il comando seguente da un host Linux separato:

```
aws ssm terminate-session --session-id session ID
```

Facoltativamente, quando non ci sono più sessioni in esecuzione sul server remoto, è possibile liberare risorse aggiuntive eseguendo il comando seguente da un host Linux separato. Questo comando termina tutti i processi di Session Manager in esecuzione sull'host remoto e, di conseguenza, tutte le sessioni sull'host remoto. Prima di eseguire questo comando, verifica che non ci siano sessioni in corso che desideri mantenere:

```
aws ssm send-command --document-name AWS-RunShellScript \  
--instance-id i-02573cafcfEXAMPLE --parameters \  
'{"commands":["sudo kill $(ps aux | grep ssm-session-worker | grep -v grep | awk  
"'"'"'{print $2}'"'"'"')"]}]'
```

Session Manager non si connette dalla console Amazon EC2

Problema: dopo aver creato una nuova istanza, il pulsante Connettiti > Session Manager nella console Amazon Elastic Compute Cloud (Amazon EC2) non ti offre la possibilità di connetterti.

Soluzione A: crea un profilo di istanza: se non l'hai già fatto (come indicato nelle informazioni nella scheda Session Manager nella console EC2), crea un profilo di istanza AWS Identity and Access Management (IAM) utilizzando Quick Setup. Quick Setup è uno strumento in AWS Systems Manager

Session Manager richiede un profilo dell'istanza IAM per connettersi all'istanza. È possibile creare un profilo dell'istanza e assegnarlo all'istanza creando una [configurazione di gestione dell'host](#) con Quick Setup. Una configurazione di gestione dell'host crea un profilo dell'istanza con le autorizzazioni richieste e lo assegna all'istanza. Una configurazione di gestione dell'host abilita anche altri strumenti di Systems Manager e crea ruoli IAM per l'esecuzione di tali strumenti. L'utilizzo di Quick Setup o degli strumenti abilitati dalla configurazione di gestione dell'host è gratuito. [Apri Quick Setup e crea una configurazione di gestione dell'host](#).

 Important

Dopo aver creato la configurazione di gestione dell'host, Amazon EC2 può impiegare alcuni minuti per registrare la modifica e aggiornare la scheda Session Manager. Se la scheda non mostra il pulsante Connetti dopo due o tre minuti, riavvia l'istanza. Dopo il riavvio, se ancora non vedi l'opzione per la connessione, apri [Configurazione rapida](#) e verifica che esista una sola configurazione di gestione dell'host. Se ne esistono due, elimina la configurazione precedente e attendi qualche minuto.

Se non riesci ancora a connetterti dopo aver creato una configurazione di gestione dell'host o se ricevi un errore, incluso un errore relativo a SSM Agent, consulta una delle seguenti soluzioni:

- [Soluzione B: nessun errore, ma non riesci ancora a connetterti](#)
- [Soluzione C: errore relativo alla mancanza di SSM Agent](#)

Soluzione B: nessun errore, ma non riesci ancora a connetterti

Se hai creato la configurazione di gestione dell'host, hai aspettato diversi minuti prima di provare a connetterti e non riesci ancora a connetterti, potrebbe essere necessario applicare manualmente la

configurazione di gestione dell'host all'istanza. Utilizza la procedura seguente per aggiornare una configurazione di gestione dell'host di Quick Setup e applicare le modifiche a un'istanza.

Per aggiornare una configurazione di gestione dell'host utilizzando Quick Setup

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Quick Setup.
3. Nell'elenco Configurazioni, scegli la configurazione Gestione host che hai creato.
4. Scegli Operazioni, quindi Modifica configurazione.
5. Nella parte inferiore della sezione Destinazioni, in Scegli come destinare le istanze, scegli Manuale.
6. Nella sezione Istanze, scegli l'istanza che hai creato.
7. Scegli Aggiorna.

Attendi qualche minuto che EC2 aggiorni la scheda Session Manager. Se ancora non riesci a connetterti o se ricevi un errore, esamina le soluzioni rimanenti per questo problema.

Soluzione C: errore relativo alla mancanza di SSM Agent

Se non sei riuscito a creare una configurazione di gestione dell'host utilizzando Quick Setup o se hai ricevuto un errore relativo alla mancata installazione di SSM Agent, potresti dover installare SSM Agent manualmente sull'istanza. SSM Agent è un software Amazon che consente a Systems Manager di connettersi all'istanza utilizzando Session Manager. SSM Agent è installato per impostazione predefinita sulla maggior parte delle Amazon Machine Image (AMI). Se l'istanza è stata creata da un'AMI non standard o da un'AMI precedente, potrebbe essere necessario installare manualmente l'agente. Per la procedura di installazione di SSM Agent, consulta il seguente argomento che corrisponde al sistema operativo dell'istanza.

- [Windows Server](#)
- [macOS](#)
- [AlmaLinux](#)
- [Amazon Linux 2 e AL2023](#)
- [Debian Server](#)
- [Oracle Linux](#)

- [Red Hat Enterprise Linux](#)
- [Rocky Linux](#)
- [Ubuntu Server](#)

Per problemi con SSM Agent, vedi [Risoluzione dei problemi Agente SSM](#).

Nessuna autorizzazione ad avviare una sessione

Problema: tenti di avviare una sessione, ma il sistema indica che non disponi delle autorizzazioni necessarie.

- Soluzione: un amministratore di sistema non ti ha concesso le autorizzazioni relative alle policy AWS Identity and Access Management (IAM) per l'avvio delle Session Manager sessioni. Per informazioni, consulta [Controllo dell'accesso della sessione utente alle istanze](#).

SSM Agent non online

Problema: compare un messaggio nella scheda dell'istanza Amazon EC2 Session Manager che indica: "SSM Agent non è online. L'SSM Agent non è riuscito a connettersi a un endpoint di Systems Manager per registrarsi con il servizio."

Soluzione: SSM Agent è il software Amazon che viene eseguito su istanze Amazon EC2 in modo da consentire a Session Manager di connettersi. Se viene visualizzato questo errore, significa che l'SSM Agent non è in grado di stabilire una connessione con l'endpoint di Systems Manager. È possibile che l'origine del problema sia costituita da restrizioni del firewall, problemi di routing o mancanza di connessione Internet. Per risolvere il problema, esaminare i problemi di connettività di rete. Per ulteriori informazioni, consultare [Risoluzione dei problemi Agente SSM](#) e [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#). Per informazioni sugli endpoint di Systems Manager, consulta [Endpoint e quote di AWS Systems Manager](#) nel Documento di riferimento generale ad AWS .

Nessuna autorizzazione a modificare le preferenze delle sessioni

Problema: tenti di aggiornare le preferenze globali delle sessioni della tua organizzazione, ma il sistema indica che non disponi delle autorizzazioni necessarie.

- Soluzione: un amministratore di sistema non ti ha concesso le autorizzazioni di policy IAM per l'impostazione delle preferenze del Session Manager. Per informazioni, consulta [Concedere o negare a un utente le autorizzazioni per aggiornare le preferenze del Session Manager](#).

Nodo gestito non disponibile o non configurato per Session Manager

Problema 1: desideri avviare una sessione dalla pagina della console Start a session (Avvia una sessione), ma non sono presenti nodi gestiti nell'elenco.

- Soluzione A: il nodo gestito a cui desideri connetterti potrebbe non essere stato configurato AWS Systems Manager. Per ulteriori informazioni, consulta [Configurazione della console unificata di Systems Manager per un'organizzazione](#).

Note

Se AWS Systems Manager SSM Agent è già in esecuzione su un nodo gestito quando colleghi il profilo dell'istanza IAM, potrebbe essere necessario riavviare l'agente prima che l'istanza venga elencata nella pagina Avvia una console di sessione.

- Soluzione B: la configurazione proxy applicata al SSM Agent sul tuo nodo gestito potrebbe essere corretta. Se la configurazione del proxy non è corretta, il nodo gestito non sarà in grado di raggiungere gli endpoint del servizio necessari oppure il nodo potrebbe fare riferimento a un sistema operativo diverso a Systems Manager. Per ulteriori informazioni, consultare [Configurazione Agente SSM usare un proxy su nodi Linux](#) e [Configurazione di SSM Agent per utilizzare un proxy per le istanze Windows Server](#).

Problema 2: un nodo gestito che desideri connettere si trova nell'elenco nella pagina della console Avvia una sessione, ma la pagina segnala che "L'istanza selezionata non è configurata per l'uso di Session Manager."

- Soluzione A: il nodo gestito è stato configurato per l'uso con il servizio di Systems Manager, ma il profilo dell'istanza IAM collegato al nodo potrebbe non includere le autorizzazioni per lo strumento di Session Manager. Per informazioni, consulta la sezione [Verifica o creazione di un profilo dell'istanza IAM con autorizzazioni Session Manager](#).
- Soluzione B: il nodo gestito non esegue una versione dell'SSM Agent che supporta il Session Manager. Aggiorna l'SSM Agent sul nodo alla versione 2.3.68.0 o successiva.

Aggiorna l'SSM Agent manualmente su un nodo gestito seguendo la procedura descritta nei passi [Installazione e disinstallazione manuali Agente SSM su istanze EC2 per Windows Server](#), [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#) o [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per macOS](#), a seconda del sistema operativo in uso.

In alternativa, utilizza il documento [Run Command AWS-UpdateSSMAgent](#) per aggiornare la versione dell'agente su uno o più nodi gestiti alla volta. Per informazioni, consulta [Aggiornamento di SSM Agent utilizzando Run Command](#).

 Tip

Per mantenere sempre aggiornato l'agente, consigliamo di aggiornare SSM Agent alla versione più recente in base a una pianificazione automatizzata che potrai definire attraverso uno dei metodi seguenti:

- Esegui `AWS-UpdateSSMAgent` nell'ambito di un'associazione State Manager. Per informazioni, consulta [Procedura dettagliata: aggiorna SSM Agent automaticamente con AWS CLI](#).
- Esegui `AWS-UpdateSSMAgent` all'interno di una finestra di manutenzione. Per ulteriori informazioni sull'uso delle finestre di manutenzione, consulta [Crea e gestisci finestre di manutenzione utilizzando la console](#) e [Tutorial: Creare e configurare una finestra di manutenzione utilizzando il AWS CLI](#).

- Soluzione C: il nodo gestito non può raggiungere gli endpoint del servizio necessari. È possibile migliorare il livello di sicurezza dei nodi gestiti utilizzando gli endpoint di interfaccia forniti da AWS PrivateLink per connettersi agli endpoint Systems Manager. L'alternativa all'utilizzo di un endpoint di interfaccia è l'abilitazione dell'accesso a Internet in uscita sui nodi gestiti. Per ulteriori informazioni, consulta [Utilizzare PrivateLink per configurare un endpoint VPC](#) per Session Manager.
- Soluzione D: il nodo gestito dispone di risorse di memoria o CPU limitate. Sebbene il nodo gestito possa essere funzionale, se non dispone di risorse sufficienti, non è possibile stabilire una sessione. Per ulteriori informazioni, consulta [Risoluzione di problemi relativi a un'istanza irraggiungibile](#).

Plug-in Session Manager non trovato

Per utilizzare i comandi AWS CLI per eseguire la sessione, il Session Manager plug-in deve essere installato anche sul computer locale. Per informazioni, consulta [Installa il Session Manager plugin per AWS CLI](#).

Il plug-in di Session Manager non viene aggiunto automaticamente al percorso della riga di comando (Windows)

Quando installi il plug-in di Session Manager su Windows, l'eseguibile `session-manager-plugin` dovrebbe essere aggiunto automaticamente alla variabile di ambiente PATH del sistema operativo. Se il comando ha esito negativo quando lo esegui per verificare se il plug-in Session Manager è stato installato correttamente (`aws ssm start-session --target instance-id`), potrebbe essere necessario impostarlo manualmente utilizzando la seguente procedura.

Modifica della variabile PATH (Windows)

1. Premi il tasto Windows e immetti **environment variables**.
2. Scegli Modifica variabili di ambiente per l'account.
3. Scegli PATH e quindi Modifica.
4. Aggiungi percorsi al campo Valore variabile, separati da punti e virgola, come illustrato in questo esempio: `C:\existing\path;C:\new\path`

`C:\existing\path` rappresenta il valore già presente nel campo. `C:\new\path` rappresenta il percorso da aggiungere, come illustrato nell'esempio seguente.

- Computer a 64 bit: `C:\Program Files\Amazon\SessionManagerPlugin\bin\`

5. Fai doppio clic su OK per applicare le nuove impostazioni.
6. Chiudi gli eventuali prompt di comando in esecuzione e riapri.

Il plug-in Session Manager non risponde

Durante una sessione di inoltro della porta, il traffico potrebbe interrompere l'inoltro se nel computer locale è installato un software antivirus. In alcuni casi, il software antivirus interferisce con il plug-in Session Manager che causa deadlock del processo. Per risolvere il problema, consentire o escludere il plug-in Session Manager dal software antivirus. Per informazioni sul percorso di installazione predefinito del plug-in Session Manager, consulta [Installa il Session Manager plugin per AWS CLI](#).

TargetNotConnected

Problema: si tenta di avviare una sessione, ma il sistema restituisce il messaggio di errore «Si è verificato un errore (TargetNotConnected) durante la chiamata all' StartSession operazione: *InstanceID* non è connesso».

- Soluzione A: questo errore viene restituito quando il nodo gestito di destinazione specificato per la sessione non è completamente configurato per l'utilizzo con Session Manager. Per informazioni, consulta [Configurazione di Session Manager](#).
- Soluzione B: questo errore viene restituito anche se si tenta di avviare una sessione su un nodo gestito che si trova in un altro Account AWS o Regione AWS.

Dopo l'avvio di una sessione viene visualizzata una schermata vuota

Problema: avvia una sessione e Session Manager visualizza una schermata vuota.

- Soluzione A: questo problema può verificarsi quando il volume principale del nodo gestito è pieno. A causa della mancanza di spazio su disco, SSM Agent sul nodo gestito smette di funzionare. Per risolvere questo problema, usa Amazon CloudWatch per raccogliere metriche e log dai sistemi operativi. Per informazioni, consulta [Raccogli metriche, log e tracce con l' CloudWatch agente](#) nella Amazon CloudWatch User Guide.
- Soluzione B: se è stato effettuato l'accesso alla console utilizzando un collegamento che include una coppia endpoint e regione non corrispondente, potrebbe essere visualizzata una schermata vuota. Ad esempio, nel seguente URL della console, us-west-2 è l'endpoint specificato, ma us-west-1 è la Regione AWS specificata:

```
https://us-west-2.console.aws.amazon.com/systems-manager/session-manager/sessions?region=us-west-1
```

- Soluzione C: il nodo gestito si connette a Systems Manager tramite endpoint VPC e Session Manager le tue preferenze scrivono l'output della sessione su un bucket Amazon S3 o un gruppo di log CloudWatch Amazon Logs, ma nel VPC non esiste un endpoint gateway logs o s3 un endpoint di interfaccia. Un endpoint s3 nel formato **com.amazonaws.region.s3** è necessario se i nodi gestiti si connettono a Systems Manager utilizzando gli endpoint VPC e le preferenze Session Manager scrivono l'output di sessione in un bucket Amazon S3. In alternativa, **com.amazonaws.region.logs** è necessario un logs endpoint in questo formato se i nodi gestiti si connettono a Systems Manager utilizzando endpoint VPC e le Session Manager preferenze scrivono l'output della sessione in CloudWatch un gruppo di log Logs. Per ulteriori informazioni, consulta [Creazione degli endpoint VPC per Systems Manager](#).
- Soluzione D: il gruppo di log o il bucket Amazon S3 specificato nelle preferenze di sessione è stato eliminato. Per risolvere questo problema, aggiornare le preferenze di sessione con un gruppo di log valido o un bucket S3.

- Soluzione E: il gruppo di log o il bucket Amazon S3 specificato nelle preferenze di sessione non è crittografato, ma hai impostato la proprietà `cloudWatchEncryptionEnabled` o input `s3EncryptionEnabled` a `true`. Per risolvere questo problema, aggiorna le preferenze di sessione con un gruppo di log o un bucket Amazon S3 crittografato oppure imposta la proprietà `cloudWatchEncryptionEnabled` o input `s3EncryptionEnabled` a `false`. Questo scenario è applicabile solo ai clienti che creano preferenze di sessione utilizzando gli strumenti a riga di comando.

Il nodo gestito non risponde durante le sessioni di esecuzione prolungata

Problema: il nodo gestito non risponde o si arresta in modo anomalo durante una sessione di esecuzione prolungata.

Soluzione: riduci la durata di conservazione dei log SSM Agent di Session Manager.

Riduzione della durata di conservazione dei log SSM Agent delle sessioni

1. Individua il plug-in `amazon-ssm-agent.json.template` nella directory `/etc/amazon/ssm/` per Linux o `C:\Program Files\Amazon\SSM` per Windows.
2. Copia il contenuto di `amazon-ssm-agent.json.template` in un nuovo file nella stessa directory denominata `amazon-ssm-agent.json`.
3. Ridurre il valore di default del valore `SessionLogsRetentionDurationHours` nella proprietà SSM e salva il file.
4. Riavvia l'SSM Agent.

Si è verificato un errore (`InvalidDocument`) durante la chiamata dell'operazione `StartSession`

Problema: quando avvii una sessione utilizzando la AWS CLI, visualizzi l'errore seguente.

```
An error occurred (InvalidDocument) when calling the StartSession operation: Document type: 'Command' is not supported. Only type: 'Session' is supported for Session Manager.
```

Soluzione: il documento SSM specificato per il parametro `--document-name` non è un documento di Sessione. Utilizza la procedura seguente per visualizzare un elenco di documenti di sessione nella Console di gestione AWS.

Visualizzazione di un elenco di documenti di sessione

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel riquadro di navigazione, scegli Documenti.
3. Nell'elenco Categorie, scegli Documenti di sessione.

AWS Systems Manager State Manager

State Manager è un servizio di gestione della configurazione sicuro e scalabile che automatizza il processo di mantenimento dei nodi gestiti e AWS delle altre risorse in uno stato definito dall'utente. Per cominciare a utilizzare State Manager, apri la [console di Systems Manager](#). Nel pannello di navigazione, scegli State Manager.

Note

State Manager e Maintenance Windows sono in grado di eseguire alcuni tipi di aggiornamenti simili sui nodi gestiti. La scelta dipende dalla necessità di automatizzare la conformità del sistema o di eseguire attività ad alta priorità e sensibili al tempo durante i periodi specificati. Per ulteriori informazioni, consulta [Scelta tra State Manager and Intervallo di manutenzione](#).

Come può State Manager avvantaggiare la mia organizzazione?

Utilizzando documenti Systems Manager preconfigurati (documenti SSM), State Manager offre i seguenti vantaggi per la gestione dei nodi:

- Bootstrap di nodi con software specifico all'avvio
- Download e aggiornamento di agenti in base a una pianificazione definita, tra cui SSM Agent
- Configurazione delle impostazioni di rete.
- Consente di aggiungere nodi a un dominio Microsoft Active Directory.
- Esecuzione di script sui nodi gestiti di Linux, macOS e Windows Server per tutto il loro ciclo di vita.

Per gestire la variazione della configurazione tra altre AWS risorse, è possibile utilizzare Automation, uno strumento di Systems Manager, che consente di State Manager eseguire i seguenti tipi di attività:

- Assegna un ruolo Systems Manager alle istanze di Amazon Elastic Compute Cloud (Amazon EC2) per renderle nodi gestiti.
- applica le regole di ingresso e di uscita desiderate per un gruppo di sicurezza;
- crea o elimina i backup di Amazon DynamoDB;
- crea o elimina gli snapshot di Amazon Elastic Block Store (Amazon EBS);
- Disattiva le autorizzazioni di lettura e scrittura per i bucket Amazon Simple Storage Service (Amazon S3);
- Avvia, riavvia o arresta i nodi gestiti e le istanze di Amazon Relational Database Service (Amazon RDS);
- applicare patch a Linux, macOS e alla finestra AMIs;

Per informazioni sull'uso di State Manager con i runbook di automazione, consulta [Pianificazione delle automazioni con State Manager associazioni](#).

Chi dovrebbe usare State Manager?

State Manager è adatto a qualsiasi AWS cliente che desideri migliorare la gestione e la governance delle proprie AWS risorse e ridurre la deriva dalla configurazione.

Quali sono le caratteristiche di State Manager?

Le funzionalità principali di State Manager comprendono:

- State Manager associazioni

Un'associazione State Manager è una configurazione che assegna alle tue AWS risorse.

La configurazione definisce lo stato che desideri mantenere sulle risorse. Ad esempio, un'associazione può specificare che il software antivirus debba essere installato ed eseguito su un nodo gestito o che determinate porte debbano essere chiuse.

Un'associazione specifica una pianificazione per quando applicare la configurazione e le destinazioni per l'associazione. Ad esempio, un'associazione per il software antivirus potrebbe essere eseguita una volta al giorno su tutti i nodi gestiti in un account AWS. Se il software non è installato su un nodo, l'associazione potrebbe istruire State Manager per installarlo. Se il software è installato, ma il servizio non è in esecuzione, l'associazione potrebbe indicare a State Manager di avviare il servizio.

- Opzioni di pianificazione flessibili

State Manager offre le seguenti opzioni per la pianificazione quando viene eseguita un'associazione:

- Elaborazione immediata o posticipata

Quando si crea un'associazione, per impostazione predefinita, il sistema la esegue immediatamente sulle istanze o destinazioni specificate. Dopo l'esecuzione iniziale, l'associazione viene eseguita a intervalli in base alla pianificazione definita.

È possibile istruire State Manager a non eseguire immediatamente un'associazione utilizzando l'associazione Applica associazione solo all'opzione intervallo Cron specificata successiva nella console o nel parametro `ApplyOnlyAtCronInterval` dalla riga di comando.

- Espressioni Cron e della frequenza

Quando si crea un'associazione, si specifica una pianificazione per l'State Manager applicazione della configurazione. State Manager supporta la maggior parte delle espressioni cron e rate standard per la pianificazione. Supporta anche espressioni cron che includono un giorno della settimana e il segno numerico (#) per designarli il n° giorno del mese. Usa il segno (L) per indicare l'ultimo giorno X del mese.

 Note

State Manager attualmente non supporta la specifica di mesi nelle espressioni cron per le associazioni.

Per controllare ulteriormente l'esecuzione di un'associazione, ad esempio se si desidera eseguire un'associazione due giorni dopo la patch di martedì, è possibile specificare un offset. Un record offset definisce quanti giorni attendere dopo il giorno programmato per eseguire un'associazione.

Per ulteriori informazioni sulla creazione di espressioni Cron/della frequenza, consulta [Riferimento: espressioni Cron e della frequenza per Systems Manager](#).

- Diverse opzioni di targeting

Un'associazione specifica anche gli obiettivi dell'associazione. State Manager supporta il targeting AWS delle risorse utilizzando tag AWS Resource Groups, ID dei singoli nodi o tutti i nodi gestiti nell'attuale Regione AWS e. Account AWS

- Supporto Amazon S3

Archivia l'output dei comandi dall'associazione in esecuzione in un bucket Amazon S3 di tua scelta. Per ulteriori informazioni, consulta [Utilizzo delle associazioni in Systems Manager](#).

- EventBridge supporto

Questo strumento Systems Manager è supportato sia come tipo di evento che come tipo di destinazione nelle EventBridge regole di Amazon. Per informazioni, consulta [Monitoraggio degli eventi di Systems Manager con Amazon EventBridge](#) e [Riferimento: modelli e tipi di EventBridge eventi Amazon per Systems Manager](#).

L'utilizzo è a pagamento State Manager?

State Manager è disponibile senza costi aggiuntivi.

Argomenti

- [Capire come State Manager funzionamento](#)
- [Utilizzo delle associazioni in Systems Manager](#)
- [Creazione di associazioni che eseguono file MOF](#)
- [Creazione di associazioni che funzionano Ansible playbook](#)
- [Creazione di associazioni che vengono eseguite Chef recipes](#)
- [Procedura dettagliata: aggiorna SSM Agent automaticamente con AWS CLI](#)
- [Spiegazione passo per passo: aggiornare automaticamente i driver PV sulle istanze EC2 per Windows Server](#)

Ulteriori informazioni

- [Combattere la deriva della configurazione utilizzando Amazon EC2 Systems Manager e Windows DSC PowerShell](#)
- [Configurare istanze Amazon EC2 in un gruppo Auto Scaling tramite State Manager](#)

Capire come State Manager funzionamento

State Manager è un servizio sicuro e scalabile che automatizza il processo di mantenimento dei nodi gestiti in un'[infrastruttura](#) ibrida e multicloud in uno stato definito dall'utente.

Ecco come funziona State Manager:

1. Determina lo stato da applicare alle tue risorse. AWS

Vuoi assicurarti che i nodi gestiti siano configurato con applicazioni specifiche, ad esempio applicazioni antivirus o malware? Vuoi automatizzare il processo di aggiornamento dell'SSM Agent o di altri pacchetti AWS , come ad esempio AWSPVDriver? Vuoi accertarti che determinate porte siano aperte o chiuse? Per iniziare State Manager, stabilisci lo stato che desideri applicare alle tue AWS risorse. Lo stato che desideri applicare determinerà quale documento SSM utilizzerai per creare un'associazione di State Manager.

Un'associazione di State Manager è una configurazione che assegna alle tue AWS risorse. La configurazione definisce lo stato che desideri mantenere sulle risorse. Ad esempio, un'associazione può specificare che il software antivirus debba essere installato ed eseguito su un nodo gestito o che determinate porte debbano essere chiuse.

Un'associazione specifica una pianificazione per quando applicare la configurazione e le destinazioni per l'associazione. Ad esempio, un'associazione per il software antivirus potrebbe essere eseguita una volta al giorno su tutti i nodi gestiti in un account AWS. Se il software non è installato su un nodo, l'associazione potrebbe istruire State Manager per installarlo. Se il software è installato, ma il servizio non è in esecuzione, l'associazione potrebbe indicare a State Manager di avviare il servizio.

2. Determina se un documento SSM preconfigurato può aiutarti a creare lo stato desiderato sulle tue AWS risorse.

Systems Manager include decine di documenti SSM preconfigurati che è possibile utilizzare per creare un'associazione. I documenti preconfigurati sono pronti per eseguire attività comuni come l'installazione di applicazioni, la configurazione di Amazon, l'esecuzione di AWS Systems Manager automazioni CloudWatch, l'esecuzione di script Shell PowerShell e l'unione di nodi gestiti a un dominio di servizi di directory per Active Directory.

È possibile visualizzare tutti i documenti SSM nella [console di Systems Manager](#). Scegliere il nome di un documento per scoprire ulteriori informazioni su ciascuno di essi. Di seguito, sono riportati due esempi: [AWS-ConfigureAWSPackage](#) e [AWS-InstallApplication](#).

3. Creazione di un'associazione

È possibile creare un'associazione utilizzando la console di Systems Manager, AWS Command Line Interface (AWS CLI), AWS Tools for Windows PowerShell (Tools for Windows PowerShell) o l'API Systems Manager. Quando viene creata l'associazione, si specifica quanto segue:

- Un nome per l'associazione.

- I parametri per il documento SSM (ad esempio, il percorso dell'applicazione da installare o lo script da eseguire sui nodi).
- I target per l'associazione. È possibile definire come target i nodi gestiti specificando i tag , scegliendo gli ID di nodi individuali o scegliendo un gruppo in AWS Resource Groups. È inoltre possibile scegliere come target tutti i nodi gestiti nell'attuale Regione AWS e Account AWS. Se le tue destinazioni includono più di 1.000 nodi, il sistema utilizza un meccanismo di limitazione (della larghezza di banda della rete). Ciò significa che potresti riscontrare imprecisioni nel conteggio dell'aggregazione dello stato, poiché il processo di aggregazione viene eseguito ogni ora e solo quando lo stato di esecuzione di un nodo cambia.
- Un ruolo utilizzato dall'associazione per intraprendere azioni per tuo conto. State Manager assumerà questo ruolo e chiamerà le API richieste durante l'invio delle configurazioni ai nodi. Per informazioni sull'impostazione del ruolo fornito in modo personalizzato, vedere. [Imposta i ruoli per AssociationDispatchAssumeRole](#) Se non viene fornito alcun ruolo, verrà utilizzato il ruolo [collegato al servizio per Systems Manager](#).

 Note

Si consiglia di definire un ruolo IAM personalizzato in modo da avere il pieno controllo delle autorizzazioni di cui dispone State Manager quando intraprende azioni per conto dell'utente.

Service-linked il supporto ai ruoli in State Manager è in fase di graduale eliminazione. Le associazioni che si affidano al ruolo legato ai servizi potrebbero richiedere aggiornamenti in futuro per continuare a funzionare correttamente.

Per informazioni sulla gestione dell'utilizzo del ruolo fornito in modo personalizzato, vedere. [Gestisci l'utilizzo di AssociationDispatchAssumeRole con ssm: AssociationDispatchAssumeRole](#)

- Una pianificazione per il momento o la frequenza di applicazione dello stato. È possibile specificare un'espressione Cron o della frequenza. Per ulteriori informazioni sulla creazione di pianificazioni utilizzando espressioni Cron e della frequenza, consulta [Espressioni Cron e della frequenza per le associazioni](#).

 Note

State Manager attualmente non supporta la specifica di mesi nelle espressioni cron per le associazioni.

Quando si esegue il comando per creare l'associazione, Systems Manager associa le informazioni specificate (pianificazione, target, documento SSM e parametri) alle risorse target. Lo stato dell'associazione inizialmente mostra "Pending" (In sospeso) mentre il sistema tenta di raggiungere tutti i target e applica immediatamente lo stato specificato nell'associazione.

 Note

Se si crea una nuova associazione pianificata per essere eseguita mentre un'associazione precedente è ancora in esecuzione, la prima associazione viene messa in timeout e viene eseguita la nuova associazione.

Systems Manager indica lo stato della richiesta di creazione di associazioni sulle risorse. È possibile visualizzare i dettagli sullo stato nella console o (per i nodi gestiti) utilizzando l'operazione [DescribeInstanceAssociationsStatus](#) API. Se si sceglie di scrivere l'output del comando in Amazon Simple Storage Service (Amazon S3) quando si crea un'associazione, è possibile anche visualizzare l'output nel bucket Amazon S3 specificato.

Per ulteriori informazioni, consulta [Utilizzo delle associazioni in Systems Manager](#).

 Note

Le operazioni API avviate dal documento SSM durante un'esecuzione di associazione non vengono registrate in AWS CloudTrail.

4. Monitorare e aggiornare.

Una volta creata l'associazione, State Manager riapplica la configurazione in base alla pianificazione definita nell'associazione. È possibile visualizzare lo stato delle associazioni nella [pagina di State Manager](#) nella console oppure chiamando direttamente l'ID di associazione generato da Systems Manager quando è stata creata l'associazione. Per ulteriori informazioni, consulta [Visualizzazione della cronologia delle associazioni](#). È possibile aggiornare i documenti delle associazioni e riapplicarli come necessario. È possibile inoltre creare più versioni di un'associazione. Per ulteriori informazioni, consulta [Modifica e creazione di una nuova versione di un'associazione](#).

Capire quando le associazioni vengono applicate alle risorse

Quando crei un'associazione, specifichi un documento SSM che definisce la configurazione, un elenco di risorse target e una pianificazione per l'applicazione della configurazione. Per impostazione predefinita, State Manager esegue l'associazione al momento della creazione e quindi in base alla pianificazione specificata. State Manager prova inoltre a eseguire l'associazione nelle seguenti situazioni:

- **Modifica dell'associazione:** State Manager esegue l'associazione dopo che un utente ha modificato e salvato le modifiche in qualsiasi campo di associazione. Qualsiasi chiamata all'azione `UpdateAssociation` API che modifica l'associazione attiva un'esecuzione immediata.
- **Modifica documento:** State Manager esegue l'associazione dopo che un utente ha modificato e salvato le modifiche al documento SSM che definisce lo stato di configurazione dell'associazione. In particolare, l'associazione viene eseguita dopo le seguenti modifiche al documento:
 - Un utente specifica una nuova versione del documento `$DEFAULT` e l'associazione era stata creata utilizzando la versione `$DEFAULT`.
 - Un utente aggiorna un documento e l'associazione era stata creata utilizzando la versione `$LATEST`.
 - Un utente elimina il documento specificato al momento della creazione dell'associazione.
- **Avvio manuale:** State Manager esegue l'associazione quando viene avviata dall'utente dalla console di Systems Manager o a livello di programmazione.
- **Modifiche alla destinazione:** State Manager esegue l'associazione dopo che si è verificata una delle seguenti attività su un nodo di destinazione:
 - Un nodo gestito passa online per la prima volta.
 - Un nodo gestito passa online dopo la mancata esecuzione di un'associazione pianificata.
 - Un nodo gestito passa online dopo essere stato arrestato per più di 30 giorni.

Note

State Manager non monitora i documenti o i pacchetti utilizzati nelle associazioni all'interno degli Account AWS. Se aggiorni un documento o un pacchetto in un account, l'aggiornamento non causerà l'esecuzione dell'associazione nel secondo account. È necessario eseguire manualmente l'associazione nel secondo account.

Impedire l'esecuzione delle associazioni quando una destinazione cambia

In alcuni casi, potresti non voler eseguire un'associazione quando una destinazione composta da nodi gestiti cambia, ma solo in base alla pianificazione specificata.

Note

L'esecuzione di un runbook di automazione comporta un costo. Se un'associazione a un runbook di automazione è diretta a tutte le istanze del tuo account e avvii regolarmente un gran numero di istanze, il runbook viene eseguito su ciascuna istanza al momento dell'avvio. Ciò può comportare costi di automazione elevati.

Per evitare che un'associazione venga eseguita quando le destinazioni di quell'associazione cambiano, seleziona la casella di controllo **Applica l'associazione solo al successivo intervallo cron specificato**. Questa casella di controllo si trova nell'area **Specifica pianificazione delle pagine Crea associazione e Modifica associazione**.

Questa opzione si applica alle associazioni che incorporano sia un runbook di automazione che un documento SSM.

Informazioni sugli aggiornamenti di destinazione con i runbook Automation

Affinché le associazioni create con i runbook di Automation vengano applicate quando vengono rilevati nuovi nodi di destinazione, devono sussistere le seguenti condizioni:

- È necessario che l'associazione sia creata da una configurazione [Quick Setup](#). Quick Setup è uno strumento di AWS Systems Manager. Le associazioni create da altri processi non sono attualmente supportate.
- È necessario che il runbook Automation indirizzi esplicitamente il tipo di risorsa `AWS::EC2::Instance` o `AWS::SSM::ManagedInstance`.
- È necessario che l'associazione specifichi parametri e destinazioni.

Nella console, i campi **Parametro** e **Destinazioni** vengono visualizzati quando si sceglie un'esecuzione per il controllo della velocità.

Execution

☐ Simple execution
Execute on targets.

☒ Rate control
Execute safely on multiple targets by defining concurrency and error thresholds.

Targets

Select the targets on which the automation document will run.

Parameter

Choose the parameter that will define how your automation will branch out.

Select a parameter ▼

Targets

Select a target ▼

Quando si utilizzano le azioni di API [CreateAssociation](#), [CreateAssociationBatch](#) o [UpdateAssociation](#), è possibile specificare questi valori utilizzando gli input `AutomationTargetParameterName` e `Targets`. In ognuna di queste azioni di API, puoi anche impedire l'esecuzione dell'associazione ogni volta che una destinazione cambia impostando il parametro `ApplyOnlyAtCronInterval` su `true`.

Per informazioni sull'utilizzo della console per controllare quando vengono eseguite le associazioni, compresi i dettagli per evitare costi inaspettatamente elevati per le esecuzioni di automazione, consulta [Capire quando le associazioni vengono applicate alle risorse](#).

Imposta i ruoli per **AssociationDispatchAssumeRole**

Per configurare l'invio personalizzato, assumi i ruoli che State Manager assume per eseguire azioni per tuo conto, i ruoli devono avere fiducia `ssm.amazonaws.com` e disporre dell'autorizzazione richiesta per chiamare `ssm:SendCommand` o in `ssm:StartAutomationExecution` base ai casi d'uso dell'associazione.

Esempio di politica di fiducia:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "ssm.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Gestisci l'utilizzo di `AssociationDispatchAssumeRole` con **ssm:**

AssociationDispatchAssumeRole

Per gestire l'utilizzo dell'invio personalizzato, assumi i ruoli che State Manager assume per eseguire azioni per tuo conto, usa la `ssm:AssociationDispatchAssumeRole` chiave di condizione.

Questa condizione controlla se le associazioni possono essere create o aggiornate senza specificare un ruolo di assunzione personalizzato per la spedizione.

Nel seguente esempio di policy, l'"Allow"istruzione concede le autorizzazioni per l'associazione, la creazione e l'aggiornamento delle API solo quando viene specificato il parametro.

`AssociationDispatchAssumeRole` Senza questo parametro nelle richieste API, la policy non concede l'autorizzazione per creare o aggiornare le associazioni:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:CreateAssociationBatch"
      ],
    }
  ]
}
```

```
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "ssm:AssociationDispatchAssumeRole": "*"
      }
    }
  }
]
```

Utilizzo delle associazioni in Systems Manager

Questa sezione descrive come creare e gestire State Manager le associazioni utilizzando la AWS Systems Manager console, il AWS Command Line Interface (AWS CLI) e AWS Strumenti per PowerShell.

Argomenti

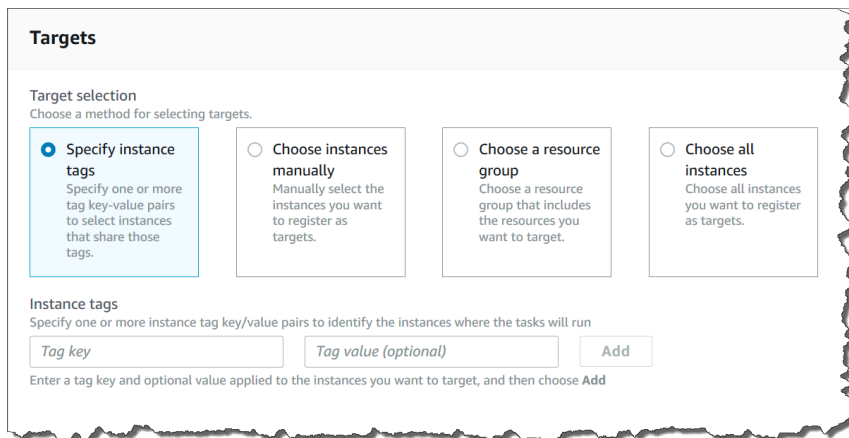
- [Comprendere gli obiettivi e i controlli delle tariffe in State Manager associazioni](#)
- [Creazione di associazioni](#)
- [Modifica e creazione di una nuova versione di un'associazione](#)
- [Eliminazione di associazioni](#)
- [Esecuzione dei gruppi Auto Scaling con associazioni](#)
- [Visualizzazione della cronologia delle associazioni](#)
- [Utilizzo delle associazioni tramite IAM](#)

Comprendere gli obiettivi e i controlli delle tariffe in State Manager associazioni

Questo argomento descrive la funzionalità di State Manager, utile per implementare al meglio un'associazione a decine o centinaia di nodi, controllando al tempo stesso il numero di nodi che eseguono l'associazione nell'ora pianificata. State Manager è uno strumento di AWS Systems Manager.

Utilizzare le destinazioni

Quando si crea un'associazione State Manager, si scelgono i nodi da configurare con l'associazione nella sezione Destinazioni della console di Systems Manager, come illustrato di seguito.



Targets

Target selection
Choose a method for selecting targets.

- ☒ **Specify instance tags**
Specify one or more tag key-value pairs to select instances that share those tags.
- ☐ **Choose instances manually**
Manually select the instances you want to register as targets.
- ☐ **Choose a resource group**
Choose a resource group that includes the resources you want to target.
- ☐ **Choose all instances**
Choose all instances you want to register as targets.

Instance tags
Specify one or more instance tag key/value pairs to identify the instances where the tasks will run

Tag key Tag value (optional)

Enter a tag key and optional value applied to the instances you want to target, and then choose Add

Se crei un'associazione utilizzando uno strumento a riga di comando, ad esempio AWS Command Line Interface (AWS CLI), devi specificare il parametro `targets`. I nodi di destinazione consentono di configurare decine, centinaia o migliaia di nodi con un'associazione senza dover specificare o scegliere gli ID dei singoli nodi.

Ogni nodo gestito può essere scelto come destinazione da un massimo di 20 associazioni.

State Manager include le seguenti opzioni di destinazione in fase di creazione di un'associazione.

Specificare i tag.

Utilizzare questa opzione per specificare una chiave di tag e (facoltativamente) un valore di tag assegnati ai nodi. Quando si esegue la richiesta, il sistema individua e tenta di creare l'associazione su tutti i nodi che corrispondono alla chiave e al valore di tag specificati. Se sono stati specificati più valori di tag, l'associazione si rivolge a qualsiasi nodo con almeno uno di questi valori di tag. Quando il sistema crea inizialmente l'associazione, la esegue. Dopo questa esecuzione iniziale, il sistema esegue l'associazione in base alla pianificazione specificata.

Se si creano nuove nodi e si assegnano la chiave e il valore di tag specificati a tali nodi, il sistema applica automaticamente l'associazione, la esegue immediatamente e quindi la esegue in base alla pianificazione. Ciò vale quando l'associazione utilizza un documento di Comando o Policy e non vale se l'associazione utilizza un runbook di Automazione. Se elimini i tag specificati da un nodo, il sistema non esegue più l'associazione su tali nodi.

Note

Se utilizzi i runbook di Automation con State Manager e la limitazione dei tag ti impedisce di raggiungere un obiettivo specifico, prendi in considerazione l'utilizzo dei runbook di

Automation con Amazon. EventBridge Per ulteriori informazioni, consulta [Esegui automazioni basate sugli eventi EventBridge](#). Per informazioni sull'uso dei runbook con State Manager, consulta [Pianificazione delle automazioni con State Manager associazioni](#).

Come procedura consigliata, si consiglia di utilizzare i tag durante la creazione di associazioni che utilizzano un documento di Comando o Policy. Si consiglia inoltre di utilizzare i tag durante la creazione di associazioni per eseguire gruppi Auto Scaling Per ulteriori informazioni, consulta [Esecuzione dei gruppi Auto Scaling con associazioni](#).

Note

Osserva le seguenti informazioni.

- Quando si crea un'associazione nei nodi Console di gestione AWS destinata ai nodi utilizzando i tag, è possibile specificare solo una chiave tag per un'associazione di automazione e cinque chiavi tag per un'associazione di comando. Tutte le chiavi di tag specificate nell'associazione devono essere attualmente assegnate al nodo. In caso contrario, State Manager non riesce a scegliere il nodo come destinazione per un'associazione.
- Se desideri utilizzare la console e i nodi di destinazione utilizzando più di una chiave tag (automazione) o cinque tag (comando), assegna le chiavi tag a un AWS Resource Groups gruppo. Aggiungi i nodi al gruppo. È possibile quindi scegliere l'opzione Gruppo di risorse nell'elenco Destinazioni quando crei l'associazione State Manager.
- È possibile specificare un massimo di cinque chiavi di tag utilizzando la AWS CLI. Se si utilizza il AWS CLI, tutte le chiavi dei tag specificate nel `create-association` comando devono essere attualmente assegnate al nodo. In caso contrario, State Manager non riesce a scegliere il nodo come destinazione per un'associazione.

Scelta manuale dei nodi

Utilizzare questa opzione per selezionare manualmente i nodi in cui si desidera creare l'associazione. Il riquadro **Istanze** mostra tutti i nodi gestiti da Systems Manager nell'attuale Account AWS e Regione AWS. È possibile selezionare manualmente tutti i nodi desiderati. Quando il sistema crea inizialmente l'associazione, la esegue. Dopo questa esecuzione iniziale, il sistema esegue l'associazione in base alla pianificazione specificata.

 Note

Se un nodo gestito Amazon EC2 che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

Scelta di un gruppo di risorse

Utilizzate questa opzione per creare un'associazione su tutti i nodi restituiti da un'interrogazione AWS Resource Groups basata su tag o AWS CloudFormation stack.

Seguono dettagli sull'individuazione dei gruppi di risorse per un'associazione.

- Se si aggiungono nuovi nodi a un gruppo, il sistema mappa automaticamente i nodi all'associazione che ha come destinazione il gruppo di risorse. Il sistema applica l'associazione ai nodi quando rileva la modifica. Dopo questa esecuzione iniziale, il sistema esegue l'associazione in base alla pianificazione specificata.
- Se crei un'associazione destinata a un gruppo di risorse e il tipo di risorsa `AWS::SSM::ManagedInstance` è stato specificato per tale gruppo, l'associazione viene eseguita sia su istanze Amazon Elastic Compute Cloud (Amazon EC2) che su nodi non EC2 in [ambienti ibridi e multicloud](#).

È vero anche il contrario. Se crei un'associazione destinata a un gruppo di risorse e il tipo di risorsa `AWS::EC2::Instance` è stato specificato per tale gruppo, quindi progettato, l'associazione viene eseguita sia su nodi non EC2 in un ambiente [ibrido e multi-cloud](#) che su istanze (Amazon EC2).

- Se crei un'associazione destinata a un gruppo di risorse, al gruppo di risorse non devono essere assegnate più di cinque chiavi di tag o più di cinque valori specificati per ciascuna chiave di tag. Se una di queste condizioni si applica ai tag e alle chiavi assegnati al gruppo di risorse, l'associazione non viene eseguita e restituisce un errore `InvalidTarget`.
- Quando si crea un'associazione destinata a un gruppo di risorse utilizzando i tag, non è possibile scegliere l'opzione (valore vuoto) per il valore del tag.
- Se elimini un gruppo di risorse, tutte le istanze del gruppo non eseguono più l'associazione. Come best practice, è consigliabile eliminare le associazioni che hanno come destinazione il gruppo.
- Al massimo è possibile assegnare come destinazione un singolo gruppo di risorse per un'associazione. I gruppi multipli o nidificati non sono supportati.

- Dopo aver creato un'associazione, State Manager la aggiorna periodicamente con le informazioni sulle risorse del gruppo di risorse. Se aggiungi nuove risorse a un gruppo di risorse, la pianificazione di quando il sistema applica l'associazione alle nuove risorse dipende da diversi fattori. È possibile determinare lo stato dell'associazione nella pagina di State Manager della console Systems Manager.

 Warning

Un utente, gruppo o ruolo AWS Identity and Access Management (IAM) con l'autorizzazione a creare un'associazione destinata a un gruppo di risorse di istanze Amazon EC2 ha automaticamente il controllo a livello di root di tutte le istanze del gruppo. Solo gli amministratori attendibili dovrebbero essere autorizzati a creare le associazioni.

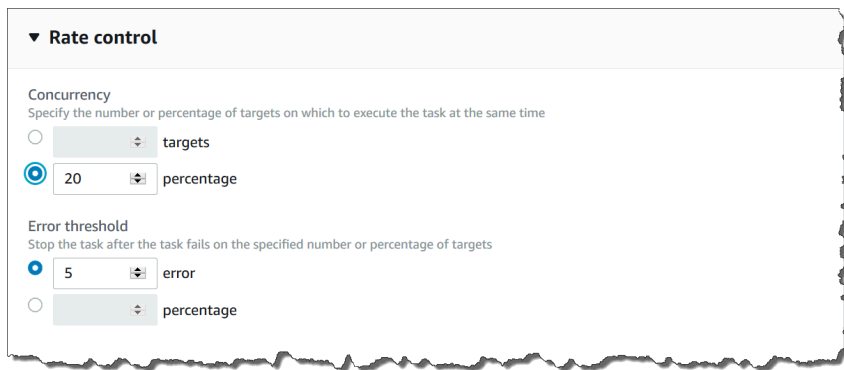
Per ulteriori informazioni sui gruppi di risorse, consulta [Che cos'è AWS Resource Groups?](#) nella Guida per l'utente di AWS Resource Groups .

Scelta di tutti i nodi

Usa questa opzione per indirizzare tutti i nodi nell'attuale e. Account AWS Regione AWS Quando si esegue la richiesta, il sistema individua e tenta di creare l'associazione su tutti i nodi nell' Account AWS and Regione AWS corrente. Quando il sistema crea inizialmente l'associazione, la esegue. Dopo questa esecuzione iniziale, il sistema esegue l'associazione in base alla pianificazione specificata. Se si creano nuovi nodi, il sistema applica automaticamente l'associazione, la esegue immediatamente e quindi la esegue in base alla pianificazione.

Utilizzo dei controlli di velocità

È possibile controllare l'esecuzione di un'associazione sui nodi specificando un valore di simultaneità e una soglia di errore. Il valore di simultaneità specifica il numero di nodi autorizzati a eseguire contemporaneamente l'associazione. Una soglia di errore specifica il numero di esecuzioni dell'associazione che possono avere esito negativo prima che Systems Manager invii un comando a ogni nodo configurato con tale associazione per arrestare l'esecuzione della stessa. Il comando interrompe l'esecuzione dell'associazione fino all'esecuzione pianificata successiva. Le funzionalità di simultaneità e soglia di errore vengono definite collettivamente controlli di velocità.



▼ Rate control

Concurrency
Specify the number or percentage of targets on which to execute the task at the same time

☐ targets

☒ 20 percentage

Error threshold
Stop the task after the task fails on the specified number or percentage of targets

☒ 5 error

☐ percentage

Concurrency (Simultaneità)

La simultaneità aiuta a limitare l'impatto sui nodi, poiché consente di specificare che solo un determinato numero di nodi può elaborare un'associazione contemporaneamente. È possibile specificare un numero assoluto di nodi gestiti, ad esempio 20, oppure una percentuale del set di target, ad esempio 10%.

La simultaneità di State Manager prevede le seguenti restrizioni e limitazioni:

- Se si sceglie di creare un'associazione utilizzando i target, ma non si specifica un valore di simultaneità, State Manager applica automaticamente un valore di simultaneità massimo di 50 nodi.
- Se nuovi nodi che soddisfano i criteri di target vanno online mentre un'associazione che utilizza la simultaneità è in esecuzione, i nuovi nodi eseguono l'associazione se il valore di simultaneità non viene superato. Se il valore di simultaneità viene superato, i nodi vengono ignorati durante l'intervallo corrente di esecuzione dell'associazione. I nodi eseguiranno l'associazione durante il successivo intervallo pianificato se sono conformi ai requisiti di simultaneità.
- Se si aggiorna un'associazione che utilizza la simultaneità e uno o più nodi stanno elaborando tale associazione quando viene aggiornata, qualsiasi nodo che esegue l'associazione può essere completato. Le associazioni non avviate vengono arrestate. Dopo il completamento dell'esecuzione delle associazioni, tutti i nodi target eseguono immediatamente di nuovo l'associazione perché è stata aggiornata. Quando l'associazione viene eseguita di nuovo, il valore di simultaneità viene applicato.

Soglie di errore

Una soglia di errore specifica il numero di esecuzioni dell'associazione che possono avere esito negativo prima che Systems Manager invii un comando a ogni nodo configurato con tale associazione. Il comando interrompe l'esecuzione dell'associazione fino all'esecuzione pianificata

successiva. È possibile specificare un numero assoluto di errori, ad esempio 10, oppure una percentuale della serie di target, ad esempio 10%.

Se specifichi un numero assoluto pari, ad esempio, a tre errori, State Manager invia un comando di arresto alla restituzione del quarto errore. Se specifichi 0, State Manager invia il comando di arresto alla restituzione del primo risultato di errore.

Se specifichi una soglia di errore pari al 10% per 50 associazioni, State Manager invia il comando di arresto alla restituzione del sesto errore. Sarà consentito il completamento delle associazioni già in esecuzione una volta raggiunta la soglia di errore. Tuttavia, è possibile che alcune di tali associazioni abbiano esito negativo. Per assicurarvi che non vi siano più errori del numero specificato per la soglia di errore, impostate il valore `Concurrency` su 1 in modo che le associazioni procedano una alla volta.

Le soglie di errore di State Manager prevedono le seguenti restrizioni e limitazioni:

- Le soglie di errore vengono applicate per l'intervallo corrente.
- Le informazioni su ogni errore, inclusi i dettagli a livello di fase, vengono registrate nella cronologia dell'associazione.
- Se scegli di creare un'associazione utilizzando destinazioni, ma non specifichi una soglia di errore, State Manager applica automaticamente una soglia pari al 100% di errori.

Creazione di associazioni

State Manager consente di mantenere le AWS risorse in uno stato definito e di ridurre la deriva dalla configurazione. Per farlo, State Manager utilizza associazioni. Un'associazione è una configurazione che assegna alle risorse AWS. La configurazione definisce lo stato che desideri mantenere sulle risorse. Ad esempio, un'associazione può specificare che il software antivirus debba essere installato ed eseguito su un nodo gestito o che determinate porte debbano essere chiuse.

Un'associazione specifica una pianificazione per quando applicare la configurazione e le destinazioni per l'associazione. Ad esempio, un'associazione per il software antivirus potrebbe essere eseguita una volta al giorno su tutti i nodi gestiti in un account AWS. Se il software non è installato su un nodo, l'associazione potrebbe istruire State Manager per installarlo. Se il software è installato, ma il servizio non è in esecuzione, l'associazione potrebbe indicare a State Manager di avviare il servizio.

Warning

Quando si crea un'associazione, è possibile scegliere un gruppo di AWS risorse di nodi gestiti come destinazione dell'associazione. Se un utente, gruppo o ruolo AWS Identity and Access

Management (IAM) dispone dell'autorizzazione per creare un'associazione destinata a un gruppo di risorse di nodi gestiti, tale utente, gruppo o ruolo ha automaticamente il controllo a livello di root di tutti i nodi del gruppo. Solo gli amministratori attendibili devono essere autorizzati a creare le associazioni.

Target di associazione e controlli di velocità

Un'associazione specifica quali nodi gestiti, oppure target, devono ricevere l'associazione. State Manager include diverse funzionalità per aiutarti a scegliere come target i nodi gestiti e controllare come l'associazione viene implementata su tali target. Per ulteriori informazioni sulle destinazioni e sui controlli di velocità, consulta [Comprendere gli obiettivi e i controlli delle tariffe in State Manager associazioni](#).

Associazione dei tag

È possibile assegnare tag a un'associazione quando la si crea utilizzando uno strumento da riga di comando come `awscli` o `PowerShell`. Aggiunta di tag a un'associazione utilizzando la console Systems Manager non è supportata.

Esecuzione delle associazioni

Per impostazione predefinita, State Manager esegue un'associazione subito dopo averla creata e successivamente in base alla pianificazione definita.

Il sistema esegue le associazioni anche secondo le seguenti regole:

- State Manager tenta di eseguire l'associazione su tutte le istanze specificate o di destinazione durante un intervallo.
- Se un'associazione non viene eseguita durante un intervallo (ad esempio, perché un valore di concorrenza limita il numero di nodi che potrebbero elaborarla), State Manager tenta di eseguire l'associazione durante l'intervallo successivo.
- State Manager esegue l'associazione dopo le modifiche alla configurazione, ai nodi target, ai documenti o ai parametri dell'associazione. Per ulteriori informazioni, consulta [Capire quando le associazioni vengono applicate alle risorse](#)
- State Manager registra la cronologia per tutti gli intervalli ignorati. È possibile visualizzare la cronologia nella scheda Cronologia di esecuzione.

Pianificazione delle associazioni

È possibile pianificare l'esecuzione delle associazioni a intervalli di base, ad esempio ogni 10 ore, oppure creare pianificazioni più avanzate utilizzando espressioni Cron e della frequenza personalizzate. È inoltre possibile impedire l'esecuzione delle associazioni durante la rispettiva creazione.

Utilizzo di espressioni Cron e della frequenza per pianificare esecuzioni di associazioni

Oltre alle espressioni Cron o della frequenza standard, State Manager supporta anche le espressioni Cron che includono un giorno della settimana e il segno numerico (#), per designare il giorno n di un mese necessario per l'esecuzione di un'associazione. Ecco un esempio che esegue un programma cron il terzo martedì di ogni mese alle 23:30 UTC:

```
cron(30 23 ? * TUE#3 *)
```

Ecco un esempio che viene eseguito il secondo giovedì di ogni mese a mezzanotte UTC:

```
cron(0 0 ? * THU#2 *)
```

State Manager supporta anche il segno (L) per indicare l'ultimo giorno X del mese. Ecco un esempio che esegue un programma cron il terzo martedì di ogni mese a mezzanotte UTC:

```
cron(0 0 ? * 3L *)
```

Per controllare ulteriormente l'esecuzione di un'associazione, ad esempio se si desidera eseguire un'associazione due giorni dopo la patch di martedì, è possibile specificare un offset. Un record offset definisce quanti giorni attendere dopo il giorno programmato per eseguire un'associazione. Ad esempio, se hai specificato un programma cron di `cron(0 0 ? * THU#2 *)`, è possibile specificare il numero 3 nel campo Offset di pianificazione per eseguire l'associazione ogni domenica dopo il secondo giovedì del mese.

Note

Per utilizzare gli offset, è necessario scegliere **Applica associazione solo all'intervallo cron** specificato successivo nella console oppure specificare l'uso del parametro `ApplyOnlyAtCronInterval` dalla linea di comando. Quando una di queste opzioni è attivata, State Manager non esegue l'associazione immediatamente dopo la creazione.

Per ulteriori informazioni sulle espressioni Cron e della frequenza, consulta [Riferimento: espressioni Cron e della frequenza per Systems Manager](#).

Creazione di un'associazione (console)

La procedura seguente descrive come utilizzare la console di Systems Manager per creare un'associazione di State Manager.

Note

Osservare le seguenti informazioni.

- Questa procedura descrive come creare un'associazione che utilizza un documento Command o Policy per i nodi gestiti di destinazione. Per informazioni sulla creazione di un'associazione che utilizza un runbook Automation per indirizzare i nodi o altri tipi di risorse AWS , consulta [Pianificazione delle automazioni con State Manager associazioni](#).
- Durante la creazione di un'associazione, è possibile specificare un massimo di cinque chiavi di tag utilizzando la Console di gestione AWS. Tutte le chiavi dei tag specificate per l'associazione devono essere attualmente assegnate al nodo. In caso contrario, State Manager non riesce a scegliere il nodo come destinazione per l'associazione.

Per creare un State Manager associazione

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli State Manager.
3. Selezionare Create association (Crea associazione).
4. Nel campo Name (Nome), specifica un nome.
5. Nell'elenco Document (Documenti), scegliere l'opzione disponibile accanto al nome del documento. Prendere nota del tipo di documento. Questa procedura si applica solo a documenti Command e Policy. Per informazioni su come creare un'associazione che utilizza un runbook Automation, consultare [Pianificazione delle automazioni con State Manager associazioni](#).

Important

State Manager non supporta associazioni in esecuzione che utilizzano una nuova versione di un documento se tale documento è condiviso da un altro account. State

Manager gestisce sempre la versione default di un documento se condivisa da un altro account, anche se la console di Systems Manager mostra che è stata elaborata una nuova versione. Se si desidera eseguire un'associazione utilizzando una nuova versione di un documento condiviso da un altro account, è necessario impostare la versione del documento su default.

6. Per Parameters (Parametri), specificare i parametri di input necessari.
- 7.
8. (Facoltativo) Scegli un CloudWatch allarme da applicare alla tua associazione per il monitoraggio.

Note

Prendi nota delle seguenti informazioni importanti relative a questa fase.

- L'elenco degli allarmi riporta un massimo di 100 allarmi. Se non vedi il tuo allarme nell'elenco, usa il pulsante AWS Command Line Interface per creare l'associazione. Per ulteriori informazioni, consulta [Creazione di un'associazione \(riga di comando\)](#).
- Per allegare un CloudWatch allarme al comando, il responsabile IAM che crea l'associazione deve disporre dell'autorizzazione per `iam:createServiceLinkedRole`. Per ulteriori informazioni sugli CloudWatch allarmi, consulta [Utilizzo degli CloudWatch allarmi Amazon](#).
- Tenere presente che se l'allarme si attiva, qualsiasi automazione o invocazione di comando in sospeso non viene eseguita.

9. Per Destinazioni, scegli un'opzione. Per informazioni sull'utilizzo delle destinazioni, consulta [Comprendere gli obiettivi e i controlli delle tariffe in State Manager associazioni](#).

Note

Affinché le associazioni create con i runbook di Automation vengano applicate quando vengono rilevati nuovi nodi di destinazione, devono essere soddisfatte determinate condizioni. Per informazioni, consulta [Informazioni sugli aggiornamenti di destinazione con i runbook Automation](#).

10. Nella sezione Specify schedule (Specifica pianificazione), scegliere On Schedule (Conforme a pianificazione) oppure No schedule (Nessuna pianificazione). Se si sceglie On Schedule

(Conforme a pianificazione), utilizzare i pulsanti disponibili per creare una pianificazione cron o rate per l'associazione.

Se non si desidera che l'associazione venga eseguita immediatamente dopo averla creata, scegli **Applica associazione solo all'intervallo Cron** specificato successivo.

11. (Facoltativo) Nel campo **Pianificazione offset**, specificare un numero compreso tra 1 e 6.
12. Nella sezione **Advanced options** (Opzioni avanzate) usare **Compliance severity** (Gravità della conformità) per scegliere un livello di gravità per l'associazione e utilizzare **Change Calendars** (Modificare i calendari) per scegliere un calendario di modifica per l'associazione.

Il report di conformità indica se l'associazione è conforme o non conforme e il livello di gravità specificato qui. Per ulteriori informazioni, consulta [Informazioni State Manager conformità delle associazioni](#).

Il calendario delle modifiche determina quando l'associazione viene eseguita. Se il calendario è chiuso, l'associazione non viene applicata. Se il calendario è aperto, l'associazione viene di conseguenza eseguita. Per ulteriori informazioni, consulta [AWS Systems Manager Modifica calendario](#).

13. Nella sezione **Rate control** (Controllo della velocità) scegli le opzioni per controllare l'esecuzione dell'associazione su più nodi gestiti. Per informazioni sull'utilizzo dei controlli di velocità, consultare [Comprendere gli obiettivi e i controlli delle tariffe in State Manager associazioni](#).

Nella sezione **Simultaneità**, scegli un'opzione:

- Scegli **destinazioni** per immettere il numero assoluto di destinazioni che possono eseguire contemporaneamente l'associazione.
- Scegli **percentuale** per immettere la percentuale del set di destinazione che può eseguire contemporaneamente l'associazione.

Nella sezione **Soglia di errore**, scegli un'opzione:

- Scegli **errori** per immettere il numero assoluto di errori consentiti prima che State Manager arresti l'esecuzione delle associazioni su altre destinazioni.
- Scegli **percentuale** per immettere una percentuale di errori consentiti prima che State Manager arresti l'esecuzione delle associazioni su altre destinazioni.

14. (Facoltativo) In **Opzioni di output**, per salvare l'output del comando in un file, seleziona la casella **Abilita scrittura in S3**. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

Note

Le autorizzazioni S3 che consentono di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza assegnate al nodo gestito e non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova in un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato all'istanza disponga delle autorizzazioni necessarie per scrivere su quel bucket.

Di seguito sono riportate le autorizzazioni minime necessarie per attivare l'output di Amazon S3 per un'associazione. È possibile limitare ulteriormente l'accesso collegando policy IAM a utenti o ruoli all'interno di un account. Come minimo, un profilo dell'istanza Amazon EC2 deve avere un ruolo IAM con la policy gestita AmazonSSMManagedInstanceCore e la seguente policy in linea.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:PutObjectAcl"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    }
  ]
}
```

Per le autorizzazioni minime, il bucket di Amazon S3 in cui esporti deve disporre delle impostazioni di default definite dalla console di Amazon S3. Per ulteriori informazioni sulla

creazione di bucket di Amazon S3, consultare [Creazione di un bucket](#) nella Guida per l'utente di Amazon S3.

 Note

Le operazioni API avviate dal documento SSM durante un'esecuzione di associazione non vengono registrate in AWS CloudTrail.

15. Scegli Crea associazione.

 Note

Se si elimina l'associazione creata, l'associazione non viene più eseguita sulle destinazioni di tale associazione.

Creazione di un'associazione (riga di comando)

La procedura seguente descrive come utilizzare AWS CLI (su Linux o Windows Server) o Tools for PowerShell creare un'associazione. In questa sezione sono inclusi diversi esempi che illustrano come utilizzare le destinazioni e i controlli di velocità. Le destinazioni e i controlli di velocità consentono di assegnare un'associazione a decine o centinaia di istanze controllando al contempo l'esecuzione di tali associazioni. Per ulteriori informazioni sulle destinazioni e sui controlli di velocità, consulta [Comprendere gli obiettivi e i controlli delle tariffe in State Manager associazioni](#).

 Important

Questa procedura descrive come creare un'associazione che utilizza un documento Command o Policy per i nodi gestiti di destinazione. Per informazioni sulla creazione di un'associazione che utilizza un runbook di automazione per indirizzare nodi o altri tipi di AWS risorse, vedere [Pianificazione delle automazioni con State Manager associazioni](#).

Prima di iniziare

Il parametro `targets` è un array di criteri di ricerca che definisce le istanze come destinazioni mediante una combinazione Key-Value specificata. Se si prevede di creare un'associazione su

decine o centinaia di istanze utilizzando il parametro `targets`, esaminare le seguenti opzioni di destinazione prima di iniziare la procedura.

Definire come destinazione nodi specifici specificando gli ID

```
--targets Key=InstanceIds,Values=instance-id-1,instance-id-2,instance-id-3
```

```
--targets  
Key=InstanceIds,Values=i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE,i-07782c72faEXAMPLE
```

Definire come destinazione le istanze utilizzando i tag

```
--targets Key=tag:tag-key,Values=tag-value-1,tag-value-2,tag-value-3
```

```
--targets Key=tag:Environment,Values=Development,Test,Pre-production
```

Scegli come target i nodi utilizzando AWS Resource Groups

```
--targets Key=resource-groups:Name,Values=resource-group-name
```

```
--targets Key=resource-groups:Name,Values=WindowsInstancesGroup
```

Scegli come target tutte le istanze nell'attuale Account AWS e Regione AWS

```
--targets Key=InstanceIds,Values=*
```

Note

Osservare le seguenti informazioni.

- State Manager non supporta associazioni in esecuzione che utilizzano una nuova versione di un documento se tale documento è condiviso da un altro account. State Manager gestisce sempre la versione default di un documento se condivisa da un altro account, anche se la console di Systems Manager mostra che è stata elaborata una nuova versione. Se si desidera eseguire un'associazione utilizzando una nuova versione di un documento condiviso da un altro account, è necessario impostare la versione del documento su default.

- State Manager non supporta il `TargetLocationAlarmConfiguration` parametro per [TargetLocation](#).
- È possibile specificare un massimo di cinque chiavi di tag utilizzando la AWS CLI. Se si utilizza il AWS CLI, tutte le chiavi dei tag specificate nel `create-association` comando devono essere attualmente assegnate al nodo. In caso contrario, State Manager non riesce a scegliere il nodo come destinazione per un'associazione.
- Quando crei un'associazione, specifica quando eseguire la pianificazione. Specificare la pianificazione utilizzando un'espressione Cron o della frequenza. Per ulteriori informazioni sulle espressioni Cron e della frequenza, consulta [Espressioni Cron e della frequenza per le associazioni](#).
- Affinché le associazioni create con i runbook di Automation vengano applicate quando vengono rilevati nuovi nodi di destinazione, devono essere soddisfatte determinate condizioni. Per informazioni, consulta [Informazioni sugli aggiornamenti di destinazione con i runbook Automation](#).

Per creare un'associazione

1. Installa e configura il AWS CLI o il AWS Strumenti per PowerShell, se non l'hai già fatto.

Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

2. Usa il seguente formato per creare un comando che crea un'associazione State Manager. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux & macOS

```
aws ssm create-association \
  --name document_name \
  --document-version version_of_document_applied \
  --instance-id instances_to_apply_association_on \
  --parameters (if any) \
  --targets target_options \
  --association-dispatch-assume-
role arn_of_role_to_be_used_when_dispatching_configurations \
  --schedule-expression "cron_or_rate_expression" \
  --apply-only-at-cron-interval required_parameter_for_schedule_offsets \
  --schedule-offset number_between_1_and_6 \
  --output-location s3_bucket_to_store_output_details \
```

```
--association-name association_name \
--max-errors a_number_of_errors_or_a_percentage_of_target_set \
--max-concurrency a_number_of_instances_or_a_percentage_of_target_set \
--compliance-severity severity_level \
--calendar-names change_calendar_names \
--target-locations aws_region_or_account \
--tags "Key=tag_key,Value=tag_value"
```

Windows

```
aws ssm create-association ^
--name document_name ^
--document-version version_of_document_applied ^
--instance-id instances_to_apply_association_on ^
--parameters (if any) ^
--targets target_options ^
--association-dispatch-assume-
role arn_of_role_to_be_used_when_dispatching_configurations ^
--schedule-expression "cron_or_rate_expression" ^
--apply-only-at-cron-interval required_parameter_for_schedule_offsets ^
--schedule-offset number_between_1_and_6 ^
--output-location s3_bucket_to_store_output_details ^
--association-name association_name ^
--max-errors a_number_of_errors_or_a_percentage_of_target_set ^
--max-concurrency a_number_of_instances_or_a_percentage_of_target_set ^
--compliance-severity severity_level ^
--calendar-names change_calendar_names ^
--target-locations aws_region_or_account ^
--tags "Key=tag_key,Value=tag_value"
```

PowerShell

```
New-SSMAssociation `
-Name document_name `
-DocumentVersion version_of_document_applied `
-InstanceId instances_to_apply_association_on `
-Parameters (if any) `
-Target target_options `
-
AssociationDispatchAssumeRole arn_of_role_to_be_used_when_dispatching_configurations `
-ScheduleExpression "cron_or_rate_expression" `
-ApplyOnlyAtCronInterval required_parameter_for_schedule_offsets `
```

```
-ScheduleOffset number_between_1_and_6 `
-OutputLocation s3_bucket_to_store_output_details `
-AssociationName association_name `
-MaxError a_number_of_errors_or_a_percentage_of_target_set
-MaxConcurrency a_number_of_instances_or_a_percentage_of_target_set `
-ComplianceSeverity severity_level `
-CalendarNames change_calendar_names `
-TargetLocations aws_region_or_account `
-Tags "Key=tag_key,Value=tag_value"
```

L'esempio seguente crea un'associazione sulle istanze con il tag "Environment, Linux". L'associazione usa il documento AWS-UpdateSSMAgent per aggiornare SSM Agent sui nodi target alle 2:00 ogni domenica mattina. Questa associazione viene eseguita contemporaneamente su un massimo di 10 nodi in qualsiasi momento. Inoltre, l'esecuzione dell'associazione viene arrestata su più nodi durante un determinato intervallo di esecuzione se il conteggio degli errori restituiti supera 5. Per la creazione di report di conformità, a questa associazione viene assegnato un livello di gravità Medium (Medio).

Linux & macOS

```
aws ssm create-association \
  --association-name Update_SSM_Agent_Linux \
  --targets Key=tag:Environment,Values=Linux \
  --name AWS-UpdateSSMAgent \
  --association-dispatch-assume-role arn:aws:iam::123456789012:role/
myAssociationDispatchAssumeRole \
  --compliance-severity "MEDIUM" \
  --schedule-expression "cron(0 2 ? * SUN *)" \
  --max-errors "5" \
  --max-concurrency "10"
```

Windows

```
aws ssm create-association ^
  --association-name Update_SSM_Agent_Linux ^
  --targets Key=tag:Environment,Values=Linux ^
  --name AWS-UpdateSSMAgent ^
  --association-dispatch-assume-role arn:aws:iam::123456789012:role/
myAssociationDispatchAssumeRole ^
  --compliance-severity "MEDIUM" ^
```

```
--schedule-expression "cron(0 2 ? * SUN *)" ^
--max-errors "5" ^
--max-concurrency "10"
```

PowerShell

```
New-SSMAssociation `
  -AssociationName Update_SSM_Agent_Linux `
  -Name AWS-UpdateSSMAgent `
  -AssociationDispatchAssumeRole "arn:aws:iam::123456789012:role/
myAssociationDispatchAssumeRole" `
  -Target @{
    "Key"="tag:Environment"
    "Values"="Linux"
  } `
  -ComplianceSeverity MEDIUM `
  -ScheduleExpression "cron(0 2 ? * SUN *)" `
  -MaxConcurrency 10 `
  -MaxError 5
```

L'esempio seguente fa riferimento agli ID nodi mediante un carattere jolly (*). Ciò consente a Systems Manager di creare un'associazione su tutti i nodi nell'attuale Account AWS e Regione AWS. Questa associazione viene eseguita contemporaneamente su un massimo di 10 nodi in qualsiasi momento. Inoltre, l'esecuzione dell'associazione viene arrestata su più nodi durante un determinato intervallo di esecuzione se il conteggio degli errori restituiti supera 5. Per la creazione di report di conformità, a questa associazione viene assegnato un livello di gravità Medium (Medio). Questa associazione utilizza un offset di pianificazione, il che significa che viene eseguito due giorni dopo la pianificazione cron specificata. Include anche il parametro `ApplyOnlyAtCronInterval`, che è necessario per utilizzare l'offset della pianificazione e il che significa che l'associazione non verrà eseguita immediatamente dopo la creazione.

Linux & macOS

```
aws ssm create-association \
  --association-name Update_SSM_Agent_Linux \
  --name "AWS-UpdateSSMAgent" \
  --association-dispatch-assume-role arn:aws:iam::123456789012:role/
myAssociationDispatchAssumeRole \
  --targets "Key=instanceids,Values=*" \
  --compliance-severity "MEDIUM" \
```



```
--schedule-expression "cron(0 2 ? * SUN#2 *)" \
--apply-only-at-cron-interval \
--schedule-offset 2 \
--max-errors "5" \
--max-concurrency "10" \
```

Windows

```
aws ssm create-association ^
  --association-name Update_SSM_Agent_Linux ^
  --name "AWS-UpdateSSMAgent" ^
  --association-dispatch-assume-role arn:aws:iam::123456789012:role/
myAssociationDispatchAssumeRole ^
  --targets "Key=instanceids,Values=*" ^
  --compliance-severity "MEDIUM" ^
  --schedule-expression "cron(0 2 ? * SUN#2 *)" ^
  --apply-only-at-cron-interval ^
  --schedule-offset 2 ^
  --max-errors "5" ^
  --max-concurrency "10" ^
  --apply-only-at-cron-interval
```

PowerShell

```
New-SSMAssociation `
  -AssociationName Update_SSM_Agent_All `
  -Name AWS-UpdateSSMAgent `
  -AssociationDispatchAssumeRole "arn:aws:iam::123456789012:role/
myAssociationDispatchAssumeRole" `
  -Target @{
    "Key"="InstanceIds"
    "Values"="*"
  } `
  -ScheduleExpression "cron(0 2 ? * SUN#2 *)" `
  -ApplyOnlyAtCronInterval `
  -ScheduleOffset 2 `
  -MaxConcurrency 10 `
  -MaxError 5 `
  -ComplianceSeverity MEDIUM `
  -ApplyOnlyAtCronInterval
```

L'esempio seguente crea un'associazione sui nodi in Resource Groups. Il gruppo è denominato "HR-Department». L'associazione usa il documento AWS-UpdateSSMAgent per aggiornare SSM Agent sui nodi target alle 2:00 ogni domenica mattina. Questa associazione viene eseguita contemporaneamente su un massimo di 10 nodi in qualsiasi momento. Inoltre, l'esecuzione dell'associazione viene arrestata su più nodi durante un determinato intervallo di esecuzione se il conteggio degli errori restituiti supera 5. Per la creazione di report di conformità, a questa associazione viene assegnato un livello di gravità Medium (Medio). Questa associazione viene eseguita nella pianificazione Cron specificata. Non viene eseguita immediatamente dopo la creazione dell'associazione.

Linux & macOS

```
aws ssm create-association \  
  --association-name Update_SSM_Agent_Linux \  
  --targets Key=resource-groups:Name,Values=HR-Department \  
  --name AWS-UpdateSSMAgent \  
  --association-dispatch-assume-role arn:aws:iam::123456789012:role/  
myAssociationDispatchAssumeRole \  
  --compliance-severity "MEDIUM" \  
  --schedule-expression "cron(0 2 ? * SUN *)" \  
  --max-errors "5" \  
  --max-concurrency "10" \  
  --apply-only-at-cron-interval
```

Windows

```
aws ssm create-association ^  
  --association-name Update_SSM_Agent_Linux ^  
  --targets Key=resource-groups:Name,Values=HR-Department ^  
  --name AWS-UpdateSSMAgent ^  
  --association-dispatch-assume-role arn:aws:iam::123456789012:role/  
myAssociationDispatchAssumeRole ^  
  --compliance-severity "MEDIUM" ^  
  --schedule-expression "cron(0 2 ? * SUN *)" ^  
  --max-errors "5" ^  
  --max-concurrency "10" ^  
  --apply-only-at-cron-interval
```

PowerShell

```
New-SSMAssociation `
-AssociationName Update_SSM_Agent_Linux `
-Name AWS-UpdateSSMAgent `
-AssociationDispatchAssumeRole "arn:aws:iam::123456789012:role/
myAssociationDispatchAssumeRole" `
-Target @{
    "Key"="resource-groups:Name"
    "Values"="HR-Department"
} `
-ScheduleExpression "cron(0 2 ? * SUN *)" `
-MaxConcurrency 10 `
-MaxError 5 `
-ComplianceSeverity MEDIUM `
-ApplyOnlyAtCronInterval
```

Nell'esempio seguente viene creata un'associazione che viene eseguita sui nodi con il tag di un ID di nodo specifico. L'associazione utilizza il documento di SSM Agent per aggiornare SSM Agent sui nodi di destinazione una volta quando il calendario delle modifiche è aperto. L'associazione controlla lo stato del calendario durante l'esecuzione. Se il calendario viene chiuso al momento dell'avvio e l'associazione viene eseguita una sola volta, non verrà eseguito più perché la finestra di esecuzione dell'associazione è passata. Se il calendario è aperto, l'associazione viene di conseguenza eseguita.

Note

Se si aggiungono nuovi nodi ai tag o ai gruppi di risorse su cui agisce un'associazione quando il calendario delle modifiche è chiuso, l'associazione viene applicata a tali nodi una volta aperto il calendario delle modifiche.

Linux & macOS

```
aws ssm create-association \
--association-name CalendarAssociation \
--targets "Key=instanceids,Values=i-0cb2b964d3e14fd9f" \
--name AWS-UpdateSSMAgent \
```

```
--association-dispatch-assume-role arn:aws:iam::123456789012:role/
myAssociationDispatchAssumeRole \
--calendar-names "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1" \
--schedule-expression "rate(1day)"
```

Windows

```
aws ssm create-association ^
--association-name CalendarAssociation ^
--targets "Key=instanceids,Values=i-0cb2b964d3e14fd9f" ^
--name AWS-UpdateSSMAgent ^
--association-dispatch-assume-role arn:aws:iam::123456789012:role/
myAssociationDispatchAssumeRole ^
--calendar-names "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1" ^
--schedule-expression "rate(1day)"
```

PowerShell

```
New-SSMAssociation `
-AssociationName CalendarAssociation `
-Target @{
    "Key"="tag:instanceids"
    "Values"="i-0cb2b964d3e14fd9f"
} `
-Name AWS-UpdateSSMAgent `
-AssociationDispatchAssumeRole "arn:aws:iam::123456789012:role/
myAssociationDispatchAssumeRole" `
-CalendarNames "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1" `
-ScheduleExpression "rate(1day)"
```

Nell'esempio seguente viene creata un'associazione che viene eseguita sui nodi con il tag di un ID di nodo specifico. L'associazione usa il documento SSM Agent per aggiornare SSM Agent sui nodi target ogni domenica mattina alle 2:00. Questa associazione viene eseguita solo nella pianificazione Cron specificata quando il calendario delle modifiche è aperto. Quando viene creata, l'associazione controlla lo stato del calendario. Se il calendario è chiuso, l'associazione non viene applicata. Quando l'intervallo di applicazione dell'associazione inizia alle 2:00 di domenica, l'associazione verifica se il calendario è aperto. Se il calendario è aperto, l'associazione viene di conseguenza eseguita.

Note

Se si aggiungono nuovi nodi ai tag o ai gruppi di risorse su cui agisce un'associazione quando il calendario delle modifiche è chiuso, l'associazione viene applicata a tali nodi una volta aperto il calendario delle modifiche.

Linux & macOS

```
aws ssm create-association \
  --association-name MultiCalendarAssociation \
  --targets "Key=instanceids,Values=i-0cb2b964d3e14fd9f" \
  --name AWS-UpdateSSMAgent \
  --association-dispatch-assume-role arn:aws:iam::123456789012:role/
myAssociationDispatchAssumeRole \
  --calendar-names "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1"
"arn:aws:ssm:us-east-2:123456789012:document/testCalendar2" \
  --schedule-expression "cron(0 2 ? * SUN *)"
```

Windows

```
aws ssm create-association ^
  --association-name MultiCalendarAssociation ^
  --targets "Key=instanceids,Values=i-0cb2b964d3e14fd9f" ^
  --name AWS-UpdateSSMAgent ^
  --association-dispatch-assume-role arn:aws:iam::123456789012:role/
myAssociationDispatchAssumeRole ^
  --calendar-names "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1"
"arn:aws:ssm:us-east-2:123456789012:document/testCalendar2" ^
  --schedule-expression "cron(0 2 ? * SUN *)"
```

PowerShell

```
New-SSMAssociation `
  -AssociationName MultiCalendarAssociation `
  -Name AWS-UpdateSSMAgent `
  -AssociationDispatchAssumeRole "arn:aws:iam::123456789012:role/
myAssociationDispatchAssumeRole" `
  -Target @{
    "Key"="tag:instanceids"
```

```
"Values"="i-0cb2b964d3e14fd9f"
} `
-CalendarNames "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1"
"arn:aws:ssm:us-east-2:123456789012:document/testCalendar2" `
-ScheduleExpression "cron(0 2 ? * SUN *)"
```

Note

Se si elimina l'associazione creata, l'associazione non viene più eseguita sulle destinazioni di tale associazione. Inoltre, se è stato specificato il parametro `apply-only-at-cron-interval`, è possibile reimpostare questa opzione. A tale scopo, specificare il parametro `no-apply-only-at-cron-interval` quando si aggiorna l'associazione dalla riga di comando. Questo parametro forza l'esecuzione dell'associazione immediatamente dopo l'aggiornamento dell'associazione e in base all'intervallo specificato.

Modifica e creazione di una nuova versione di un'associazione

È possibile modificare un'associazione di State Manager per specificare un nome, una pianificazione, un livello di gravità, destinazioni e nuovi valori. Per le associazioni basate su Command-type documenti SSM, puoi anche scegliere di scrivere l'output del comando in un bucket Amazon Simple Storage Service (Amazon S3). Dopo la modifica di un'associazione, State Manager crea una nuova versione. È possibile visualizzare diverse versioni dopo la modifica, come descritto nelle procedure seguenti.

Note

Affinché le associazioni create con i runbook di Automation vengano applicate quando vengono rilevati nuovi nodi di destinazione, devono essere soddisfatte determinate condizioni. Per informazioni, consulta [Informazioni sugli aggiornamenti di destinazione con i runbook Automation](#).

Le procedure seguenti descrivono come modificare e creare una nuova versione di un'associazione utilizzando la console di Systems Manager, AWS Command Line Interface (AWS CLI) e AWS Strumenti per PowerShell (Tools for PowerShell).

 Important

State Manager non supporta associazioni in esecuzione che utilizzano una nuova versione di un documento se tale documento è condiviso da un altro account. State Manager gestisce sempre la versione default di un documento se condivisa da un altro account, anche se la console di Systems Manager mostra che è stata elaborata una nuova versione. Se si desidera eseguire un'associazione utilizzando una nuova versione di un documento condiviso da un altro account, è necessario impostare la versione del documento su default.

Modifica di un'associazione (console)

La procedura seguente descrive come utilizzare la console di Systems Manager per modificare e creare una nuova versione di un'associazione.

 Note

Per le associazioni che utilizzano documenti SSM Command e non runbook Automation, per svolgere questa procedura è necessario disporre dell'accesso in scrittura a un bucket Amazon S3 esistente. Se non hai mai usato Amazon S3 in precedenza, tieni presente che dovrai sostenere dei costi per l'utilizzo di Amazon S3. Per informazioni su come creare un bucket, consulta [Crea un bucket](#).

Per modificare un State Manager associazione

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli State Manager.
3. Scegliere un'associazione esistente, quindi Modifica.
4. Riconfigurare l'associazione per soddisfare i requisiti correnti.

Per informazioni sulle opzioni di associazione sui documenti Command e Policy, consulta [Creazione di associazioni](#). Per informazioni sulle opzioni di associazione con i runbook Automation, consulta [Pianificazione delle automazioni con State Manager associazioni](#).

5. Scegli Salva modifiche.

6. (Facoltativo) Per visualizzare le informazioni sull'associazione, nella pagina Associations (Associazioni), scegliere il nome dell'associazione modificata, quindi selezionare la scheda Versions (Versioni). Il sistema elenca tutte le versioni dell'associazione create e modificate.
7. (Facoltativo) Per visualizzare l'output delle associazioni basate su documenti SSM Command, procedi come segue:
 - a. Apri la console Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
 - b. Scegliere il nome del bucket Amazon S3 specificato per archiviare l'output del comando, quindi selezionare la cartella denominata con l'ID del nodo che ha eseguito l'associazione. Se è stato scelto di archiviare l'output in una cartella del bucket, aprire innanzitutto tale cartella.
 - c. Eseguire il drill-down su diversi livelli nella cartella `awsrunPowerShell` fino al file `stdout`.
 - d. Per visualizzare il nome host, scegliere Open (Apri) o Download (Scarica).

Modifica di un'associazione (riga di comando)

La procedura seguente descrive come utilizzare AWS CLI (su Linux o Windows Server) o AWS Strumenti per PowerShell modificare e creare una nuova versione di un'associazione.

Per modificare un State Manager associazione

1. Installa e configura AWS CLI o AWS Strumenti per PowerShell, se non l'hai già fatto.

Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

2. Utilizza il formato seguente per creare un comando per modificare e creare una nuova versione di un'associazione State Manager esistente. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Important

Quando chiami [update-association](#), il sistema elimina tutti i parametri opzionali dalla richiesta e sovrascrive l'associazione con valori nulli per tali parametri. Si tratta di un'impostazione predefinita. È necessario specificare tutti i parametri opzionali nella chiamata, anche se non si modificano i parametri. Questo include il parametro `--name`. Prima di chiamare questa azione, consigliamo di chiamare l'operazione [describe-](#)

[association](#) e prendere nota di tutti i parametri opzionali richiesti per la chiamata `update-association`.

Linux & macOS

```
aws ssm update-association \
  --name document_name \
  --document-version version_of_document_applied \
  --instance-id instances_to_apply_association_on \
  --parameters (if any) \
  --targets target_options \
  --association-dispatch-assume-
role arn_of_role_to_be_used_when_dispatching_configurations \
  --schedule-expression "cron_or_rate_expression" \
  --schedule-offset "number_between_1_and_6" \
  --output-location s3_bucket_to_store_output_details \
  --association-name association_name \
  --max-errors a_number_of_errors_or_a_percentage_of_target_set \
  --max-concurrency a_number_of_instances_or_a_percentage_of_target_set \
  --compliance-severity severity_level \
  --calendar-names change_calendar_names \
  --target-locations aws_region_or_account
```

Windows

```
aws ssm update-association ^
  --name document_name ^
  --document-version version_of_document_applied ^
  --instance-id instances_to_apply_association_on ^
  --parameters (if any) ^
  --targets target_options ^
  --association-dispatch-assume-
role arn_of_role_to_be_used_when_dispatching_configurations ^
  --schedule-expression "cron_or_rate_expression" ^
  --schedule-offset "number_between_1_and_6" ^
  --output-location s3_bucket_to_store_output_details ^
  --association-name association_name ^
  --max-errors a_number_of_errors_or_a_percentage_of_target_set ^
  --max-concurrency a_number_of_instances_or_a_percentage_of_target_set ^
  --compliance-severity severity_level ^
  --calendar-names change_calendar_names ^
```

```
--target-locations aws_region_or_account
```

PowerShell

```
Update-SSMAssociation `
    -Name document_name `
    -DocumentVersion version_of_document_applied `
    -InstanceId instances_to_apply_association_on `
    -Parameters (if any) `
    -Target target_options `
    -
AssociationDispatchAssumeRole arn_of_role_to_be_used_when_dispatching_configurations `
    -ScheduleExpression "cron_or_rate_expression" `
    -ScheduleOffset "number_between_1_and_6" `
    -OutputLocation s3_bucket_to_store_output_details `
    -AssociationName association_name `
    -MaxError a_number_of_errors_or_a_percentage_of_target_set `
    -MaxConcurrency a_number_of_instances_or_a_percentage_of_target_set `
    -ComplianceSeverity severity_level `
    -CalendarNames change_calendar_names `
    -TargetLocations aws_region_or_account
```

L'esempio seguente aggiorna un'associazione esistente per modificare il nome in TestHostnameAssociation2. La nuova versione di associazione viene eseguita ogni ora e scrive l'output dei comandi nel bucket Amazon S3 specificato.

Linux & macOS

```
aws ssm update-association \
    --association-id 8dfe3659-4309-493a-8755-01234EXAMPLE \
    --association-name TestHostnameAssociation2 \
    --parameters commands="echo Association" \
    --association-dispatch-assume-role arn:aws:iam::123456789012:role/
myAssociationDispatchAssumeRole \
    --output-location S3Location='{OutputS3Region=us-
east-1,OutputS3BucketName=amzn-s3-demo-bucket,OutputS3KeyPrefix=logs}' \
    --schedule-expression "cron(0 */1 * * ? *)"
```

Windows

```
aws ssm update-association ^
  --association-id 8dfe3659-4309-493a-8755-01234EXAMPLE ^
  --association-name TestHostnameAssociation2 ^
  --parameters commands="echo Association" ^
  --association-dispatch-assume-role arn:aws:iam::123456789012:role/
myAssociationDispatchAssumeRole ^
  --output-location S3Location='{OutputS3Region=us-
east-1,OutputS3BucketName=amzn-s3-demo-bucket,OutputS3KeyPrefix=logs}' ^
  --schedule-expression "cron(0 */1 * * ? *)"
```

PowerShell

```
Update-SSMAssociation `
  -AssociationId b85ccafe-9f02-4812-9b81-01234EXAMPLE `
  -AssociationName TestHostnameAssociation2 `
  -Parameter @{"commands"="echo Association"} `
  -AssociationDispatchAssumeRole "arn:aws:iam::123456789012:role/
myAssociationDispatchAssumeRole" `
  -S3Location_OutputS3BucketName amzn-s3-demo-bucket `
  -S3Location_OutputS3KeyPrefix logs `
  -S3Location_OutputS3Region us-east-1 `
  -ScheduleExpression "cron(0 */1 * * ? *)"
```

L'esempio seguente aggiorna un'associazione esistente per modificare il nome in `CalendarAssociation`. La nuova associazione viene eseguita quando il calendario è aperto e scrive l'output del comando nel bucket Amazon S3 specificato.

Linux & macOS

```
aws ssm update-association \
  --association-id 8dfe3659-4309-493a-8755-01234EXAMPLE \
  --association-name CalendarAssociation \
  --parameters commands="echo Association" \
  --output-location S3Location='{OutputS3Region=us-
east-1,OutputS3BucketName=amzn-s3-demo-bucket,OutputS3KeyPrefix=logs}' \
  --calendar-names "arn:aws:ssm:us-east-1:123456789012:document/testCalendar2"
```

Windows

```
aws ssm update-association ^
--association-id 8dfe3659-4309-493a-8755-01234EXAMPLE ^
--association-name CalendarAssociation ^
--parameters commands="echo Association" ^
--output-location S3Location='{OutputS3Region=us-
east-1,OutputS3BucketName=amzn-s3-demo-bucket,OutputS3KeyPrefix=logs}' ^
--calendar-names "arn:aws:ssm:us-east-1:123456789012:document/testCalendar2"
```

PowerShell

```
Update-SSMAssociation `
-AssociationId b85ccafe-9f02-4812-9b81-01234EXAMPLE `
-AssociationName CalendarAssociation `
-AssociationName OneTimeAssociation `
-Parameter @{"commands"="echo Association"} `
-S3Location_OutputS3BucketName amzn-s3-demo-bucket `
-CalendarNames "arn:aws:ssm:us-east-1:123456789012:document/testCalendar2"
```

L'esempio seguente aggiorna un'associazione esistente per modificare il nome in MultiCalendarAssociation. La nuova associazione viene eseguita quando i calendari sono aperti e scrive l'output del comando nel bucket Amazon S3 specificato.

Linux & macOS

```
aws ssm update-association \
--association-id 8dfe3659-4309-493a-8755-01234EXAMPLE \
--association-name MultiCalendarAssociation \
--parameters commands="echo Association" \
--output-location S3Location='{OutputS3Region=us-
east-1,OutputS3BucketName=amzn-s3-demo-bucket,OutputS3KeyPrefix=logs}' \
--calendar-names "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1"
"arn:aws:ssm:us-east-2:123456789012:document/testCalendar2"
```

Windows

```
aws ssm update-association ^
--association-id 8dfe3659-4309-493a-8755-01234EXAMPLE ^
--association-name MultiCalendarAssociation ^
```

```
--parameters commands="echo Association" ^
--output-location S3Location='{OutputS3Region=us-
east-1,OutputS3BucketName=amzn-s3-demo-bucket,OutputS3KeyPrefix=logs}' ^
--calendar-names "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1"
"arn:aws:ssm:us-east-2:123456789012:document/testCalendar2"
```

PowerShell

```
Update-SSMAssociation `
-AssociationId b85ccafe-9f02-4812-9b81-01234EXAMPLE `
-AssociationName MultiCalendarAssociation `
-Parameter @{"commands"="echo Association"} `
-S3Location_OutputS3BucketName amzn-s3-demo-bucket `
-CalendarNames "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1"
"arn:aws:ssm:us-east-2:123456789012:document/testCalendar2"
```

3. Per visualizzare la nuova versione dell'associazione, esegui il comando seguente.

Linux & macOS

```
aws ssm describe-association \
--association-id b85ccafe-9f02-4812-9b81-01234EXAMPLE
```

Windows

```
aws ssm describe-association ^
--association-id b85ccafe-9f02-4812-9b81-01234EXAMPLE
```

PowerShell

```
Get-SSMAssociation `
-AssociationId b85ccafe-9f02-4812-9b81-01234EXAMPLE | Select-Object *
```

Il sistema restituisce informazioni simili alle seguenti.

Linux & macOS

```
{
  "AssociationDescription": {
    "ScheduleExpression": "cron(0 */1 * * ? *)",
```

```

    "OutputLocation": {
      "S3Location": {
        "OutputS3KeyPrefix": "logs",
        "OutputS3BucketName": "amzn-s3-demo-bucket",
        "OutputS3Region": "us-east-1"
      }
    },
    "Name": "AWS-RunPowerShellScript",
    "Parameters": {
      "commands": [
        "echo Association"
      ]
    },
    "LastExecutionDate": 1559316400.338,
    "Overview": {
      "Status": "Success",
      "DetailedStatus": "Success",
      "AssociationStatusAggregatedCount": {}
    },
    "AssociationId": "b85ccafe-9f02-4812-9b81-01234EXAMPLE",
    "DocumentVersion": "$DEFAULT",
    "LastSuccessfulExecutionDate": 1559316400.338,
    "LastUpdateAssociationDate": 1559316389.753,
    "Date": 1559314038.532,
    "AssociationVersion": "2",
    "AssociationName": "TestHostnameAssociation2",
    "Targets": [
      {
        "Values": [
          "Windows"
        ],
        "Key": "tag:Environment"
      }
    ]
  }
}

```

Windows

```

{
  "AssociationDescription": {
    "ScheduleExpression": "cron(0 */1 * * ? *)",
    "OutputLocation": {

```

```

        "S3Location": {
            "OutputS3KeyPrefix": "logs",
            "OutputS3BucketName": "amzn-s3-demo-bucket",
            "OutputS3Region": "us-east-1"
        },
        "Name": "AWS-RunPowerShellScript",
        "Parameters": {
            "commands": [
                "echo Association"
            ]
        },
        "LastExecutionDate": 1559316400.338,
        "Overview": {
            "Status": "Success",
            "DetailedStatus": "Success",
            "AssociationStatusAggregatedCount": {}
        },
        "AssociationId": "b85ccafe-9f02-4812-9b81-01234EXAMPLE",
        "DocumentVersion": "$DEFAULT",
        "LastSuccessfulExecutionDate": 1559316400.338,
        "LastUpdateAssociationDate": 1559316389.753,
        "Date": 1559314038.532,
        "AssociationVersion": "2",
        "AssociationName": "TestHostnameAssociation2",
        "Targets": [
            {
                "Values": [
                    "Windows"
                ],
                "Key": "tag:Environment"
            }
        ]
    }
}

```

PowerShell

```

AssociationId           : b85ccafe-9f02-4812-9b81-01234EXAMPLE
AssociationName          : TestHostnameAssociation2
AssociationVersion       : 2
AutomationTargetParameterName :
ComplianceSeverity      :

```

```

Date                : 5/31/2019 2:47:18 PM
DocumentVersion     : $DEFAULT
InstanceId          :
LastExecutionDate   : 5/31/2019 3:26:40 PM
LastSuccessfulExecutionDate : 5/31/2019 3:26:40 PM
LastUpdateAssociationDate : 5/31/2019 3:26:29 PM
MaxConcurrency      :
MaxErrors           :
Name                : AWS-RunPowerShellScript
OutputLocation      :
  Amazon.SimpleSystemsManagement.Model.InstanceAssociationOutputLocation
Overview            :
  Amazon.SimpleSystemsManagement.Model.AssociationOverview
Parameters          : {[commands,
  Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
ScheduleExpression  : cron(0 */1 * * ? *)
Status              :
Targets              : {tag:Environment}

```

Eliminazione di associazioni

Utilizza la procedura seguente per eliminare un'associazione mediante la console AWS Systems Manager .

Per eliminare un'associazione

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli State Manager.
3. Seleziona un'associazione e scegli Elimina.

È possibile eliminare più associazioni in un'unica operazione eseguendo un'automazione dalla AWS Systems Manager console. Quando si selezionano più associazioni da eliminare, State Manager avvia la pagina iniziale del runbook Automation con gli ID delle associazioni immessi come valori dei parametri di input.

Per eliminare più associazioni in un'unica operazione

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.

2. Nel pannello di navigazione, scegli State Manager.
3. Selezionare ogni associazione che si desidera eliminare e scegliere Elimina.
4. (Facoltativo) Nell'area Parametri di input aggiuntivi, seleziona il nome della risorsa Amazon (ARN) per il ruolo di assunzione che desideri venga utilizzato dall'automazione durante l'esecuzione. Per creare un nuovo ruolo, selezionare Crea.
5. Seleziona Invia.

Esecuzione dei gruppi Auto Scaling con associazioni

La best practice nell'utilizzo di associazioni per l'esecuzione di gruppi Auto Scaling è utilizzare destinazioni con tag. Il mancato utilizzo di tag potrebbe causare il raggiungimento del limite di associazione.

Se tutti i nodi sono contrassegnati con la stessa chiave e lo stesso valore, è necessaria una sola associazione per eseguire il gruppo Auto Scaling. La procedura seguente descrive come creare tale associazione.

Per creare un'associazione che esegua gruppi Auto Scaling

1. Assicurati che tutti i nodi del gruppo Auto Scaling siano contrassegnati con la stessa chiave e lo stesso valore. Per ulteriori istruzioni su come assegnare tag ai nodi, consulta [Assegnazione dei tag ai gruppi Auto Scaling e alle istanze](#) nella Guida per l'utente di AWS Auto Scaling .
2. Creare un'associazione utilizzando la procedura descritta in [Utilizzo delle associazioni in Systems Manager](#).

Se si sta lavorando nella console, scegliere Specifica tag delle istanze nel campo Targets (Destinazioni). In Tag di istanza, immetti la chiave e il valore del tag per il gruppo Auto Scaling.

Se stai usando la AWS Command Line Interface (AWS CLI), specifica `--targets Key=tag:tag-key,Values=tag-value` dove la chiave e il valore corrispondono a ciò con cui hai taggato i tuoi nodi.

Visualizzazione della cronologia delle associazioni

È possibile visualizzare tutte le esecuzioni per un ID di associazione specifico utilizzando l'operazione [DescribeAssociationExecutions](#) API. Utilizzare questa operazione per vedere lo stato e i relativi dettagli, i risultati, l'ora dell'ultima esecuzione e altre informazioni per un'associazione State Manager.

State Manager è uno strumento di AWS Systems Manager. L'operazione API include inoltre filtri che consentono di individuare le associazioni in base ai criteri specificati. Ad esempio, è possibile specificare una data e un'ora esatte e utilizzare il filtro `GREATER_THAN` per visualizzare le esecuzioni elaborate dopo la data e l'ora specificate.

Se, ad esempio, l'esecuzione di un'associazione non è riuscita, puoi approfondire i dettagli di un'esecuzione specifica utilizzando l'operazione [DescribeAssociationExecutionTargets](#) API. Questa operazione mostra le risorse, come gli ID di nodo, in cui l'associazione è stata eseguita e i diversi stati dell'associazione. Puoi quindi visualizzare la risorsa o il nodo che non è riuscito a eseguire un'associazione. Mediante l'ID risorsa puoi visualizzare i dettagli di esecuzione del comando per vedere quale passaggio del comando ha avuto esito negativo.

Gli esempi in questa sezione includono anche informazioni su come utilizzare l'operazione [StartAssociationsOnce](#) API per eseguire un'associazione una sola volta al momento della creazione. Puoi utilizzare questa operazione API per esaminare le esecuzioni di associazioni con esito negativo. Se vedi un'associazione non riuscita, puoi modificare la risorsa ed eseguire immediatamente l'associazione per verificare se la modifica alla risorsa consente la corretta esecuzione dell'associazione.

Note

Le operazioni API avviate dal documento SSM durante un'esecuzione di associazione non vengono registrate in AWS CloudTrail.

Visualizzazione della cronologia delle associazioni (console)

Segui la procedura riportata sotto per visualizzare la cronologia delle esecuzioni di un ID associazione specifico e visualizzare i dettagli delle esecuzioni per una o più risorse.

Per visualizzare la cronologia di esecuzioni per un ID associazione specifico

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Scegli State Manager.
3. Nel campo ID associazione, scegli un'associazione di cui si desidera visualizzare la cronologia.
4. Selezionare il pulsante View details (Visualizza dettagli).
5. Scegliere la scheda Cronologia delle esecuzioni.

6. Scegliere un'associazione di cui si desidera visualizzare i dettagli delle esecuzioni a livello di risorsa. Ad esempio, scegliere un'associazione che mostri uno stato Failed (Non riuscito). È possibile quindi visualizzare i dettagli delle esecuzioni per i nodi che non sono riusciti a eseguire l'associazione.

Utilizzare i filtri della casella di ricerca per individuare l'esecuzione di cui visualizzare i dettagli.

7. Scegliere un ID di esecuzione. Viene aperta la pagina Association execution targets (Target di esecuzione dell'associazione). In questa pagina sono mostrate tutte le risorse che hanno eseguito l'associazione.
8. Scegliere un ID risorsa per visualizzare informazioni specifiche sulla risorsa.

Utilizzare i filtri della casella di ricerca per individuare la risorsa di cui visualizzare i dettagli.

9. Se si sta esaminando un'associazione che non è stato possibile eseguire, è possibile utilizzare il pulsante Apply association now (Applica associazione) per eseguire un'associazione una volta al momento della creazione. Dopo avere effettuato le modifiche alla risorsa in cui non è stato possibile eseguire l'associazione, scegliere il collegamento Association ID (ID associazione) nel percorso di navigazione.
10. Scegliere il pulsante Apply association now (Applica associazione). Dopo il completamento dell'esecuzione, verificare che l'associazione sia stata eseguita correttamente.

Visualizzazione della cronologia delle associazioni (riga di comando)

La procedura seguente descrive come utilizzare AWS Command Line Interface (AWS CLI) (su Linux o Windows Server) o AWS Strumenti per PowerShell visualizzare la cronologia di esecuzione per un ID di associazione specifico. In seguito, la procedura descrive come visualizzare i dettagli di esecuzione per una o più risorse.

Per visualizzare la cronologia di esecuzioni per un ID associazione specifico

1. Installa e configura il AWS CLI o il AWS Strumenti per PowerShell, se non l'hai già fatto.

Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

2. Eseguire il comando riportato sotto per visualizzare un elenco di esecuzioni per un ID associazione specifico.

Linux & macOS

```
aws ssm describe-association-executions \  
  --association-id ID \  
  --filters Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=GREATER_THAN
```

Note

Questo comando include un filtro per limitare i risultati solo alle esecuzioni che si sono verificate dopo una data e un'ora specifiche. Per visualizzare tutte le esecuzioni per un determinato ID associazione, rimuovere il parametro `--filters` e il valore `Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=GREATER_THAN`.

Windows

```
aws ssm describe-association-executions ^  
  --association-id ID ^  
  --filters Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=GREATER_THAN
```

Note

Questo comando include un filtro per limitare i risultati solo alle esecuzioni che si sono verificate dopo una data e un'ora specifiche. Per visualizzare tutte le esecuzioni per un determinato ID associazione, rimuovere il parametro `--filters` e il valore `Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=GREATER_THAN`.

PowerShell

```
Get-SSMAssociationExecution `  
  -AssociationId ID `  
  -Filter  
  @{"Key"="CreatedTime";"Value"="2019-06-01T19:15:38.372Z";"Type"="GREATER_THAN"}
```

Note

Questo comando include un filtro per limitare i risultati solo alle esecuzioni che si sono verificate dopo una data e un'ora specifiche. Per visualizzare tutte le esecuzioni per un determinato ID associazione, rimuovere il parametro `-Filter` e il valore `@{"Key"="CreatedTime";"Value"="2019-06-01T19:15:38.372Z";"Type"="GREAT`

Il sistema restituisce informazioni simili alle seguenti.

Linux & macOS

```
{
  "AssociationExecutions":[
    {
      "Status":"Success",
      "DetailedStatus":"Success",
      "AssociationId":"c336d2ab-09de-44ba-8f6a-6136cEXAMPLE",
      "ExecutionId":"76a5a04f-caf6-490c-b448-92c02EXAMPLE",
      "CreatedTime":1523986028.219,
      "AssociationVersion":"1"
    },
    {
      "Status":"Success",
      "DetailedStatus":"Success",
      "AssociationId":"c336d2ab-09de-44ba-8f6a-6136cEXAMPLE",
      "ExecutionId":"791b72e0-f0da-4021-8b35-f95dfEXAMPLE",
      "CreatedTime":1523984226.074,
      "AssociationVersion":"1"
    },
    {
      "Status":"Success",
      "DetailedStatus":"Success",
      "AssociationId":"c336d2ab-09de-44ba-8f6a-6136cEXAMPLE",
      "ExecutionId":"ecec60fa-6bb0-4d26-98c7-140308EXAMPLE",
      "CreatedTime":1523982404.013,
      "AssociationVersion":"1"
    }
  ]
}
```

Windows

```
{
  "AssociationExecutions":[
    {
      "Status":"Success",
      "DetailedStatus":"Success",
      "AssociationId":"c336d2ab-09de-44ba-8f6a-6136cEXAMPLE",
      "ExecutionId":"76a5a04f-caf6-490c-b448-92c02EXAMPLE",
      "CreatedTime":1523986028.219,
      "AssociationVersion":"1"
    },
    {
      "Status":"Success",
      "DetailedStatus":"Success",
      "AssociationId":"c336d2ab-09de-44ba-8f6a-6136cEXAMPLE",
      "ExecutionId":"791b72e0-f0da-4021-8b35-f95dfEXAMPLE",
      "CreatedTime":1523984226.074,
      "AssociationVersion":"1"
    },
    {
      "Status":"Success",
      "DetailedStatus":"Success",
      "AssociationId":"c336d2ab-09de-44ba-8f6a-6136cEXAMPLE",
      "ExecutionId":"ecec60fa-6bb0-4d26-98c7-140308EXAMPLE",
      "CreatedTime":1523982404.013,
      "AssociationVersion":"1"
    }
  ]
}
```

PowerShell

```
AssociationId      : c336d2ab-09de-44ba-8f6a-6136cEXAMPLE
AssociationVersion  : 1
CreatedTime        : 8/18/2019 2:00:50 AM
DetailedStatus     : Success
ExecutionId        : 76a5a04f-caf6-490c-b448-92c02EXAMPLE
LastExecutionDate   : 1/1/0001 12:00:00 AM
ResourceCountByStatus : {Success=1}
Status             : Success
```

```

AssociationId      : c336d2ab-09de-44ba-8f6a-6136cEXAMPLE
AssociationVersion  : 1
CreatedTime        : 8/11/2019 2:00:54 AM
DetailedStatus     : Success
ExecutionId        : 791b72e0-f0da-4021-8b35-f95dfEXAMPLE
LastExecutionDate  : 1/1/0001 12:00:00 AM
ResourceCountByStatus : {Success=1}
Status             : Success

AssociationId      : c336d2ab-09de-44ba-8f6a-6136cEXAMPLE
AssociationVersion  : 1
CreatedTime        : 8/4/2019 2:01:00 AM
DetailedStatus     : Success
ExecutionId        : ecec60fa-6bb0-4d26-98c7-140308EXAMPLE
LastExecutionDate  : 1/1/0001 12:00:00 AM
ResourceCountByStatus : {Success=1}
Status             : Success

```

È possibile limitare i risultati utilizzando uno o più filtri. L'esempio seguente restituisce tutte le associazioni eseguite prima di una data e un'ora specifiche.

Linux & macOS

```

aws ssm describe-association-executions \
  --association-id ID \
  --filters Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=LESS_THAN

```

Windows

```

aws ssm describe-association-executions ^
  --association-id ID ^
  --filters Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=LESS_THAN

```

PowerShell

```

Get-SSMAssociationExecution `
  -AssociationId 14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE `
  -Filter
  @{"Key"="CreatedTime";"Value"="2019-06-01T19:15:38.372Z";"Type"="LESS_THAN"}

```

L'esempio seguente restituisce tutte le associazioni eseguite correttamente dopo una data e un'ora specifiche.

Linux & macOS

```
aws ssm describe-association-executions \  
  --association-id ID \  
  --filters Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=GREATER_THAN  
  Key=Status,Value=Success,Type=EQUAL
```

Windows

```
aws ssm describe-association-executions ^  
  --association-id ID ^  
  --filters Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=GREATER_THAN  
  Key=Status,Value=Success,Type=EQUAL
```

PowerShell

```
Get-SSMAssociationExecution `   
  -AssociationId 14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE `   
  -Filter @{   
    "Key"="CreatedTime";   
    "Value"="2019-06-01T19:15:38.372Z";   
    "Type"="GREATER_THAN"   
  },   
  @{   
    "Key"="Status";   
    "Value"="Success";   
    "Type"="EQUAL"   
  }   
}
```

3. Eseguire il comando riportato seguente per visualizzare tutti i target in cui l'associazione specifica è stata eseguita.

Linux & macOS

```
aws ssm describe-association-execution-targets \  
  --association-id ID \  
  --filters Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=GREATER_THAN  
  Key=Status,Value=Success,Type=EQUAL
```



```
--execution-id ID
```

Windows

```
aws ssm describe-association-execution-targets ^  
  --association-id ID ^  
  --execution-id ID
```

PowerShell

```
Get-SSMAssociationExecutionTarget `   
  -AssociationId 14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE `   
  -ExecutionId 76a5a04f-caf6-490c-b448-92c02EXAMPLE
```

È possibile limitare i risultati utilizzando uno o più filtri. L'esempio seguente restituisce informazioni su tutti i target in cui l'associazione specifica non è stata eseguita.

Linux & macOS

```
aws ssm describe-association-execution-targets \  
  --association-id ID \  
  --execution-id ID \  
  --filters Key=Status,Value="Failed"
```

Windows

```
aws ssm describe-association-execution-targets ^  
  --association-id ID ^  
  --execution-id ID ^  
  --filters Key=Status,Value="Failed"
```

PowerShell

```
Get-SSMAssociationExecutionTarget `   
  -AssociationId 14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE `   
  -ExecutionId 76a5a04f-caf6-490c-b448-92c02EXAMPLE `   
  -Filter @{   
    "Key"="Status";   
    "Value"="Failed"
```

```
}
```

L'esempio seguente restituisce informazioni su un nodo gestito specifico in cui un'associazione non è stata eseguita.

Linux & macOS

```
aws ssm describe-association-execution-targets \
  --association-id ID \
  --execution-id ID \
  --filters Key=Status,Value=Failed Key=ResourceId,Value="i-02573cafcfEXAMPLE"
  Key=ResourceType,Value=ManagedInstance
```

Windows

```
aws ssm describe-association-execution-targets ^
  --association-id ID ^
  --execution-id ID ^
  --filters Key=Status,Value=Failed Key=ResourceId,Value="i-02573cafcfEXAMPLE"
  Key=ResourceType,Value=ManagedInstance
```

PowerShell

```
Get-SSMAssociationExecutionTarget `
  -AssociationId 14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE `
  -ExecutionId 76a5a04f-caf6-490c-b448-92c02EXAMPLE `
  -Filter @{
    "Key"="Status";
    "Value"="Success"
  },
  @{
    "Key"="ResourceId";
    "Value"="i-02573cafcfEXAMPLE"
  },
  @{
    "Key"="ResourceType";
    "Value"="ManagedInstance"
  }
}
```

4. Se stai esaminando un'associazione che non è riuscita a funzionare, puoi utilizzare l'operazione [StartAssociationsOnce](#) API per eseguire un'associazione immediatamente e solo una volta.

Dopo aver modificato la risorsa in cui non è stato possibile eseguire l'associazione, eseguire il comando riportato sotto per eseguire l'associazione immediatamente e una sola volta.

Linux & macOS

```
aws ssm start-associations-once \  
--association-id ID
```

Windows

```
aws ssm start-associations-once ^  
--association-id ID
```

PowerShell

```
Start-SSMAssociationsOnce `  
-AssociationId ID
```

Utilizzo delle associazioni tramite IAM

State Manager utilizza [gli obiettivi](#) per scegliere con quali istanze configurare le associazioni. Originariamente, le associazioni venivano create specificando un nome di documento (Name) e un ID di istanza (InstanceId). In questo modo è stata creata un'associazione tra un documento e un'istanza o nodo gestito. Le associazioni erano identificate da questi parametri. Questi parametri sono ora obsoleti, ma sono comunque supportati. Le risorse `instanceemanaged-instances` sono stati aggiunti come risorse alle azioni `WithNameeInstanceId`.

AWS Identity and Access Management Il comportamento di applicazione delle policy (IAM) dipende dal tipo di risorsa specificata. Le risorse per operazioni di State Manager vengono applicate solo in base alla richiesta inoltrata. State Manager non esegue un controllo approfondito delle proprietà delle risorse nell'account. Una richiesta viene convalidata in base alle risorse di policy solo se il parametro della richiesta contiene le risorse di policy specificate. Ad esempio, se si specifica un'istanza nel blocco di risorse, la policy viene applicata se la richiesta utilizza il parametro `InstanceId`. Il parametro `Targets` per ogni risorsa nell'account non viene controllato per questo `InstanceId`.

Di seguito sono riportati alcuni casi con comportamento confuso:

- [DescribeAssociation](#), [DeleteAssociation](#), e [UpdateAssociation](#) usa `instancemanaged-instance`, e `document` risorse per specificare il modo obsoleto di riferirsi alle associazioni. Ciò include tutte le associazioni create con il parametro obsoleto `InstanceId`.
- [CreateAssociation](#), [CreateAssociationBatch](#), e [UpdateAssociation](#) usa `instance` e `managed-instance` risorse per specificare il modo obsoleto di riferirsi alle associazioni. Ciò include tutte le associazioni create con il parametro obsoleto `InstanceId`. Il tipo di risorsa `document` fa parte del modo obsoleto di riferirsi alle associazioni ed è proprietà effettiva di un'associazione. Ciò significa che è possibile creare policy IAM con autorizzazioni `Allow` o `Deny` per entrambe le azioni `Create` e `Update` in base al nome del documento.

Per ulteriori informazioni sull'uso delle policy IAM con Systems Manager, consultare [Gestione delle identità e degli accessi per AWS Systems Manager](#) oppure [Operazioni, risorse e chiavi di condizione per AWS Systems Manager](#) nella Guida all'autorizzazione dei servizi.

Creazione di associazioni che eseguono file MOF

È possibile eseguire file MOF (Managed Object Format) per imporre uno stato di destinazione sui nodi Windows Server gestiti con State Manager, utilizzando il documento `AWS-ApplyDSCMofs` SSM. Il documento `AWS-ApplyDSCMofs` è caratterizzato da due modalità di esecuzione. La prima consente di configurare l'associazione per analizzare e segnalare se i nodi gestiti sono nello stato desiderato definito nei file MOF specificati. La seconda consente di eseguire i file MOF e modificare la configurazione dei nodi in base alle risorse e ai relativi valori definiti nei file MOF. Il `AWS-ApplyDSCMofs` documento consente di scaricare ed eseguire i file di configurazione MOF da Amazon Simple Storage Service (Amazon S3), da una condivisione locale o da un sito Web sicuro con un dominio HTTPS.

State Manager registra e indica lo stato di ciascuna esecuzione di file MOF durante l'esecuzione di ogni associazione. State Manager, inoltre, indica l'output di ogni esecuzione di file MOF come evento di conformità che è possibile visualizzare nella pagina [Conformità di AWS Systems Manager](#).

L'esecuzione dei file MOF è basata su Windows PowerShell Desired State Configuration (PowerShell DSC). PowerShell DSC è una piattaforma dichiarativa utilizzata per la configurazione, l'implementazione e la gestione dei sistemi Windows. PowerShell DSC consente agli amministratori di descrivere, in semplici documenti di testo denominati configurazioni DSC, come desiderano configurare un server. Una configurazione PowerShell DSC è uno PowerShell script specializzato che indica cosa fare, ma non come farlo. L'esecuzione della configurazione produce un file MOF. Il file MOF può essere applicato a uno o più server per ottenere la configurazione desiderata per tali server. PowerShell Le risorse DSC svolgono il lavoro effettivo di applicazione della configurazione.

Per ulteriori informazioni, vedere Panoramica della configurazione dello stato PowerShell desiderato di [Windows](#).

Argomenti

- [Utilizzo di Amazon S3 per archiviare gli artefatti](#)
- [Risoluzione delle credenziali nei file MOF](#)
- [Utilizzo di token nei file MOF](#)
- [Prerequisiti per la creazione di associazioni che eseguono file MOF](#)
- [Creazione di un'associazione che esegue i file MOF](#)
- [Risoluzione dei problemi relativi alla creazione di associazioni che eseguono file MOF](#)
- [Visualizzazione dei dettagli di conformità delle risorse DSC](#)

Utilizzo di Amazon S3 per archiviare gli artefatti

Se utilizzi Amazon S3 per archiviare PowerShell moduli, file MOF, report di conformità o report sullo stato, allora il ruolo AWS Identity and Access Management (IAM) utilizzato da AWS Systems Manager SSM Agent must have `GetObject` e `ListBucket` le autorizzazioni sul bucket. Se non disponi di queste autorizzazioni, il sistema restituisce un errore Accesso negato. Ecco informazioni importanti sulla memorizzazione degli artefatti in Amazon S3.

- Se il bucket si trova in un altro bucket Account AWS, crea una policy sulle risorse del bucket che conceda l'account (o il ruolo IAM) e le autorizzazioni. `GetObject` `ListBucket`
- Se desideri utilizzare le risorse DSC personalizzate, è possibile scaricarle da un bucket Amazon S3. Puoi anche installarli automaticamente dalla galleria. PowerShell
- Se utilizzi Amazon S3 come sorgente del modulo, carica il modulo come file Zip nel seguente formato con distinzione tra maiuscole e minuscole: *Module***Name** _ .zip. *Module***Version** Ad esempio: _1.0.0.zip. MyModule
- Tutti i file devono trovarsi nella radice del bucket. Le strutture di cartella non sono supportate.

Risoluzione delle credenziali nei file MOF

Le credenziali vengono risolte utilizzando [AWS Secrets Manager](#) o [AWS Systems Manager Parameter Store](#). Ciò consente di impostare la rotazione automatica delle credenziali. Questo consente inoltre a DSC di propagare automaticamente le credenziali sui tuoi server senza ridistribuire i file MOF.

Per utilizzare un AWS Secrets Manager segreto in una configurazione, create un oggetto `PSCredential` in cui il nome utente sia il `SecretId` o il `secretARN` del segreto che contiene la credenziale. È possibile specificare qualsiasi valore per la password. Il valore viene ignorato. Di seguito è riportato un esempio.

```
Configuration MyConfig
{
    $ss = ConvertTo-SecureString -String 'a_string' -AsPlaintext -Force
    $credential = New-Object PSCredential('a_secret_or_ARN', $ss)

    Node localhost
    {
        File file_name
        {
            DestinationPath = 'C:\MyFile.txt'
            SourcePath = '\\FileServer\Share\MyFile.txt'
            Credential = $credential
        }
    }
}
```

Compila il tuo MOF utilizzando l'impostazione nei dati di configurazione. `PsAllowPlaintextPassword`. Questo è consentito perché la credenziale contiene solo un'etichetta.

In Secrets Manager, assicurati che il nodo abbia `GetSecretValue` accesso a una IAM Managed Policy e, facoltativamente, alla `Secret Resource Policy`, se ne esiste una. Per funzionare con DSC, il segreto deve essere nel formato seguente.

```
{ 'Username': 'a_name', 'Password': 'a_password' }
```

Il segreto può avere altre proprietà (ad esempio, proprietà utilizzate per la rotazione), ma deve avere almeno le proprietà del nome utente e della password.

Ti consigliamo di utilizzare un metodo di rotazione multiutente, in cui hai due nomi utente e password diversi e la AWS Lambda funzione di rotazione passa da uno all'altro. Questo metodo consente di avere più account attivi eliminando il rischio di bloccare un utente durante la rotazione.

Utilizzo di token nei file MOF

I token offrono la possibilità di modificare i valori di proprietà della risorsa dopo la compilazione del file MOF. Ciò consente di riutilizzare i file MOF comuni su più server che richiedono configurazioni simili.

La sostituzione dei token funziona solo per le proprietà della risorsa di tipo `String`. Tuttavia, se la risorsa ha una proprietà del nodo CIM nidificata, risolverà anche i token delle proprietà `String` in tale nodo CIM. Non è possibile usare la sostituzione dei token per numeri o array.

Ad esempio, si consideri uno scenario in cui si utilizza la `ComputerManagement` risorsa `x` e si desidera rinominare il computer utilizzando DSC. In genere avresti bisogno di un file MOF dedicato per quel computer. Tuttavia, con il supporto dei token, è possibile creare un singolo file MOF e applicarlo a tutti i nodi. Nella proprietà `ComputerName`, invece dell'hard coding del nome del computer nel MOF, è possibile utilizzare un token del tipo tag di istanza. Il valore viene risolto durante l'analisi del file MOF. Guarda l'esempio seguente.

```
Configuration MyConfig
{
    xComputer Computer
    {
        ComputerName = '{tag:ComputerName}'
    }
}
```

È possibile quindi impostare un tag sul nodo gestito nella console Systems Manager oppure un tag Amazon Elastic Compute Cloud (Amazon EC2) nella console Amazon EC2. Quando eseguite il documento, lo script sostituisce il token `{tag:ComputerName}` con il valore del tag di istanza.

Inoltre, è possibile combinare più tag in una singola proprietà, come mostrato nell'esempio che segue:

```
Configuration MyConfig
{
    File MyFile
    {
        DestinationPath = '{env:TMP}\{tag:ComputerName}'
        Type = 'Directory'
    }
}
```

È possibile utilizzare 5 diversi tipi di token:

- `tag`: tag di Amazon EC2 o di nodi gestiti.
- `tagb64`: è uguale a `tag`, ma il sistema utilizza base64 per decodificare il valore. Ciò consente di utilizzare caratteri speciali nei valori dei tag.

- `env`: risolve variabili di ambiente.
- `ssm`: valori di Parameter Store (archivio parametri). Sono supportati solo i tipi `String` e `Secure String`.
- `tagssm`: è uguale al `tag`, ma se il `tag` non è impostato sul nodo, il sistema cerca di risolvere il valore da un parametro di Systems Manager con lo stesso nome. È utile in situazioni in cui si desidera un valore predefinito globale, ma si vuole sovrascriverlo su un singolo nodo (per esempio, distribuzioni `one-box`).

Ecco un esempio di Parameter Store (archivio parametri) che usa il tipo di token `ssm`.

```
File MyFile
{
    DestinationPath = "C:\ProgramData\ConnectionData.txt"
    Content = "{ssm:%servicePath%/ConnectionData}"
}
```

I token giocano un ruolo importante nel ridurre il codice ridondante, rendendo i file MOF generici e riutilizzabili. Se è possibile evitare file MOF specifici del server, non è necessario un servizio di creazione di file MOF. Un servizio di creazione di file MOF aumenta i costi, rallenta i tempi di provisioning e aumenta il rischio di deviazioni di configurazione tra i nodi raggruppate, a causa dell'installazione di diverse versioni dei moduli sul server di sviluppo durante la compilazione dei file MOF.

Prerequisiti per la creazione di associazioni che eseguono file MOF

Prima di creare un'associazione che esegue i file MOF, verifica che sui nodi gestiti siano installati i seguenti prerequisiti:

- Windows PowerShell versione 5.0 o successiva. Per ulteriori informazioni, vedi Requisiti PowerShell di sistema [Windows](#) su Microsoft.com.
- [AWS Tools for Windows PowerShell](#) 3.3.261.0 o versioni successive
- SSM Agent 2.2 o versione successiva.

Creazione di un'associazione che esegue i file MOF

Per creare un'associazione che esegue i file MOF

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli State Manager.
3. Selezionare State Manager poi Crea associazione.
4. Nel campo Name (Nome), specifica un nome. Questo passaggio è facoltativo, ma è consigliato. Un nome può aiutare a comprendere lo scopo dell'associazione al momento della creazione. Gli spazi non sono consentiti nel nome.
5. Nell'elenco Document (Documento) scegliere **AWS-ApplyDSCMofs**.
6. Nella sezione Parameters (Parametri), specificare le proprie scelte per i parametri di input obbligatori e opzionali.
 - a. Mofs To Apply (MOF da applicare): specificare uno o più file MOF da eseguire durante l'esecuzione dell'associazione. Utilizzare le virgole per separare un elenco di file MOF. Systems Manager itera attraverso l'elenco dei file MOF e li esegue nell'ordine specificato dall'elenco separato da virgole.
 - Un nome del bucket Amazon S3. I nomi di bucket devono utilizzare lettere minuscole. Specificare queste informazioni nel seguente formato.

```
s3:amzn-s3-demo-bucket:MOF_file_name.mof
```

Se vuoi specificare un Regione AWS, usa il seguente formato.

```
s3:bucket_Region:amzn-s3-demo-bucket:MOF_file_name.mof
```

- Un sito web sicuro. Specificare queste informazioni nel seguente formato.

```
https://domain_name/MOF_file_name.mof
```

Ecco un esempio.

```
https://www.example.com/TestMOF.mof
```

- Un file system su una condivisione locale. Specificare queste informazioni nel seguente formato.

```
\server_name\shared_folder_name\MOF_file_name.mof
```

Ecco un esempio.

```
\StateManagerAssociationsBox\MOFs_folder\MyMof.mof
```

- Service Path (Percorso del servizio):** (facoltativo) un percorso del servizio è un prefisso di bucket Amazon S3 in cui si desidera scrivere i report e le informazioni sullo stato. In alternativa, un percorso del servizio è un percorso per i tag basati sul parametro Parameter Store. Quando risolve i tag basati su parametri, il sistema utilizza {ssm: %ServicePath %/*parameter_name*} per inserire il valore ServicePath nel nome del parametro. Ad esempio, se il percorso del servizio è "", il sistema risolve il parametro come:/. WebServers/Production WebServers/Production *parameter_name* Questa funzione è utile quando si eseguono più ambienti nello stesso account.
- Report Bucket Name (Nome bucket per report):** (facoltativo) immettere il nome di un bucket Amazon S3 in cui si desidera scrivere i dati di conformità. I report vengono salvati in questo bucket in formato JSON.

 Note

È possibile aggiungere come prefisso al nome del bucket una regione in cui si trova il bucket. Ecco un esempio: us-west-2: MyMOFBucket. Se si sta usando un proxy per gli endpoint Amazon S3 in una determinata regione che non include us-east-1, aggiungere come prefisso al nome del bucket una regione. Se al nome del bucket non viene applicato un prefisso, troverà automaticamente la regione del bucket utilizzando l'endpoint us-east-1.

- Mof Operation Mode (Modalità operazione MOF):** scegliere il comportamento di State Manager durante l'esecuzione dell'associazione **AWS-ApplyDSCMofs**:
 - **Apply (Applica):** correggere le configurazioni non conformi dei nodi.
 - **ReportOnly:** non correggete le configurazioni dei nodi, ma registrate invece tutti i dati di conformità e segnalate i nodi non conformi.

- e. **Status Bucket Name (Nome bucket stato):** (facoltativo) immettere il nome di un bucket Amazon S3 in cui si desidera scrivere le informazioni sullo stato di esecuzione del file MOF. Questi report di stato sono riepiloghi singleton dell'esecuzione di conformità più recente di un nodo. Ciò significa che il report verrà sovrascritto la volta successiva che l'associazione eseguirà i file MOF.

 Note

È possibile aggiungere come prefisso al nome del bucket una regione in cui si trova il bucket. Ecco un esempio: `us-west-2:amzn-s3-demo-bucket`. Se si sta usando un proxy per gli endpoint Amazon S3 in una determinata regione che non include `us-east-1`, aggiungere come prefisso al nome del bucket una regione. Se al nome del bucket non viene applicato un prefisso, troverà automaticamente la regione del bucket utilizzando l'endpoint `us-east-1`.

- f. **Nome del bucket di origine del modulo:** (Facoltativo) Inserisci il nome di un bucket Amazon S3 che contiene i file del modulo. PowerShell Se si specifica `None` (Nessuno), scegliere `True` (Vero) come opzione successiva, `Allow PS Gallery Module Source` (Consenti origine del modulo della galleria PS).

 Note

È possibile aggiungere come prefisso al nome del bucket una regione in cui si trova il bucket. Ecco un esempio: `us-west-2:amzn-s3-demo-bucket`. Se si sta usando un proxy per gli endpoint Amazon S3 in una determinata regione che non include `us-east-1`, aggiungere come prefisso al nome del bucket una regione. Se al nome del bucket non viene applicato un prefisso, troverà automaticamente la regione del bucket utilizzando l'endpoint `us-east-1`.

- g. **Consenti sorgente del modulo PS Gallery:** (Facoltativo) Scegli `True` da cui scaricare PowerShell i moduli. <https://www.powershellgallery.com/> Se scegli `False`, specifica una fonte per l'opzione precedente, `ModuleSourceBucketName`.
- h. **Proxy Uri (Uri proxy):** (facoltativo) utilizzare questa opzione per scaricare i file MOF da un server proxy.
- i. **Reboot Behavior (Comportamento di riavvio):** (facoltativo) specificare uno dei seguenti comportamenti di riavvio se l'esecuzione del file MOF richiede il riavvio:

- **AfterMof:** riavvia il nodo dopo che tutte le esecuzioni MOF sono state completate. Anche se più esecuzioni di file MOF richiedono il riavvio, il sistema attende che tutte le esecuzioni vengano completate prima di riavviare.
 - **Immediately (Immediatamente):** riavvia il nodo ogni volta che un'esecuzione di file MOF lo richiede. Se si eseguono più file MOF che richiedono il riavvio, i nodi saranno riavviati più volte.
 - **Never (Mai):** i nodi non vengono riavviati, neanche se l'esecuzione di file MOF lo richiede esplicitamente.
- j. **Use Computer Name For Reporting (Usa nome computer per il reporting):** (facoltativo) abilitare questa opzione per utilizzare il nome del computer per il reporting delle informazioni di conformità. Il valore predefinito è `false` (falso): ciò significa che il sistema utilizza l'ID nodo per il reporting delle informazioni di conformità.
- k. **Abilita registrazione dettagliata:** (facoltativo) si consiglia di abilitare la registrazione dettagliata quando si distribuiscono i file MOF per la prima volta.

 Important

Se abilitata, la registrazione dettagliata scrive più dati sul bucket Amazon S3 rispetto alla registrazione standard dell'esecuzione di un'associazione. Questo può comportare un rallentamento delle prestazioni e costi di archiviazione maggiori per Amazon S3. Per ridurre i problemi di dimensioni dell'archiviazione, si consiglia di abilitare le policy del ciclo di vita del bucket Amazon S3. Per ulteriori informazioni, consulta [Come creare una policy del ciclo di vita per un bucket S3](#) nella Guida per l'utente Amazon Simple Storage Service.

- l. **Abilita registrazione di debug:** (facoltativo) si consiglia di abilitare la registrazione di debug se si desidera risolvere gli errori dei file MOF. È inoltre consigliabile disattivare questa opzione per l'uso normale.

 Important

Quando è abilitata, la registrazione di debug scrive più dati nel bucket Amazon S3 rispetto alla registrazione standard di esecuzione dell'associazione. Questo può comportare un rallentamento delle prestazioni e costi di archiviazione maggiori per Amazon S3. Per ridurre i problemi di dimensioni dell'archiviazione, si consiglia di abilitare le policy del ciclo di vita del bucket Amazon S3. Per ulteriori informazioni,

consulta [Come creare una policy del ciclo di vita per un bucket S3](#) nella Guida per l'utente Amazon Simple Storage Service.

- m. Compliance Type (Tipo di conformità): (facoltativo) specificare il tipo di conformità da utilizzare per il reporting delle informazioni di conformità. Il tipo di conformità predefinito è. Custom:DSC Se si creano più associazioni che eseguono i file MOF, assicurarsi di specificare un tipo di conformità diverso per ogni associazione. In caso contrario, ogni associazione aggiuntiva utilizzata Custom:DSC sovrascrive i dati di conformità esistenti.
 - n. Pre Reboot Script (Script di pre-riavvio): (facoltativo) specificare uno script da eseguire se la configurazione ha indicato la necessità di un riavvio. Lo script viene eseguito prima del riavvio. Lo script deve essere una singola riga. Separare le righe aggiuntive utilizzando il punto e virgola.
7. Nella sezione Destinazioni, scegli Specifica di tag o Selezione manuale delle istanze. Se si sceglie di definire le risorse come target mediante i tag, immettere una chiave e un valore del tag nei campi disponibili. Per ulteriori informazioni sull'utilizzo di target, consultare [Comprendere gli obiettivi e i controlli delle tariffe in State Manager associazioni](#).
8. Nella sezione Specify schedule (Specifica pianificazione), scegliere On Schedule (Conforme a pianificazione) oppure No schedule (Nessuna pianificazione). Se si sceglie Pianificato, utilizzare i pulsanti disponibili per creare una pianificazione Cron o della frequenza per l'associazione.
9. Nella sezione Opzioni avanzate:
- In Gravità conformità, scegli un livello di gravità per l'associazione. Il report di conformità indica se l'associazione è conforme o non conforme e il livello di gravità specificato qui. Per ulteriori informazioni, consulta [Informazioni State Manager conformità delle associazioni](#).
10. Nella sezione Controllo velocità, configurare le opzioni per l'esecuzione delle associazioni di State Manager in tutto il parco istanze di nodi gestiti. Per ulteriori informazioni su queste opzioni, consulta [Comprendere gli obiettivi e i controlli delle tariffe in State Manager associazioni](#).

Nella sezione Simultaneità, scegli un'opzione:

- Scegli destinazioni per immettere il numero assoluto di destinazioni che possono eseguire contemporaneamente l'associazione.
- Scegli percentuale per immettere la percentuale del set di destinazione che può eseguire contemporaneamente l'associazione.

Nella sezione Soglia di errore. scegli un'opzione:

- Scegliere errors (errori) per immettere il numero assoluto di errori consentiti prima che State Manager arresti l'esecuzione delle associazioni su altri target.
 - Scegliere percentage (percentuale) per immettere una percentuale di errori consentiti prima che State Manager arresti l'esecuzione delle associazioni su altri target.
11. (Facoltativo) In Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Abilita scrittura in S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

 Note

Le autorizzazioni S3 che consentono di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza assegnate al nodo gestito e non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova in un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato all'istanza disponga delle autorizzazioni necessarie per scrivere su quel bucket.

12. Scegli Crea associazione.

State Manager crea ed esegue immediatamente l'associazione sui nodi o sulle destinazioni specificate. Dopo l'esecuzione iniziale, l'associazione viene eseguita a intervalli in base alla pianificazione definita e in base alle regole seguenti:

- State Manager esegue associazioni sui nodi che sono online quando inizia l'intervallo e salta i nodi non in linea.
- State Manager tenta di eseguire l'associazione su tutti i nodi configurati durante un intervallo.
- Se un'associazione non viene eseguita durante un intervallo (ad esempio, perché un valore di simultaneità ha limitato il numero di nodi che possono elaborare l'associazione contemporaneamente), State Manager tenta di eseguire l'associazione nell'intervallo successivo.
- State Manager registra la cronologia per tutti gli intervalli ignorati. È possibile visualizzare la cronologia nella scheda Cronologia di esecuzione.

 Note

L'AWS-ApplyDSCMofs è un documento Command di Systems Manager. Ciò significa che è anche possibile eseguire questo documento utilizzando Run Command. Per ulteriori informazioni, consulta [AWS Systems Manager Run Command](#).

Risoluzione dei problemi relativi alla creazione di associazioni che eseguono file MOF

Questa sezione include informazioni utili per la risoluzione dei problemi di creazione delle associazioni che eseguono file MOF.

Attiva la registrazione migliorata

Come primo passo per la risoluzione dei problemi, abilita la registrazione migliorata. Nello specifico, svolgi le seguenti operazioni:

1. Verifica che l'associazione sia configurata per scrivere l'output dei comandi su Amazon S3 o Amazon CloudWatch Logs ()CloudWatch.
2. Imposta il parametro Abilita registrazione dettagliata su True.
3. Imposta il parametro Abilita registrazione di debug su True.

Quando abiliti la registrazione dettagliata e di debug, il file di output Stdout include informazioni sull'esecuzione dello script. Questo file di output può aiutarti a identificare gli esiti negativi dello script. Il file di output Stderr contiene gli errori che si sono verificati durante l'esecuzione di uno script.

Problemi comuni nella creazione di associazioni che eseguono file MOF

Questa sezione include informazioni sui problemi comuni che possono verificarsi durante la creazione di associazioni in grado di eseguire i file MOF e la procedura per risolvere questi problemi.

Il file MOF non è stato applicato

Se State Manager non riesce ad applicare l'associazione ai nodi, inizia a esaminare il file di output Stderr. Questo file può aiutarti a comprendere la causa principale del problema. Inoltre, verifica quanto segue:

- Il nodo dispone delle autorizzazioni di accesso richieste a tutti i bucket MOF-related Amazon S3. Nello specifico:

- s3: GetObject autorizzazioni: sono necessarie per i file MOF nei bucket Amazon S3 privati e per i moduli personalizzati nei bucket Amazon S3.
- s3: PutObject autorizzazione: necessaria per scrivere report di conformità e stato di conformità nei bucket Amazon S3.
- Se stai usando i tag, assicurati che il nodo abbia la policy IAM richiesta. L'utilizzo di tag richiede che il ruolo IAM dell'istanza abbia una policy che consenta le operazioni `ec2:DescribeInstances` e `ssm:ListTagsForResource`.
- Assicurati che al nodo siano assegnati i tag o i parametri SSM previsti.
- Assicurati che i tag o i parametri SSM non siano scritti in modo errato.
- Prova ad applicare il file MOF localmente sul nodo per assicurarti che non vi sia un problema con il file MOF.

Sembrava che il file MOF avesse esito negativo, ma l'esecuzione di Systems Manager è andata a buon fine

Se il documento `AWS-ApplyDSCTMofs` è stato eseguito correttamente, lo stato dell'esecuzione di Systems Manager risulta Success (Riuscito). Questo stato non riflette lo stato di conformità del nodo in rapporto ai requisiti di configurazione nel file MOF. Per visualizzare lo stato di conformità dei nodi, visualizza i report di conformità. È possibile visualizzare un report JSON nel bucket per i report di Amazon S3. Questo si applica alle esecuzioni di Run Command e State Manager. Inoltre, per State Manager è possibile visualizzare i dettagli di conformità nella pagina Conformità di Systems Manager.

Stati Stderr: errore di risoluzione del nome durante il raggiungimento del servizio

Questo errore indica che lo script non è in grado di raggiungere un servizio remoto. Molto probabilmente lo script non è in grado di raggiungere Amazon S3. Questo problema si verifica il più delle volte quando lo script tenta di scrivere i report di conformità o lo stato di conformità nel bucket Amazon S3 fornito nei parametri del documento. In genere, questo errore si verifica quando un ambiente di elaborazione utilizza un firewall o un proxy trasparente che include una lista dei permessi. Per risolvere il problema:

- Usa la sintassi del Region-specific bucket per tutti i parametri del bucket Amazon S3. Ad esempio, il parametro Mofs to Apply (MOF da applicare) deve avere il seguente formato:

```
s3::: .mof. bucket-region amzn-s3-demo-bucket mof-file-name
```

Ecco un esempio: `s3:us-west-2:amzn-s3-demo-bucket:my-mof.mof`

I nomi di report, stato e bucket dell'origine del modulo devono avere il seguente formato.

bucket-regionamzn-s3-demo-bucket:. Ecco un esempio: `us-west-1:amzn-s3-demo-bucket`;

- Se la Region-specific sintassi non risolve il problema, assicurati che i nodi interessati possano accedere ad Amazon S3 nella regione desiderata. Per verificare ciò:
 1. Trova il nome dell'endpoint per Amazon S3 nella regione Amazon S3 appropriata. Per ulteriori informazioni, consulta [service endpoints](#) (Endpoint del servizio della console) nei Riferimenti generali di Amazon Web Services.
 2. Accedi al nodo di destinazione ed esegui il seguente comando ping.

```
ping s3.s3-region.amazonaws.com
```

Se il ping non è riuscito, significa che Amazon S3 è inattivo o che un firewall/transparent proxy sta bloccando l'accesso alla regione Amazon S3 o che il nodo non può accedere a Internet.

Visualizzazione dei dettagli di conformità delle risorse DSC

Systems Manager acquisisce informazioni relative alla conformità sugli errori delle risorse DSC nello Status Bucket (bucket dello stato) di Amazon S3 specificato quando è stato eseguito il documento `AWS-ApplyDSCMofs`. La ricerca di informazioni sugli errori delle risorse DSC in un bucket Amazon S3 può essere dispendiosa in termini di tempo. È invece possibile visualizzare queste informazioni nella pagina Compliance (Conformità) di Systems Manager.

Nella sezione Riepilogo risorse di conformità è visualizzato il conteggio delle risorse non riuscite. Nell'esempio seguente, la risorsa `ComplianceType is Custom:DSC` e one non sono conformi.

Note

`Custom:DSC` è il `ComplianceType` valore predefinito nel documento. `AWS-ApplyDSCMofs` Il valore è personalizzabile.

Compliance resources summary

Compliance type	Compliant resources	Non-Compliant resources	Critical resources	High resources	Medium resources	Low resources	Informational resources	Unspecified resources
Custom:DSC	0	1	1	0	0	0	0	0

La sezione Panoramica dei dettagli per le risorse mostra le informazioni sulla AWS risorsa con la risorsa DSC non conforme. Questa sezione include inoltre il nome MOF, le fasi dell'esecuzione dello script e (se applicabile) un link View output (Visualizza output) per visualizzare informazioni dettagliate sullo stato.

Details overview for resources

ID	Resource type	Compliance type	Overall severity	Overall status	Execution time
i-0462a3207a1b63e72	ManagedInstance	Custom:DSC	Critical	Non-compliant	Mon, 20 May 2019 23:50:18 GMT

Compliance rule

Q: All Non-compliant

Status: Equal : Non-compliant ComplianceType: Equal : Custom:DSC Severity: Equal : All ResourceId: Equal : i-0462a3207a1b63e72

ID	Compliance type	Resource ID	Severity	Status	Execution time	Detailed status
[Mof]FailingConfig	Custom:DSC	i-0462a3207a1b63e72	Critical	Non-compliant	Mon, 20 May 2019 23:50:18 GMT	-
[FailingConfig]	Custom:DSC	i-0462a3207a1b63e72	Medium	Non-compliant	Mon, 20 May 2019 23:50:18 GMT	View output
[Script]EACContinueFailure	Custom:DSC	i-0462a3207a1b63e72	Critical	Non-compliant	Mon, 20 May 2019 23:50:18 GMT	View output

Il link Visualizzazione dell'output mostra gli ultimi 4.000 caratteri dello stato dettagliato. Systems Manager inizia con l'eccezione come primo elemento, quindi esegue un'analisi a ritroso nei messaggi dettagliati e aggiunge caratteri come prefisso fino a raggiungere la quota 4.000. Questo processo mostra i messaggi di log generati prima dell'eccezione ovvero i messaggi più rilevanti per la risoluzione dei problemi.

View detailed status

```
[2019-05-20 23:50:16.587] LCM: [ Start Set ]
[2019-05-20 23:50:16.599] Performing the operation "Set-TargetResource" on target "Executing the SetSc
[2019-05-20 23:50:16.607] WARNING: This resource should fail
[2019-05-20 23:50:16.611] This is verbose message '1' from the SetScript scriptblock
[2019-05-20 23:50:16.612] This is verbose message '2' from the SetScript scriptblock
[2019-05-20 23:50:16.613] This is verbose message '3' from the SetScript scriptblock
[2019-05-20 23:50:16.614] This is verbose message '4' from the SetScript scriptblock
[2019-05-20 23:50:16.616] This is verbose message '5' from the SetScript scriptblock
[2019-05-20 23:50:16.617] This is verbose message '6' from the SetScript scriptblock
[2019-05-20 23:50:16.618] This is verbose message '7' from the SetScript scriptblock
[2019-05-20 23:50:16.619] This is verbose message '8' from the SetScript scriptblock
[2019-05-20 23:50:16.620] This is verbose message '9' from the SetScript scriptblock
[2019-05-20 23:50:16.621] This is verbose message '10' from the SetScript scriptblock
[2019-05-20 23:50:16.649] LCM: [ End Set ] in 0.0510 seconds.
ERROR: Microsoft.Management.Infrastructure.Internal.CimException: PowerShell DSC resource MSFT_ScriptResource
at Microsoft.Management.Infrastructure.Internal.Operations.CimAsyncObserverProxyBase`1.ProcessNative
```

Per informazioni su come visualizzare le informazioni di conformità, consulta [AWS Systems Manager Conformità](#).

Situazioni che influiscono sulla creazione di report sulla conformità

Se l'associazione State Manager ha esito negativo, non viene creato alcun report sui dati di conformità. Più precisamente, se l'elaborazione di un MOF non riesce, Systems Manager non crea report sui problemi di conformità, in quanto le associazioni hanno esito negativo. Ad esempio, se Systems Manager tenta di scaricare un MOF da un bucket Amazon S3 per il cui accesso il nodo non dispone di autorizzazione, l'associazione ha esito negativo e non viene creato alcun report sui dati di conformità.

Se una risorsa in un secondo MOF ha esito negativo, Systems Manager invece crea un report sui dati di conformità. Ad esempio, se un MOF tenta di creare un file su un'unità che non esiste, Systems Manager segnala la conformità perché il `AWS-ApplyDSCMofs` documento può essere elaborato completamente, il che significa che l'associazione viene eseguita correttamente.

Creazione di associazioni che funzionano Ansible playbook

È possibile creare associazioni State Manager che eseguono playbook Ansible utilizzando il documento `SSM AWS-ApplyAnsiblePlaybooks`. State Manager è uno strumento di AWS Systems Manager. Questo documento offre i seguenti vantaggi per l'esecuzione di playbook:

- Supporto per l'esecuzione di playbook complessi
- Supporto per il download di playbook da GitHub e Amazon Simple Storage Service (Amazon S3)
- Supporto per la struttura di playbook compressa
- Registrazione migliorata
- Possibilità di specificare quale playbook eseguire quando i playbook sono raggruppati

Note

Systems Manager include due documenti SSM che consentono di creare associazioni State Manager che eseguono playbook Ansible: `AWS-RunAnsiblePlaybook` e `AWS-ApplyAnsiblePlaybooks`. Il documento `AWS-RunAnsiblePlaybook` è obsoleto. Rimane disponibile in Systems Manager per scopi di legacy. Ti consigliamo di utilizzare il documento `AWS-ApplyAnsiblePlaybooks` come conseguenza dei miglioramenti descritti qui. Le associazioni che eseguono playbook Ansible non sono supportate in macOS.

Supporto per l'esecuzione di playbook complessi

Il documento `AWS-ApplyAnsiblePlaybooks` supporta playbook complessi, raggruppati perché copia l'intera struttura di file in una directory locale prima di eseguire il playbook principale specificato. È possibile fornire playbook di origine in file zip o in una struttura di directory. Il file Zip o la directory sono archiviabili in GitHub o Amazon S3.

Supporto per il download di playbook da GitHub

Il documento `AWS-ApplyAnsiblePlaybooks` utilizza il plugin `aws:downloadContent` per scaricare i file di playbook. I file sono archiviabili in GitHub in un singolo file o come un set combinato di file di playbook. Per scaricare contenuti da GitHub, specificare le informazioni sul repository GitHub in formato JSON. Ecco un esempio.

```
{
  "owner": "TestUser",
  "repository": "GitHubTest",
  "path": "scripts/python/test-script",
  "getOptions": "branch:master",
  "tokenInfo": "{{ssm-secure:secure-string-token}}"
}
```

Supporto per il download di playbook da Amazon S3

È possibile anche archiviare e scaricare playbook Ansible in Amazon S3 come singolo file .zip o una struttura di directory. Per scaricare contenuti da Amazon S3, specificare il percorso del file. Qui di seguito sono riportati due esempi.

Esempio 1: download di un file di playbook specifico

```
{
  "path": "https://s3.amazonaws.com/amzn-s3-demo-bucket/playbook.yml"
}
```

Esempio 2: download dei contenuti di una directory

```
{
  "path": "https://s3.amazonaws.com/amzn-s3-demo-bucket/ansible/webserver/"
}
```

 Important

Se specifichi Amazon S3, il profilo dell'istanza AWS Identity and Access Management (IAM) sui nodi gestiti deve includere le autorizzazioni per il bucket S3. Per ulteriori informazioni, consulta la pagina [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#).

Supporto per la struttura di playbook compressa

Il `AWS-ApplyAnsiblePlaybooks` documento consente di eseguire file .zip compressi nel pacchetto scaricato. Il documento verifica se i file scaricati contengono un file compresso in formato .zip. Quando viene trovato un file .zip, il documento decompone automaticamente il file e quindi esegue l'automazione Ansible specificata.

Registrazione migliorata

Il documento `AWS-ApplyAnsiblePlaybooks` include un parametro facoltativo per specificare diversi livelli di registrazione. Specifica `-v` per basso livello di dettaglio, `-vv` o `-vvv` per medio livello di dettaglio e `-vvvv` per la registrazione a livello di debug. Queste opzioni sono mappate direttamente alle opzioni di livello di dettaglio Ansible.

Possibilità di specificare quale playbook eseguire quando i playbook sono raggruppati

Il documento `AWS-ApplyAnsiblePlaybooks` include un parametro obbligatorio per specificare quale playbook eseguire quando più playbook vengono raggruppati. Questa opzione offre flessibilità per l'esecuzione di playbook per supportare diversi casi d'uso.

Comprensione delle dipendenze installate

Se si specifica `True` per il `InstallDependencies` parametro, Systems Manager verifica che nei nodi siano installate le seguenti dipendenze:

- Ubuntu Server/Debian Server: Apt-get (Gestione dei pacchetti), Python 3, Unzip Ansible
- Versioni supportate da Amazon Linux: Ansible
- RHEL: Python 3, Ansible, Unzip

Se una o più di queste dipendenze non vengono trovate, Systems Manager le installa automaticamente.

Crea un'associazione che funzioni Ansible playbook (console)

La procedura seguente descrive come utilizzare la console di Systems Manager per creare un'associazione State Manager che esegua playbook Ansible utilizzando il documento AWS-ApplyAnsiblePlaybooks.

Per creare un'associazione che funzioni Ansible playbook (console)

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli State Manager.
3. Selezionare State Manager poi Crea associazione.
4. Per Nome, specifica un nome che consente di ricordare lo scopo dell'associazione.
5. Nell'elenco Documento, scegli **AWS-ApplyAnsiblePlaybooks**.
6. Nella sezione Parametri, per Tipo di sorgente, scegli uno GitHub o S3.

GitHub

Se si sceglie GitHub, immetti le informazioni sul repository nel formato seguente.

```
{
  "owner": "user_name",
  "repository": "name",
  "path": "path_to_directory_or_playbook_to_download",
  "getOptions": "branch:branch_name",
  "tokenInfo": "{((Optional)_token_information)}"
}
```

S3

Se si sceglie S3, immetti le informazioni sul percorso nel formato seguente.

```
{
  "path": "https://s3.amazonaws.com/path_to_directory_or_playbook_to_download"
}
```

7. Per Installa dipendenze, scegli un'opzione.
8. (Facoltativo) Per File di playbook, immetti un nome file. Se il playbook è contenuto in un file Zip, specificare un percorso relativo al file Zip.

9. (Facoltativo) Per Variabili extra, immetti le variabili per l'invio da State Manager ad Ansible in fase di runtime.
10. (Facoltativo) Per Verifica, scegli un'opzione.
11. (Facoltativo) Per Modalità dettagliata, scegli un'opzione.
12. Per Destinazioni, scegli un'opzione. Per informazioni sull'utilizzo delle destinazioni, consulta [Comprendere gli obiettivi e i controlli delle tariffe in State Manager associazioni](#).
13. Nella sezione Specifica pianificazione, scegli Conforme a pianificazione o Nessuna pianificazione. Se si sceglie Conforme a pianificazione, utilizzare i pulsanti disponibili per creare una pianificazione Cron o rate per l'associazione.
14. Nella sezione Opzioni avanzate, per Gravità conformità, scegliere un livello di gravità per l'associazione. Il report di conformità indica se l'associazione è conforme o non conforme e il livello di gravità specificato qui. Per ulteriori informazioni, consulta [Informazioni State Manager conformità delle associazioni](#).
15. Nella sezione Controllo velocità, configura le opzioni per eseguire le associazioni di State Manager in tutto il parco istanze nodi gestiti. Per informazioni sull'utilizzo dei controlli di velocità, consulta [Comprendere gli obiettivi e i controlli delle tariffe in State Manager associazioni](#).

Nella sezione Simultaneità, scegli un'opzione:

- Scegli destinazioni per immettere il numero assoluto di destinazioni che possono eseguire contemporaneamente l'associazione.
- Scegli percentuale per immettere la percentuale del set di destinazione che può eseguire contemporaneamente l'associazione.

Nella sezione Soglia di errore, scegli un'opzione:

- Scegli errori per immettere il numero assoluto di errori consentiti prima che State Manager arresti l'esecuzione delle associazioni su altre destinazioni.
 - Scegli percentuale per immettere una percentuale di errori consentiti prima che State Manager arresti l'esecuzione delle associazioni su altre destinazioni.
16. (Facoltativo) In Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Abilita scrittura in S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

Note

Le autorizzazioni S3 che consentono di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza assegnate al nodo gestito e non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova in un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato all'istanza disponga delle autorizzazioni necessarie per scrivere su quel bucket.

17. Scegli Crea associazione.**Note**

Se utilizzi i tag per creare un'associazione su uno o più nodi di destinazione e quindi rimuovi i tag da un nodo, tale nodo non eseguirà più l'associazione. Il nodo viene dissociato dal documento di State Manager.

Create un'associazione che viene eseguita Ansible playbook (CLI)

La procedura seguente descrive come utilizzare AWS Command Line Interface (AWS CLI) per creare un'associazione che esegua Ansible i playbook utilizzando il documento. `AWS-ApplyAnsiblePlaybooks`

Per creare un'associazione che funzioni Ansible playbook (CLI)

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Esegui uno dei seguenti comandi per creare un'associazione che esegue playbook Ansible eseguendo il targeting dei nodi tramite tag. Sostituisci ogni *example resource placeholder* con le tue informazioni. Il comando (A) specifica GitHub come tipo di origine. Il comando (B) specifica Amazon S3 come tipo di origine.

(A) GitHub fonte

Linux & macOS

```
aws ssm create-association --name "AWS-ApplyAnsiblePlaybooks" \
  --targets Key=tag:TagKey,Values=TagValue \
  --parameters '{"SourceType":["GitHub"],"SourceInfo":
["{\"owner\": \"owner_name\", \"repository\": \"name\",
  \"getOptions\": \"branch:master\"}"],"InstallDependencies":
["True_or_False"],"PlaybookFile":["file_name.yml"],"ExtraVariables":["key/
value_pairs_separated_by_a_space"],"Check":["True_or_False"],"Verbose":["-v, -
vv, -vvv, or -vvvv"],"TimeoutSeconds":["3600"]}' \
  --association-name "name" \
  --schedule-expression "cron_or_rate_expression"
```

Windows

```
aws ssm create-association --name "AWS-ApplyAnsiblePlaybooks" ^
  --targets Key=tag:TagKey,Values=TagValue ^
  --parameters '{"SourceType":["GitHub"],"SourceInfo":
["{\"owner\": \"owner_name\", \"repository\": \"name\",
  \"getOptions\": \"branch:master\"}"],"InstallDependencies":
["True_or_False"],"PlaybookFile":["file_name.yml"],"ExtraVariables":["key/
value_pairs_separated_by_a_space"],"Check":["True_or_False"],"Verbose":["-v, -
vv, -vvv, or -vvvv"],"TimeoutSeconds":["3600"]}' ^
  --association-name "name" ^
  --schedule-expression "cron_or_rate_expression"
```

Ecco un esempio.

```
aws ssm create-association --name "AWS-ApplyAnsiblePlaybooks" \
  --targets "Key=tag:OS,Values=Linux" \
  --parameters '{"SourceType":["GitHub"],"SourceInfo":["{\"owner\":
  \"ansibleDocumentTest\", \"repository\": \"Ansible\", \"getOptions\":
  \"branch:master\"}"],"InstallDependencies":["True"],"PlaybookFile":["hello-world-
  playbook.yml"],"ExtraVariables":["SSM=True"],"Check":["False"],"Verbose":["-v"]}' \
  --association-name "AnsibleAssociation" \
  --schedule-expression "cron(0 2 ? * SUN *)"
```

(B) Origine S3

Linux & macOS

```
aws ssm create-association --name "AWS-ApplyAnsiblePlaybooks" \
  --targets Key=tag:TagKey,Values=TagValue \
  --parameters '{"SourceType":["S3"],"SourceInfo":["{"path\":"https://
s3.amazonaws.com/
path_to_zip_file,_directory,_or_playbook_to_download\"}],\"InstallDependencies\":
[\"True_or_False\"],\"PlaybookFile\":[\"file_name.yaml\"],\"ExtraVariables\":[\"key/
value_pairs_separated_by_a_space\"],\"Check\":[\"True_or_False\"],\"Verbose\":[\"-v,-
vv,-vvv, or -vvvv\"]}' \
  --association-name "name" \
  --schedule-expression "cron_or_rate_expression"
```

Windows

```
aws ssm create-association --name "AWS-ApplyAnsiblePlaybooks" ^
  --targets Key=tag:TagKey,Values=TagValue ^
  --parameters '{"SourceType":["S3"],"SourceInfo":["{"path\":"https://
s3.amazonaws.com/
path_to_zip_file,_directory,_or_playbook_to_download\"}],\"InstallDependencies\":
[\"True_or_False\"],\"PlaybookFile\":[\"file_name.yaml\"],\"ExtraVariables\":[\"key/
value_pairs_separated_by_a_space\"],\"Check\":[\"True_or_False\"],\"Verbose\":[\"-v,-
vv,-vvv, or -vvvv\"]}' ^
  --association-name "name" ^
  --schedule-expression "cron_or_rate_expression"
```

Ecco un esempio.

```
aws ssm create-association --name "AWS-ApplyAnsiblePlaybooks" \
  --targets "Key=tag:OS,Values=Linux" \
  --parameters '{"SourceType":["S3"],"SourceInfo":["{"path\":"https://
s3.amazonaws.com/amzn-s3-demo-bucket/playbook.yaml\"}],\"InstallDependencies\":
[\"True\"],\"PlaybookFile\":[\"playbook.yaml\"],\"ExtraVariables\":[\"SSM=True\"],\"Check\":
[\"False\"],\"Verbose\":[\"-v\"]}' \
  --association-name "AnsibleAssociation" \
  --schedule-expression "cron(0 2 ? * SUN *)"
```

 Note

Le associazioni di State Manager non supportano tutte le espressioni Cron e della frequenza. Per ulteriori informazioni sulla creazione di espressioni Cron e della frequenza per le associazioni, consulta [Riferimento: espressioni Cron e della frequenza per Systems Manager](#).

Il sistema tenta di creare l'associazione sui nodi e di applicare immediatamente lo stato.

3. Eseguire il comando riportato sotto per visualizzare uno stato aggiornato dell'associazione appena creata.

```
aws ssm describe-association --association-id "ID"
```

Creazione di associazioni che vengono eseguite Chef recipes

È possibile creare associazioni State Manager che eseguono ricette Chef utilizzando il documento SSM AWS-ApplyChefRecipes. State Manager è uno strumento di AWS Systems Manager. È possibile indirizzare i nodi gestiti di Linux-based Systems Manager con il documento AWS-ApplyChefRecipes SSM. Questo documento offre i seguenti vantaggi per l'esecuzione di ricette Chef:

- Supporta più versioni di Chef (da Chef 11 a Chef 18).
- Installa automaticamente il software client Chef nei nodi di destinazione.
- Facoltativamente esegue [controlli di conformità Systems Manager](#) su nodi di destinazione e memorizza i risultati dei controlli di conformità in un bucket Amazon Simple Storage Service (Amazon S3).
- Esegue più cookbook e ricette in un'unica esecuzione del documento.
- Facoltativamente esegue le ricette in modalità `why-run`, per mostrare quali ricette cambieranno nei nodi di destinazione senza apportare modifiche.
- Facoltativamente applica attributi JSON personalizzati alle esecuzioni `chef-client`.
- Facoltativamente, applica attributi JSON personalizzati da un file di origine archiviato in una posizione specificata dall'utente.

È possibile utilizzare i bucket [Git](#), [GitHub](#), [HTTP](#), o [Amazon S3](#) come origini di download per i cookbook e le ricette Chef specificate in un documento AWS-ApplyChefRecipes.

Note

Le associazioni che eseguono ricette Chef non sono supportate su macOS.

Nozioni di base

Prima di creare un documento AWS-ApplyChefRecipes, prepara i cookbook Chef e il relativo repository. Se non hai già un Chef ricettario da usare, puoi iniziare usando un HelloWorld ricettario di prova che AWS ha preparato per te. Il documento AWS-ApplyChefRecipes punta già a questo cookbook per impostazione predefinita. I tuoi cookbook dovrebbero essere impostati in modo simile alla seguente struttura di directory. Nell'esempio seguente, jenkins e nginx sono esempi di cookbook Chef disponibili su [Chef Supermarket](#) sul sito web Chef.

Sebbene non sia AWS possibile supportare ufficialmente i libri di cucina sul [Chef Supermarket](#) sito Web, molti di essi funzionano con il documento. AWS-ApplyChefRecipes Di seguito sono riportati esempi di criteri per stabilire quando si sta testando un cookbook della community:

- Il ricettario dovrebbe supportare i sistemi Linux-based operativi dei nodi gestiti di Systems Manager a cui ti rivolgi.
- Il cookbook è valido per la versione client Chef (Chef Chef 11 a Chef 18) che utilizzi.
- Il cookbook è compatibile con Chef Infra Client e non richiede un server Chef.

Verifica di avere la possibilità di accedere al sito web Chef .io, in modo che tutti i cookbook specificati nell'elenco di esecuzione siano installati quando viene eseguito il documento di Systems Manager (documento SSM). L'utilizzo di una cartella cookbooks nidificata è supportato, ma non obbligatorio; è possibile memorizzare i cookbook direttamente sotto il livello radice.

```
<Top-level directory, or the top level of the archive file (ZIP or tgz or tar.gz)>
  ### cookbooks (optional level)
    ### jenkins
    #   ### metadata.rb
    #   ### recipes
    ### nginx
    #   ### metadata.rb
    #   ### recipes
```

⚠ Important

Prima di creare un'associazione State Manager che esegua ricette Chef, è necessario tenere presente che l'esecuzione del documento installa il software client Chef nei nodi gestiti di Systems Manager, a meno che non si imposti i valori della versione client Chef a None. Questa operazione utilizza uno script di installazione Chef per installare i componenti Chef per conto dell'utente. Prima di eseguire un documento AWS-ApplyChefRecipes, assicurati che l'azienda sia in grado di soddisfare tutti i requisiti legali applicabili, incluse le condizioni di licenza applicabili all'uso del software Chef. Per ulteriori informazioni, consulta il [sito web Chef](#).

Systems Manager può fornire report di conformità a un bucket S3, alla console di Systems Manager o rendere disponibili i risultati di conformità in risposta ai comandi dell'API Systems Manager. Per eseguire report di conformità di Systems Manager, il profilo dell'istanza collegato con i nodi Systems Manager gestiti deve disporre delle autorizzazioni per scrivere nel bucket S3. Il profilo dell'istanza deve disporre delle autorizzazioni per utilizzare l'API PutComplianceItem Systems Manager. Per ulteriori informazioni sulla conformità di Systems Manager, consultare [AWS Systems Manager Conformità](#).

Registrazione dell'esecuzione del documento

Quando esegui un documento Systems Manager (documento SSM) utilizzando un'associazione State Manager, puoi configurare l'associazione per scegliere l'output dell'esecuzione del documento e puoi inviare l'output ad Amazon S3 o CloudWatch Amazon Logs (LogsCloudWatch). Per facilitare la risoluzione dei problemi al termine dell'esecuzione di un'associazione, verifica che l'associazione sia configurata per scrivere l'output dei comandi su un bucket Amazon S3 o su LogsCloudWatch. Per ulteriori informazioni, consulta [Utilizzo delle associazioni in Systems Manager](#).

Applicazione degli attributi JSON alle destinazioni durante l'esecuzione di una ricetta

È possibile specificare gli attributi JSON che il client Chef applica ai nodi di destinazione durante l'esecuzione di un'associazione. Durante la configurazione dell'associazione, è possibile fornire un formato JSON non elaborato o specificare il percorso di un file JSON archiviato in Amazon S3.

Usa gli attributi JSON quando desideri personalizzare il modo in cui viene eseguita la ricetta senza dover modificare la ricetta stessa, ad esempio:

- Sovrascrivere un numero limitato di attributi

Utilizza un formato JSON personalizzato per evitare di dover mantenere più versioni di una ricetta per adattarla a piccole differenze.

- Fornire valori variabili

Usa un formato JSON personalizzato per specificare valori che possono cambiare da un'esecuzione all'altra. Ad esempio, se i cookbook Chef configurano un'applicazione di terze parti che accetta pagamenti, è possibile utilizzare un formato JSON personalizzato per specificare l'URL dell'endpoint di pagamento.

Definizione degli attributi in formato JSON non elaborato

Di seguito è riportato un esempio del formato da utilizzare per specificare attributi JSON personalizzati per la ricetta Chef.

```
{"filepath":"/tmp/example.txt", "content":"Hello, World!"}
```

Definizione di un percorso per un file JSON

Di seguito è riportato un esempio del formato da utilizzare per specificare il percorso degli attributi JSON personalizzati per la ricetta Chef.

```
{"sourceType":"s3", "sourceInfo":"someS3URL1"}, {"sourceType":"s3",  
"sourceInfo":"someS3URL2"}
```

Utilizzo di Git come origine di un cookbook

Il documento AWS-ApplyChefRecipes utilizza il plug-in [aws:downloadContent](#) per scaricare cookbook Chef. Per scaricare contenuti da Git, specifica le informazioni sul repository Git in formato JSON come nel seguente esempio. Sostituisci ogni *example-resource-placeholder* con le tue informazioni.

```
{  
  "repository":"GitCookbookRepository",  
  "privateSSHKey":"{{ssm-secure:ssh-key-secure-string-parameter}}",  
  "skipHostKeyChecking":"false",  
  "getOptions":"branch:refs/head/main",  
  "username":"{{ssm-secure:username-secure-string-parameter}}",  
  "password":"{{ssm-secure:password-secure-string-parameter}}"  
}
```

Utilizzo GitHub come fonte di libri di cucina

Il documento AWS-ApplyChefRecipes utilizza il plug-in [aws:downloadContent](#) per scaricare cookbook. Per scaricare contenuti da GitHub, specifica le informazioni sul repository GitHub in formato JSON come nel seguente esempio. Sostituisci ogni *example-resource-placeholder* con le tue informazioni.

```
{
  "owner": "TestUser",
  "repository": "GitHubCookbookRepository",
  "path": "cookbooks/HelloWorld",
  "getOptions": "branch:refs/head/main",
  "tokenInfo": "{{ssm-secure:token-secure-string-parameter}}"
}
```

Utilizzo di HTTP come origine di un cookbook

È possibile archiviare i cookbook Chef in una posizione HTTP personalizzata come singolo file .zip o tar.gz oppure come struttura di directory. Per scaricare contenuti da HTTP, specifica il percorso del file o della directory in formato JSON, come nell'esempio seguente. Sostituisci ogni *example-resource-placeholder* con le tue informazioni.

```
{
  "url": "https://my.website.com/chef-cookbooks/HelloWorld.zip",
  "allowInsecureDownload": "false",
  "authMethod": "Basic",
  "username": "{{ssm-secure:username-secure-string-parameter}}",
  "password": "{{ssm-secure:password-secure-string-parameter}}"
}
```

Utilizzo di Amazon S3 come fonte di cookbook

È possibile anche archiviare e scaricare i cookbook Chef in Amazon S3 come singolo file .zip o tar.gz oppure come struttura di directory. Per scaricare contenuti da Amazon S3, specifica il percorso del file in formato JSON, come negli esempi seguenti. Sostituisci ogni *example-resource-placeholder* con le tue informazioni.

Esempio 1: Scaricare un cookbook

```
{
```

```
{  
  "path": "https://s3.amazonaws.com/chef-cookbooks/HelloWorld.zip"  
}
```

Esempio 2: download dei contenuti di una directory

```
{  
  "path": "https://s3.amazonaws.com/chef-cookbooks-test/HelloWorld"  
}
```

Important

Se specifichi Amazon S3, il profilo dell'istanza AWS Identity and Access Management (IAM) sui nodi gestiti deve essere configurato con la AmazonS3ReadOnlyAccess policy. Per ulteriori informazioni, consulta la pagina [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#).

Crea un'associazione che funzioni Chef ricette (console)

La procedura seguente descrive come utilizzare la console di Systems Manager per creare un'associazione State Manager che esegua i cookbook Chef utilizzando il documento AWS-ApplyChefRecipes.

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli State Manager.
3. Selezionare State Manager poi Crea associazione.
4. Per Name (Nome), specificare un nome che consente di ricordare lo scopo dell'associazione.
5. Nell'elenco Document (Documento) scegliere **AWS-ApplyChefRecipes**.
6. In Parametri, per Tipo di origine, seleziona Git, GitHub, HTTP, oppure S3.
7. Per informazioni origine, inserisci le informazioni sull'origine del cookbook utilizzando il formato appropriato per Tipo di origine selezionato nel passaggio 6. Per ulteriori informazioni, consulta i seguenti argomenti:
 - [the section called “Utilizzo di Git come origine di un cookbook”](#)
 - [the section called “Utilizzo GitHub come fonte di libri di cucina”](#)
 - [the section called “Utilizzo di HTTP come origine di un cookbook”](#)

- [the section called “Utilizzo di Amazon S3 come fonte di cookbook”](#)
8. In Esegui elenco, elencare le ricette che si desidera eseguire nel formato seguente, separando ogni ricetta con una virgola come mostrato. Non includere uno spazio dopo la virgola. Sostituisci ogni *example-resource-placeholder* con le tue informazioni.
- ```
recipe[cookbook-name1::recipe-name],recipe[cookbook-name2::recipe-name]
```
9. (Facoltativo) Specifica gli attributi JSON personalizzati che desideri che il client Chef passi ai nodi di destinazione.
- a. In Contenuto degli attributi JSON, aggiungi qualsiasi attributo che desideri che il client Chef passi ai nodi di destinazione.
  - b. In Origini degli attributi JSON, aggiungi i percorsi degli attributi che desideri che il client Chef passi ai nodi di destinazione.

Per ulteriori informazioni, consulta [the section called “Applicazione degli attributi JSON alle destinazioni durante l'esecuzione di una ricetta”](#).

10. Per la versione client Chef, specificare una versione Chef. I valori validi sono compresi tra 11 e 18 o None. Se si specifica un numero compreso tra 11 e 18 (incluso), Systems Manager installa la versione client Chef corretta nei nodi di destinazione. Se si specifica None, Systems Manager non installa il client Chef nei nodi di destinazione prima di eseguire le ricette del documento.
11. (Facoltativo) In Argomenti del client Chef, specificare argomenti aggiuntivi supportati per la versione di Chef utilizzata. Per ulteriori informazioni sugli argomenti supportati, eseguire `chef-client -h` su un nodo che esegue il client Chef.
12. (Facoltativo) Why-runAttivala per mostrare le modifiche apportate ai nodi di destinazione se le ricette vengono eseguite, senza modificare effettivamente i nodi di destinazione.
13. In Gravità della conformità, scegliere la gravità dei risultati della conformità di Systems Manager che si desidera segnalare. Il report di conformità indica se l'associazione è conforme o non conforme e il livello di gravità specificato qui. I report di conformità vengono archiviati in un bucket S3 specificato come valore del parametro Compliance report bucket (bucket del report di conformità) (passaggio 14). Per ulteriori informazioni sulla conformità, consultare [Scopri i dettagli sulla conformità](#) in questa guida.

Le scansioni di conformità misurano la differenza tra la configurazione specificata nelle ricette Chef e le risorse di nodo. I valori validi sono Critical, High, Medium, Low, Informational, Unspecified o None. Per ignorare la segnalazione di conformità, scegliere None.

14. Per Tipo di conformità, specificare il tipo di conformità per il quale si desidera segnalare i risultati. I valori validi sono Association per State Manager le associazioni, o Custom: *custom-type*. Il valore predefinito è Custom: Chef.
15. Per Bucket del report di conformità, immettere il nome di un bucket S3 in cui memorizzare le informazioni su ogni esecuzione Chef effettuata da questo documento, inclusi i risultati della configurazione delle risorse e della conformità.
16. Nella sezione Controllo velocità, configurare le opzioni per eseguire le associazioni di State Manager in tutto il parco istanze nodi gestiti. Per informazioni sull'utilizzo dei controlli di velocità, consulta [Comprendere gli obiettivi e i controlli delle tariffe in State Manager associazioni](#).

In Convaluta, scegli un'opzione:

- Scegli destinazioni per immettere il numero assoluto di destinazioni che possono eseguire contemporaneamente l'associazione.
- Scegli percentuale per immettere la percentuale del set di destinazione che può eseguire contemporaneamente l'associazione.

In Soglia di errore, scegli un'opzione:

- Scegli errori per immettere il numero assoluto di errori consentiti prima che State Manager arresti l'esecuzione delle associazioni su altre destinazioni.
  - Scegli percentuale per immettere una percentuale di errori consentiti prima che State Manager arresti l'esecuzione delle associazioni su altre destinazioni.
17. (Facoltativo) In Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Abilita scrittura in S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

#### Note

Le autorizzazioni S3 che consentono di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza assegnate al nodo gestito e non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova in un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato all'istanza disponga delle autorizzazioni necessarie per scrivere su quel bucket.

## 18. Scegli Crea associazione.

Crea un'associazione che venga eseguita Chef ricette (CLI)

La procedura seguente descrive come utilizzare AWS Command Line Interface (AWS CLI) per creare un'associazione che esegua i libri di cucina Chef utilizzando il AWS-ApplyChefRecipes documento.

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Esegui uno dei seguenti comandi per creare un'associazione che esegue cookbook Chef sui nodi di destinazione che presentano i tag specificati. Usa il comando appropriato per il tipo di origine del cookbook e il sistema operativo. Sostituisci ogni *example-resource-placeholder* con le tue informazioni.

### a. Origine Git

Linux & macOS

```
aws ssm create-association --name "AWS-ApplyChefRecipes" \
 --targets Key=tag:TagKey,Values=TagValue \
 --parameters '{"SourceType":["Git"],"SourceInfo":["{"repository\":"
 "\"repository-name\"\", \"getOptions\":" \"branch:branch-name\"\", \"username
 \": \"{{ ssm-secure:username-secure-string-parameter }}\"\", \"password\":"
 \"{{ ssm-secure:password-secure-string-parameter }}\"\"}], \"RunList\":
 [\"{\\\"recipe[cookbook-name-1::recipe-name]\\\", \\\"recipe[cookbook-
 name-2::recipe-name]\\\"}], \"JsonAttributesContent\": [\"{custom-json-
 content}\"], \"JsonAttributesSources\": \"{\\\"sourceType\\\":\\\"s3\\\", \\\"sourceInfo
 \":\\\"s3-bucket-endpoint-1\\\"\", {\\\"sourceType\\\":\\\"s3\\\", \\\"sourceInfo\\\":
 \\\"s3-bucket-endpoint-2\\\"\"\", \"ChefClientVersion\": [\"version-number\"],
 \"ChefClientArguments\": [\"chef-client-arguments\"], \"WhyRun\": boolean,
 \"ComplianceSeverity\": [\"severity-value\"], \"ComplianceType\":
 [\"Custom:Chef\"], \"ComplianceReportBucket\": [\"s3-bucket-name\"]}' \
 --association-name \"name\" \
 --schedule-expression \"cron-or-rate-expression\"
```

## Windows

```
aws ssm create-association --name "AWS-ApplyChefRecipes" ^
 --targets Key=tag:TagKey,Values=TagValue ^
 --parameters '{"SourceType":["Git"],"SourceInfo":["{"repository\":"
 \repository-name\\", \"getOptions\": \"branch:branch-name\\", \"username
 \": \"{{ ssm-secure:username-secure-string-parameter }}\\", \"password\":
 \"{{ ssm-secure:password-secure-string-parameter }}\\"]\", \"RunList\":
 [\"{\\\"recipe[cookbook-name-1::recipe-name]\\\", \"recipe[cookbook-
 name-2::recipe-name]\\\"}], \"JsonAttributesContent\": [\"{custom-json}\"],
 \"JsonAttributesSources\": [\"{\\\"sourceType\\\":\\\"s3\\\", \"sourceInfo\\\":
 \\\"s3-bucket-endpoint-1\\\", {\\\"sourceType\\\":\\\"s3\\\", \"sourceInfo\\\":
 \\\"s3-bucket-endpoint-2\\\"}], \"ChefClientVersion\": [\"version-number\"],
 \"ChefClientArguments\": [\"{chef-client-arguments}\"], \"WhyRun\": boolean,
 \"ComplianceSeverity\": [\"severity-value\"], \"ComplianceType\":
 [\"Custom:Chef\"], \"ComplianceReportBucket\": [\"s3-bucket-name]\"}' ^
 --association-name "name" ^
 --schedule-expression "cron-or-rate-expression"
```

### b. GitHub source (origine)

## Linux & macOS

```
aws ssm create-association --name "AWS-ApplyChefRecipes" \
 --targets Key=tag:TagKey,Values=TagValue \
 --parameters '{"SourceType":["GitHub"],"SourceInfo":["{"owner\":"
 \owner-name\\", \"repository\":" \name\\", \"path\":" \path-to-directory-
 or-cookbook-to-download\\", \"getOptions\":" \"branch:branch-name\\"]\",
 \"RunList\": [\"{\\\"recipe[cookbook-name-1::recipe-name]\\\", \"recipe[cookbook-
 name-2::recipe-name]\\\"}], \"JsonAttributesContent\": [\"{custom-json}\"],
 \"ChefClientVersion\": [\"version-number\"], \"ChefClientArguments\": [\"{chef-
 client-arguments}\"], \"WhyRun\": boolean, \"ComplianceSeverity\": [\"severity-
 value\"], \"ComplianceType\": [\"Custom:Chef\"], \"ComplianceReportBucket\": [\"s3-
 bucket-name]\"}' \
 --association-name "name" \
 --schedule-expression "cron-or-rate-expression"
```

## Windows

```
aws ssm create-association --name "AWS-ApplyChefRecipes" ^
 --targets Key=tag:TagKey,Values=TagValue \
```

```
--parameters '{"SourceType":["GitHub"],"SourceInfo":["{\\"owner\\":
\\"owner-name\\", \\"repository\\": \\"name\\", \\"path\\": \\"path-to-directory-
or-cookbook-to-download\\", \\"getOptions\\": \\"branch:branch-name\\"}"],
"RunList":["{\\"recipe[cookbook-name-1::recipe-name]\\", \\"recipe[cookbook-
name-2::recipe-name]\\"}"], "JsonAttributesContent": [{"custom-json}],
"ChefClientVersion": ["version-number"], "ChefClientArguments":["{chef-
client-arguments}], "WhyRun": boolean, "ComplianceSeverity": ["severity-
value"], "ComplianceType": ["Custom:Chef"], "ComplianceReportBucket": ["s3-
bucket-name"]}' ^
--association-name "name" ^
--schedule-expression "cron-or-rate-expression"
```

Ecco un esempio.

## Linux & macOS

```
aws ssm create-association --name "AWS-ApplyChefRecipes" \
 --targets Key=tag:OS,Values=Linux \
 --parameters '{"SourceType":["GitHub"],"SourceInfo":["{\\"owner
\\":\\"ChefRecipeTest\\", \\"repository\\": \\"ChefCookbooks\\", \\"path
\\": \\"cookbooks/HelloWorld\\", \\"getOptions\\": \\"branch:master
\\"}"], "RunList":["{\\"recipe[HelloWorld::HelloWorldRecipe]\\",
\\"recipe[HelloWorld::InstallApp]\\"}"], "JsonAttributesContent":
[{"\\"state\\": \\"visible\\",\\"colors\\": {\\"foreground\\": \\"light-blue
\\",\\"background\\": \\"dark-gray\\"}}"], "ChefClientVersion": ["14"],
"ChefClientArguments":["{--fips}], "WhyRun": false, "ComplianceSeverity":
["Medium"], "ComplianceType": ["Custom:Chef"], "ComplianceReportBucket":
["ChefComplianceResultsBucket"]}' \
 --association-name "MyChefAssociation" \
 --schedule-expression "cron(0 2 ? * SUN *)"
```

## Windows

```
aws ssm create-association --name "AWS-ApplyChefRecipes" ^
 --targets Key=tag:OS,Values=Linux ^
 --parameters '{"SourceType":["GitHub"],"SourceInfo":["{\\"owner
\\":\\"ChefRecipeTest\\", \\"repository\\": \\"ChefCookbooks\\", \\"path
\\": \\"cookbooks/HelloWorld\\", \\"getOptions\\": \\"branch:master
\\"}"], "RunList":["{\\"recipe[HelloWorld::HelloWorldRecipe]\\",
\\"recipe[HelloWorld::InstallApp]\\"}"], "JsonAttributesContent":
[{"\\"state\\": \\"visible\\",\\"colors\\": {\\"foreground\\": \\"light-blue
\\",\\"background\\": \\"dark-gray\\"}}"], "ChefClientVersion": ["14"],
```

```
"ChefClientArguments":["{--fips}"], "WhyRun": false, "ComplianceSeverity":
["Medium"], "ComplianceType": ["Custom:Chef"], "ComplianceReportBucket":
["ChefComplianceResultsBucket"]}' ^
--association-name "MyChefAssociation" ^
--schedule-expression "cron(0 2 ? * SUN *)"
```

### c. Origine HTTP

#### Linux & macOS

```
aws ssm create-association --name "AWS-ApplyChefRecipes" \
--targets Key=tag:TagKey,Values=TagValue \
--parameters '{"SourceType":["HTTP"],"SourceInfo":["{"url":"url-
to-zip-file/directory/cookbook", "authMethod": "auth-method",
"username": "{ ssm-secure:username-secure-string-parameter }",
"password": "{ ssm-secure:password-secure-string-parameter }"}"],
"RunList":["{"recipe[cookbook-name-1::recipe-name]", "recipe[cookbook-
name-2::recipe-name]"}"], "JsonAttributesContent": [{"custom-json-
content}"], "JsonAttributesSources": [{"sourceType":"s3", "sourceInfo
":"s3-bucket-endpoint-1"}, {"sourceType":"s3", "sourceInfo":
"s3-bucket-endpoint-2"}], "ChefClientVersion": ["version-number"],
"ChefClientArguments":["{chef-client-arguments}"], "WhyRun": boolean,
"ComplianceSeverity": ["severity-value"], "ComplianceType":
["Custom:Chef"], "ComplianceReportBucket": ["s3-bucket-name"]}' \
--association-name "name" \
--schedule-expression "cron-or-rate-expression"
```

#### Windows

```
aws ssm create-association --name "AWS-ApplyChefRecipes" ^
--targets Key=tag:TagKey,Values=TagValue ^
--parameters '{"SourceType":["HTTP"],"SourceInfo":["{"url":"url-
to-zip-file/directory/cookbook", "authMethod": "auth-method",
"username": "{ ssm-secure:username-secure-string-parameter }",
"password": "{ ssm-secure:password-secure-string-parameter }"}"],
"RunList":["{"recipe[cookbook-name-1::recipe-name]", "recipe[cookbook-
name-2::recipe-name]"}"], "JsonAttributesContent": [{"custom-json-
content}"], "JsonAttributesSources": [{"sourceType":"s3", "sourceInfo
":"s3-bucket-endpoint-1"}, {"sourceType":"s3", "sourceInfo":
"s3-bucket-endpoint-2"}], "ChefClientVersion": ["version-number"],
"ChefClientArguments":["{chef-client-arguments}"], "WhyRun": boolean,
"ComplianceSeverity": ["severity-value"], "ComplianceType":
["Custom:Chef"], "ComplianceReportBucket": ["s3-bucket-name"]}' \
```

```
--association-name "name" ^
--schedule-expression "cron-or-rate-expression"
```

#### d. Origine Amazon S3

##### Linux & macOS

```
aws ssm create-association --name "AWS-ApplyChefRecipes" \
 --targets Key=tag:TagKey,Values=TagValue \
 --parameters '{"SourceType":["S3"],"SourceInfo":["{"path\":"https://s3.amazonaws.com/path_to_zip_file_directory_or_cookbook_to_download\"}],
 "RunList":["{"recipe[cookbook_name1::recipe_name]\",
 \"recipe[cookbook_name2::recipe_name]\"}"], "JsonAttributesContent":
 [{"Custom_JSON"}], "ChefClientVersion": [version_number"],
 "ChefClientArguments":["{chef_client_arguments}"], "WhyRun": true_or_false,
 "ComplianceSeverity": [severity_value"], "ComplianceType":
 ["Custom:Chef"], "ComplianceReportBucket": ["amzn-s3-demo-bucket"]}' \
 --association-name "name" \
 --schedule-expression "cron_or_rate_expression"
```

##### Windows

```
aws ssm create-association --name "AWS-ApplyChefRecipes" ^
 --targets Key=tag:TagKey,Values=TagValue ^
 --parameters '{"SourceType":["S3"],"SourceInfo":["{"path\":"https://s3.amazonaws.com/path_to_zip_file_directory_or_cookbook_to_download\"}],
 "RunList":["{"recipe[cookbook_name1::recipe_name]\",
 \"recipe[cookbook_name2::recipe_name]\"}"], "JsonAttributesContent":
 [{"Custom_JSON"}], "ChefClientVersion": [version_number"],
 "ChefClientArguments":["{chef_client_arguments}"], "WhyRun": true_or_false,
 "ComplianceSeverity": [severity_value"], "ComplianceType":
 ["Custom:Chef"], "ComplianceReportBucket": ["amzn-s3-demo-bucket"]}' ^
 --association-name "name" ^
 --schedule-expression "cron_or_rate_expression"
```

Ecco un esempio.

##### Linux & macOS

```
aws ssm create-association --name "AWS-ApplyChefRecipes" \
 --targets "Key=tag:OS,Values= Linux" \
```

```
--parameters '{"SourceType":["S3"],"SourceInfo":["{"path
\": \"https://s3.amazonaws.com/amzn-s3-demo-bucket/HelloWorld
\"}], "RunList":["{"recipe[HelloWorld::HelloWorldRecipe]\",
\"recipe[HelloWorld::InstallApp]\"}], "JsonAttributesContent":
["{\"state\": \"visible\", \"colors\": {\"foreground\": \"light-blue
\", \"background\": \"dark-gray\"}}"], "ChefClientVersion": [\"14\"],
\"ChefClientArguments\": [\"--fips\"], \"WhyRun\": false, \"ComplianceSeverity\":
[\"Medium\"], \"ComplianceType\": [\"Custom:Chef\"], \"ComplianceReportBucket\":
[\"ChefComplianceResultsBucket\"]}' \
--association-name "name" \
--schedule-expression "cron(0 2 ? * SUN *)"
```

## Windows

```
aws ssm create-association --name "AWS-ApplyChefRecipes" ^
--targets "Key=tag:OS,Values= Linux" ^
--parameters '{"SourceType":["S3"],"SourceInfo":["{"path
\": \"https://s3.amazonaws.com/amzn-s3-demo-bucket/HelloWorld
\"}], "RunList":["{"recipe[HelloWorld::HelloWorldRecipe]\",
\"recipe[HelloWorld::InstallApp]\"}], "JsonAttributesContent":
["{\"state\": \"visible\", \"colors\": {\"foreground\": \"light-blue
\", \"background\": \"dark-gray\"}}"], "ChefClientVersion": [\"14\"],
\"ChefClientArguments\": [\"--fips\"], \"WhyRun\": false, \"ComplianceSeverity\":
[\"Medium\"], \"ComplianceType\": [\"Custom:Chef\"], \"ComplianceReportBucket\":
[\"ChefComplianceResultsBucket\"]}' ^
--association-name "name" ^
--schedule-expression "cron(0 2 ? * SUN *)"
```

Il sistema crea l'associazione e, a meno che l'espressione Cron o della frequenza specificata non lo impedisca, esegue l'associazione sui nodi di destinazione.

### Note

Le associazioni di State Manager non supportano tutte le espressioni Cron e della frequenza. Per ulteriori informazioni sulla creazione di espressioni Cron e della frequenza per le associazioni, consulta [Riferimento: espressioni Cron e della frequenza per Systems Manager](#).

3. Esegui il comando riportato sotto per visualizzare lo stato dell'associazione appena creata.



```
aws ssm describe-association --association-id "ID"
```

## Visualizzazione dei dettagli di conformità delle risorse Chef

Systems Manager acquisisce le informazioni di conformità sulle risorse gestite da Chef nel valore del Compliance report bucket (bucket del report di conformità) di Amazon S3 specificato durante l'esecuzione del documento `AWS-ApplyChefRecipes`. La ricerca di informazioni sugli errori delle risorse Chef in un bucket S3 richiede del tempo. È invece possibile visualizzare queste informazioni nella pagina Compliance (Conformità) di Systems Manager.

Un'analisi della conformità di Systems Manager raccoglie informazioni sulle risorse dei nodi gestiti create o controllate nell'esecuzione Chef più recente. Le risorse possono includere file, directory, servizi `systemd`, pacchetti `yum`, file con modelli, pacchetti `gem` e cookbook dipendenti, tra gli altri.

Nella sezione (Riepilogo risorse di conformità è visualizzato il conteggio delle risorse non riuscite. Nell'esempio seguente, `ComplianceType` è `Custom: Chef` e una risorsa non è conforme.

### Note

`Custom: Chef` è il `ComplianceType` valore predefinito nel documento. `AWS-ApplyChefRecipes` Il valore è personalizzabile.

| Compliance type | Compliant resources                                                                   | Non-Compliant resources                                                               | Critical resources                                                                    | High resources                                                                        | Medium resources                                                                      | Low resources                                                                         | Informational resources                                                               | Unspecified resources                                                                 |
|-----------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Custom:Chef     |  1 |  0 |  0 |  0 |  0 |  0 |  0 |  0 |

La sezione Panoramica dei dettagli delle risorse mostra le informazioni sulla AWS risorsa che non è conforme. Questa sezione include anche il tipo di risorsa Chef per cui è stata eseguita la conformità, la gravità del problema, lo stato di conformità e i collegamenti a ulteriori informazioni, se applicabile.

Details overview for resources

| ID     | Resource type   | Compliance type | Overall severity | Overall status | Execution time                |
|--------|-----------------|-----------------|------------------|----------------|-------------------------------|
| i-0... | ManagedInstance | Custom:Chef     | Critical         | Compliant      | Wed, 19 Feb 2020 17:14:37 GMT |

Compliance rule

Search:  All Compliant < 1 >

Status: Equal: Compliant ComplianceType: Equal: Custom:Chef Severity: Equal: All ResourceId: Equal: i-0... 6

| ID                                                   | Compliance type | Resource ID | Severity | Status    | Execution time                | Detailed status |
|------------------------------------------------------|-----------------|-------------|----------|-----------|-------------------------------|-----------------|
| aws-site:install-nginx::nginx                        | Custom:Chef     | i-0... 6    | Critical | Compliant | Wed, 19 Feb 2020 17:14:37 GMT | -               |
| aws-site:install-nginx::nginx                        | Custom:Chef     | i-0... 6    | Critical | Compliant | Wed, 19 Feb 2020 17:14:37 GMT | -               |
| aws-site:install-nginx::/var/www/html/               | Custom:Chef     | i-0... 6    | Critical | Compliant | Wed, 19 Feb 2020 17:14:37 GMT | -               |
| aws-site:install-nginx::etc/nginx/nginx.conf         | Custom:Chef     | i-0... 6    | Critical | Compliant | Wed, 19 Feb 2020 17:14:37 GMT | -               |
| aws-site:deploy-app::usr/share/nginx/html/index.html | Custom:Chef     | i-0... 6    | Critical | Compliant | Wed, 19 Feb 2020 17:14:37 GMT | -               |

View output (Visualizzazione dell'output) mostra gli ultimi 4.000 caratteri dello stato dettagliato. Systems Manager inizia con l'eccezione come primo elemento, trova messaggi dettagliati e li mostra fino a raggiungere la quota di 4.000 caratteri. Questo processo mostra i messaggi di log generati prima dell'eccezione ovvero i messaggi più rilevanti per la risoluzione dei problemi.

Per informazioni su come visualizzare le informazioni di conformità, consulta [AWS Systems Manager Conformità](#).

### Important

Se l'associazione State Manager ha esito negativo, non viene creato alcun report sui dati di conformità. Ad esempio, se Systems Manager tenta di scaricare un cookbook Chef da un bucket S3 per il cui accesso il nodo non dispone di autorizzazione, l'associazione non va a buon fine e Systems Manager non crea alcun report dei dati di conformità.

## Procedura dettagliata: aggiorna SSM Agent automaticamente con AWS CLI

La procedura seguente ti guiderà attraverso il processo di creazione di un'associazione di State Manager utilizzando AWS Command Line Interface. L'associazione aggiorna automaticamente l'SSM Agent in base a una pianificazione da te specificata. Per ulteriori informazioni su SSM Agent, consultare [Lavorare con Agente SSM](#). Per personalizzare la pianificazione degli aggiornamenti per SSM Agent tramite la console, consulta [Aggiornamento automatico Agente SSM](#).

Per ricevere notifiche sugli aggiornamenti dell'SSM Agent, iscriviti alla pagina [Note di rilascio dell'SSM Agent](#) su GitHub.

## Prima di iniziare

Prima di completare la procedura seguente, verificare di disporre di almeno un'istanza Amazon Elastic Compute Cloud (Amazon EC2) in esecuzione per Linux, macOS o Windows Server configurata per Systems Manager. Per ulteriori informazioni, consulta [Configurazione dei nodi gestiti per AWS Systems Manager](#).

Se create un'associazione utilizzando AWS CLI o AWS Tools for Windows PowerShell, utilizzate il `--Targets` parametro per indirizzare le istanze, come illustrato nell'esempio seguente. Non utilizzare il parametro `--InstanceID`. Il parametro `--InstanceID` è un parametro legacy.

Per creare un'associazione per aggiornare automaticamente l'SSM Agent

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Esegui il comando seguente per creare un'associazione scegliendo come destinazione le istanze tramite i tag Amazon Elastic Compute Cloud (Amazon EC2). Sostituisci ogni *example resource placeholder* con le tue informazioni. Il parametro `Schedule` imposta una pianificazione per eseguire l'associazione ogni domenica mattina alle 2:00 (UTC).

Le associazioni di State Manager non supportano tutte le espressioni Cron e della frequenza. Per ulteriori informazioni sulla creazione di espressioni Cron e della frequenza per le associazioni, consulta [Riferimento: espressioni Cron e della frequenza per Systems Manager](#).

### Linux & macOS

```
aws ssm create-association \
--targets Key=tag:tag_key,Values=tag_value \
--name AWS-UpdateSSMAgent \
--schedule-expression "cron(0 2 ? * SUN *)"
```

### Windows

```
aws ssm create-association ^
--targets Key=tag:tag_key,Values=tag_value ^
--name AWS-UpdateSSMAgent ^
--schedule-expression "cron(0 2 ? * SUN *)"
```

È inoltre possibile definire come target più istanze specificando gli ID delle istanze in un elenco separato da virgole.

## Linux & macOS

```
aws ssm create-association \
--targets Key=instanceids,Values=instance_ID,instance_ID,instance_ID \
--name AWS-UpdateSSMAgent \
--schedule-expression "cron(0 2 ? * SUN *)"
```

## Windows

```
aws ssm create-association ^
--targets Key=instanceids,Values=instance_ID,instance_ID,instance_ID ^
--name AWS-UpdateSSMAgent ^
--schedule-expression "cron(0 2 ? * SUN *)"
```

È possibile specificare la versione dell'SSM Agent a cui desideri aggiornare.

## Linux & macOS

```
aws ssm create-association \
--targets Key=instanceids,Values=instance_ID,instance_ID,instance_ID \
--name AWS-UpdateSSMAgent \
--schedule-expression "cron(0 2 ? * SUN *)" \
--parameters version=ssm_agent_version_number
```

## Windows

```
aws ssm create-association ^
--targets Key=instanceids,Values=instance_ID,instance_ID,instance_ID ^
--name AWS-UpdateSSMAgent ^
--schedule-expression "cron(0 2 ? * SUN *)" ^
--parameters version=ssm_agent_version_number
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
 "AssociationDescription": {
 "ScheduleExpression": "cron(0 2 ? * SUN *)",
 "Name": "AWS-UpdateSSMAgent",
 "Overview": {
 "Status": "Pending",
 "DetailedStatus": "Creating"
 },
 "AssociationId": "123.....",
 "DocumentVersion": "$DEFAULT",
 "LastUpdateAssociationDate": 1504034257.98,
 "Date": 1504034257.98,
 "AssociationVersion": "1",
 "Targets": [
 {
 "Values": [
 "TagVaLue"
],
 "Key": "tag:TagKey"
 }
]
 }
}
```

Il sistema tenta di creare l'associazione sulla/e istanza/e e applica lo stato dopo la creazione. L'associazione presenta lo stato Pending.

3. Eseguire il comando seguente per visualizzare uno stato aggiornato dell'associazione creata.

```
aws ssm list-associations
```

Se le istanze non stanno eseguendo attualmente la versione più recente dell'SSM Agent, lo stato mostra Failed. Quando viene pubblicata una nuova versione dell'SSM Agent, l'associazione installa automaticamente il nuovo agente e lo stato mostra Success.

## Spiegazione passo per passo: aggiornare automaticamente i driver PV sulle istanze EC2 per Windows Server

Le Windows Server Amazon Machine Images (AMIs) di Amazon contengono un insieme di driver per consentire l'accesso all'hardware virtualizzato. Questi driver vengono utilizzati da Amazon Elastic

Compute Cloud (Amazon EC2) per mappare i volumi di archivio istanze e Amazon Elastic Block Store (Amazon EBS) ai rispettivi dispositivi. Ti consigliamo di installare i driver più recenti per migliorare la stabilità e le prestazioni delle istanze EC2 per Windows Server. Per ulteriori informazioni sui driver PV, consulta [Driver PV di AWS](#).

La procedura dettagliata seguente mostra come configurare un'associazione State Manager per scaricare e installare automaticamente nuovi driver AWS PV non appena i driver diventano disponibili. State Manager è uno strumento in AWS Systems Manager.

Prima di iniziare

Prima di completare la procedura seguente, verificare di disporre di almeno un'istanza Amazon EC2 per un'esecuzione in Windows Server configurata per Systems Manager. Per ulteriori informazioni, consulta [Configurazione dei nodi gestiti per AWS Systems Manager](#).

Per creare un'associazione di State Manager che aggiorna automaticamente i driver PV

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli State Manager.
3. Selezionare Create association (Crea associazione).
4. Nel campo Name, immettere un nome descrittivo per l'associazione.
5. Nell'elenco Documento, scegli AWS-ConfigureAWSPackage.
6. Nell'area Parameters (Parametri), eseguire le operazioni seguenti:
  - Per Action (Operazione), selezionare Install (Installa).
  - In Installation type (Tipo di installazione), scegliere Uninstall and reinstall (Disinstalla e reinstalla).

 Note

In-place gli aggiornamenti non sono supportati per questo pacchetto. È necessario disinstallarlo e reinstallarlo.

- In Nome, inserisci **AWSPVDriver**.

Non è necessario inserire nulla nei campi Versione e Argomenti aggiuntivi.

7. Nella sezione Destinazioni, identificare i nodi in cui si desidera eseguire questa operazione specificando i tag, selezionando manualmente le istanze, i dispositivi edge o indicando un gruppo di risorse.

 Tip

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

 Note

Se si sceglie di indirizzare le istanze mediante i tag e si specificano tag che mappano per istanze di Linux, l'associazione viene completata sull'istanza di Windows Server, ma non su quelle di Linux. Lo stato globale dell'associazione mostra Failed (Non riuscito).

8. Nell'area Specifica la pianificazione, scegli se eseguire l'associazione in base a una pianificazione configurata dall'utente, oppure solo una volta. I driver PV aggiornati vengono distribuiti più volte all'anno, perciò è possibile pianificare l'esecuzione dell'associazione una volta al mese, se si desidera.
9. Nell'area Advanced options (Opzioni avanzate), per Compliance severity (Gravità conformità), scegliere un livello di gravità per l'associazione. Il report di conformità indica se l'associazione è conforme o non conforme e il livello di gravità specificato qui. Per ulteriori informazioni, consulta [Informazioni State Manager conformità delle associazioni](#).
10. In Controllo velocità:
  - In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti come target, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.
11. (Facoltativo) In Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Abilita scrittura in S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

#### Note

Le autorizzazioni S3 che consentono di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza assegnate al nodo gestito e non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova in un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato all'istanza disponga delle autorizzazioni necessarie per scrivere su quel bucket.

12. (Facoltativo) Nella sezione CloudWatch Allarme, per Nome allarme, scegliete un CloudWatch allarme da applicare all'associazione per il monitoraggio.

#### Note

Prendi nota delle seguenti informazioni importanti relative a questa fase.

- L'elenco degli allarmi riporta un massimo di 100 allarmi. Se non vedi il tuo allarme nell'elenco, usa AWS Command Line Interface per creare l'associazione. Per ulteriori informazioni, consulta [Creazione di un'associazione \(riga di comando\)](#).
- Per allegare un CloudWatch allarme al tuo comando, il responsabile IAM che crea l'associazione deve avere l'autorizzazione per `iam:createServiceLinkedRole`. Per ulteriori informazioni sugli CloudWatch allarmi, consulta [Usare gli CloudWatch allarmi Amazon](#).
- Tenere presente che se l'allarme si attiva, qualsiasi automazione o invocazione di comando in sospeso non viene eseguita.

13. Selezionare Create association (Crea associazione), poi Close (Chiudi). Il sistema tenta di creare l'associazione sulle istanze e di applicare immediatamente lo stato.



Una volta creata l'associazione su una o più istanze Amazon EC2 per Windows Server, lo stato diventa Riuscito. Se le istanze non sono configurate per Systems Manager, oppure se sono state inavvertitamente definite come istanze Linux di destinazione, lo stato mostra Non riuscito.

Se lo stato è Non riuscito, selezionare l'ID associazione, seleziona la scheda Risorse e poi verifica che l'associazione sia stata creata correttamente nelle istanze EC2 per Windows Server. Se le istanze EC2 per Windows Server mostrano lo stato Failed, verifica che SSM Agent 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 della console unificata di Systems Manager per un'organizzazione](#).

## AWS Systems Manager strumenti di gestione delle modifiche

AWS Systems Manager fornisce i seguenti strumenti per apportare modifiche alle AWS risorse.

### Argomenti

- [AWS Systems Manager Automazione di](#)
- [AWS Systems Manager Modifica calendario](#)
- [AWS Systems Manager Change Manager](#)
- [AWS Systems Manager Documenti di](#)
- [AWS Systems Manager Intervallo di manutenzione](#)
- [AWS Systems Manager Configurazione rapida](#)

## AWS Systems Manager Automazione di

L'automazione semplifica le attività comuni di manutenzione, distribuzione e correzione per Servizi AWS Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Simple Storage Service (Amazon S3) e molti altri. Per cominciare a utilizzare Automazione, apri la [console di Systems Manager](#). Nel riquadro di navigazione, scegli Automazione.

Questa sezione contiene gli argomenti seguenti.

- [Implementazione dei controlli delle modifiche per Automazione](#)
- [Esempi di impostazione di politiche basate sull'identità](#)

- [Crea ruoli di servizio per l'automazione utilizzando CloudFormation](#)
- [Scopri gli stati restituiti da Systems Manager Automation](#)
- [Pianificazione delle automazioni con finestre di manutenzione](#)
- [Utilizzo di Generatore di documenti per la creazione di runbook](#)
- [Esegui un'automazione che richiede approvazioni](#)
- [Esecuzione di automazioni in più Regioni AWS e account](#)
- [Esegui automazioni basate sugli eventi EventBridge](#)
- [Esegui un'automazione passo dopo passo](#)
- [Utilizzo di script nei runbook](#)
- [Utilizzo di istruzioni condizionali nei runbook](#)
- [Utilizzo degli output delle operazioni come input](#)
- [Creazione di integrazioni webhook per Automazione](#)
- [Aggiornamento in corso AMI](#)
- [Aggiornamento in corso AMI utilizzando l'automazione e Jenkins](#)
- [Aggiornamento in corso AMI per gruppi Auto Scaling](#)
- [Esecuzione dello strumento EC2Rescue su istanze non raggiungibili](#)
- [Trasmissione dei dati ad Automazione tramite trasformatori di input](#)

Automazione ti consente di creare soluzioni automatizzate per implementare, configurare e gestire le risorse AWS su larga scala. Con Automazione hai un controllo granulare sulla simultaneità delle tue automazioni. Ciò significa che puoi specificare quante risorse utilizzare contemporaneamente e quanti errori possono verificarsi prima che un'automazione venga arrestata.

Per aiutarti a iniziare con Automation, sviluppa e mantiene diversi runbook predefiniti. AWS A seconda del caso d'uso, puoi utilizzare i runbook predefiniti che eseguono varie attività o creare runbook personalizzati in base alle tue specifiche esigenze. Per monitorare l'avanzamento e lo stato delle automazioni, puoi utilizzare la console di Automazione Systems Manager o lo strumento a riga di comando che preferisci. L'automazione si integra anche con Amazon EventBridge per aiutarti a creare un'architettura basata sugli eventi su larga scala.

#### Note

Per i clienti che non hanno mai utilizzato Systems Manager Automation a partire dal 14 agosto 2025, il livello gratuito di questa funzione non è disponibile. Per i clienti che già

utilizzano la funzione Automazione, il livello di servizio gratuito termina il 31 dicembre 2025. Per informazioni sugli attuali costi di servizio, consulta [Prezzi di AWS Systems Manager](#).

## Quali sono i vantaggi di Automazione per la mia azienda?

Automazione offre i seguenti vantaggi:

- Supporto per lo scripting nei contenuti del runbook

Usando l'`aws:executeScript` azione, puoi eseguire Python e PowerShell funzioni personalizzate direttamente dai tuoi runbook. In questo modo avrai una maggiore flessibilità nella creazione di runbook personalizzati, in quanto potrai completare varie attività non supportate da altre operazioni di Automazione. Avrai anche un maggiore controllo sulla logica del runbook. Per un esempio di come questa azione può essere utilizzata e di come può contribuire a migliorare una soluzione automatizzata esistente, consulta [Creazione di runbook del servizio di automazione](#).

- Esegui automazioni su più piattaforme Account AWS e Regioni AWS da una postazione centralizzata

Gli amministratori possono eseguire automazioni su risorse di diversi account e regioni dalla console di Systems Manager.

- Miglioramento della sicurezza delle operazioni

Gli amministratori dispongono di una posizione centralizzata da cui concedere e revocare l'accesso ai runbook. Utilizzando solo le policy AWS Identity and Access Management (IAM), puoi controllare quali singoli utenti o gruppi della tua organizzazione possono utilizzare Automation e a quali runbook possono accedere.

- Automazione delle attività IT comuni

L'automazione delle attività comuni può contribuire a migliorare l'efficienza operativa, a far rispettare gli standard organizzativi e a ridurre gli errori dell'operatore. Ad esempio, puoi utilizzare il `AWS-UpdateCloudFormationStackWithApproval` runbook per aggiornare le risorse che sono state distribuite utilizzando un modello. AWS CloudFormation L'aggiornamento applica un nuovo modello. È possibile configurare il servizio di automazione in modo che venga richiesta l'approvazione da parte di uno o più utenti prima che l'aggiornamento abbia inizio.

- Esecuzione sicura di attività che creano interruzioni in blocco

Automazione include funzionalità, come i controlli di velocità, che consentono di monitorare l'implementazione di un'automazione a livello di parco istanze, specificando un valore di simultaneità e una soglia di errore. Per ulteriori informazioni sull'utilizzo dei controlli di velocità, consulta [Esegui operazioni automatizzate su larga scala](#).

- Semplificazione di attività complesse

Automation fornisce runbook predefiniti che semplificano attività complesse e dispendiose in termini di tempo, come la creazione di Amazon Machine Images in versione finale (AMIs). Ad esempio, puoi utilizzare i runbook di AWS-UpdateLinuxAmi e AWS-UpdateWindowsAmi per creare AMIs in versione finale da una fonte di AMI. Utilizzando questi runbook, puoi eseguire script personalizzati prima e dopo l'applicazione degli aggiornamenti. Puoi inoltre includere o escludere l'installazione di pacchetti software specifici. Per esempi di come utilizzare questi runbook, consulta [Esercitazioni](#).

- Definizione dei vincoli per gli input

Puoi definire vincoli nei runbook personalizzati per limitare i valori che Automation accetterà per un particolare parametro di input. Ad esempio, `allowedPattern` accetterà solo valori per un parametro di input che corrispondono all'espressione regolare definita. Se specifichi `allowedValues` per un parametro di input, vengono accettati solo i valori specificati nel runbook.

- Registra l'output delle azioni di automazione su Amazon Logs CloudWatch

Per soddisfare i requisiti operativi o di sicurezza della tua organizzazione, potresti dover fornire un registro degli script eseguiti durante un runbook. Con CloudWatch Logs, puoi monitorare, archiviare e accedere a diversi file di registro Servizi AWS. È possibile inviare l'output dell'`aws:executeScriptazione` a un gruppo di CloudWatch log Logs per scopi di debug e risoluzione dei problemi. I dati di registro possono essere inviati al gruppo di log con o senza AWS KMS crittografia utilizzando la chiave KMS. Per ulteriori informazioni, consulta [Uscita dell'azione Logging Automation con Logs CloudWatch](#).

- Integrazione con Amazon EventBridge

L'automazione è supportata come tipo di destinazione nelle EventBridge regole di Amazon. Ciò significa che puoi attivare i runbook utilizzando gli eventi. Per ulteriori informazioni, consulta [Monitoraggio degli eventi di Systems Manager con Amazon EventBridge](#) e [Riferimento: modelli e tipi di EventBridge eventi Amazon per Systems Manager](#).

- Condivisione delle best practice organizzative

Puoi definire le best practice per la gestione delle risorse, le attività operative e altro ancora nei runbook condivisi tra account e regioni.

## Chi deve utilizzare Automation?

- Qualsiasi AWS cliente che desideri migliorare la propria efficienza operativa su larga scala, ridurre gli errori associati all'intervento manuale e ridurre i tempi di risoluzione dei problemi comuni.
- Esperti di infrastruttura che desiderano automatizzare le attività di implementazione e configurazione.
- Amministratori che desiderano risolvere in modo affidabile i problemi comuni, migliorare l'efficienza della risoluzione dei problemi e ridurre le operazioni ripetitive.
- Utenti che desiderano automatizzare un'attività che in genere eseguono manualmente.

## Cos'è un'automazione?

Un'automazione è costituita da tutte le attività definite in un runbook ed eseguite dal servizio Automation. Automation utilizza i seguenti componenti per eseguire le automazioni.

| Concetto               | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| runbook di Automazione | Un runbook di Systems Manager Automation definisce l'automazione (le azioni che Systems Manager esegue sui nodi e sulle AWS risorse gestiti). Il servizio di Automazione include numerosi runbook predefiniti che puoi utilizzare e per eseguire processi comuni, ad esempio il riavvio di una o più istanze di Amazon EC2 o la creazione di un'Amazon Machine Image (AMI). Puoi anche creare runbook personalizzati. I runbook utilizzano il formato YAML o JSON e includono le fasi e i parametri specificati. Le fasi vengono eseguite in ordine sequenziale. Per ulteriori informazioni, consulta <a href="#">Creazione di runbook personalizzati</a> . |

| Concetto                  | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           | <p>I runbook sono documenti di Systems Manager di tipo Automation , a differenza dei documenti di Command, Policy, Session.</p> <p>I runbook supportano la versione dello schema 0.3. I documenti di comando utilizzano la versione dello schema 1.2, 2.0 o 2.2. I documenti di Policy utilizzano la versione dello schema 2.0 o successiva.</p>                                                                                                                                         |
| Operazione di automazione | <p>L'automazione definita in un runbook include una o più fasi. Ogni passaggio è associato a un'operazione specifica. L'operazione determina gli input, il comportamento e l'output della fase. Le fasi vengono definite nella sezione <code>mainSteps</code> del runbook. L'automazione supporta 20 tipi di operazioni distinte.</p> <p>Per ulteriori informazioni, consulta la sezione <a href="#">Riferimento alle operazioni del servizio di automazione di Systems Manager</a>.</p> |

| Concetto                        | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Quota di automazione            | <p>Ciascuno Account AWS può eseguire 100 automazioni contemporaneamente. Ciò include le automazioni figlio (automazioni avviate da un'altra automazione) e le automazioni di controllo della velocità. Se provi a eseguire un numero maggiore di automazioni, Systems Manager aggiungerà le altre automazioni a una coda e visualizzerà lo stato In attesa. Questa quota può essere regolata utilizzando la simultaneità adattiva. Per ulteriori informazioni, consulta la pagina <a href="#">Consentire ad Automation di adattarsi alle esigenze di simultaneità</a>. Per ulteriori informazioni sull'esecuzione delle automazioni, consulta la pagina <a href="#">Esegui un'operazione automatizzata basata su Systems Manager Automation</a>.</p> |
| Quota della coda di automazioni | <p>Se provi a eseguire più automazioni rispetto al limite di automazioni simultanee, le automazioni successive saranno aggiunte a una coda. Ogni Account AWS può mettere in coda 5.000 automazioni. Quando un'automazione è completa (o raggiunge la fase terminale), viene avviata la prima esecuzione presente nella coda.</p>                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Concetto                                                  | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Quota di automazione del controllo della velocità         | Ciascuno Account AWS può eseguire 25 automazioni di controllo della tariffa contemporaneamente. Se si prova a eseguire più automazioni di controllo della velocità rispetto al limite simultaneo di automazione del controllo della velocità, Systems Manager aggiunge le successive automazioni di controllo della velocità a una coda e visualizza lo stato come Pending. Per ulteriori informazioni sull'esecuzione di automazioni per il controllo della velocità, consulta <a href="#">Esegui operazioni automatizzate su larga scala</a> . |
| Quota di coda di automazione del controllo della velocità | Se si prova a eseguire più automazioni rispetto al limite simultaneo di automazione del controllo della velocità, le automazioni successive vengono aggiunte a una coda. Ciascuna Account AWS può mettere in coda 1.000 automazioni di controllo della tariffa. Quando un'automazione è completa (o raggiunge la fase terminale), viene avviata la prima automazione presente nella coda.                                                                                                                                                        |

## Configurazione del servizio di automazione

Per configurare il servizio di automazione, è necessario verificare l'accesso utente al servizio di automazione e configurare i ruoli in base alla situazione in modo che il servizio possa eseguire operazioni sulle risorse. Ti consigliamo inoltre di accedere alla modalità di simultaneità adattiva nelle preferenze di Automation. La simultaneità adattiva dimensiona automaticamente la quota di automazione per soddisfare le tue esigenze. Per ulteriori informazioni, consulta [Consentire ad Automation di adattarsi alle esigenze di simultaneità](#).

Per assicurarti di avere un accesso corretto all' AWS Systems Manager automazione, esamina i seguenti requisiti relativi ai ruoli utente e di servizio.



## Verifica dell'accesso utente per runbook

Verifica di disporre dell'autorizzazione per utilizzare i runbook. Se all'utente, al gruppo o al ruolo sono assegnate le autorizzazioni di amministratore, potrai accedere all'Automazione di Systems Manager. Se non disponi delle autorizzazioni di amministratore, un amministratore dovrà concedere le autorizzazioni necessarie assegnando la policy gestita AmazonSSMFullAccess oppure una policy che conceda autorizzazioni analoghe all'utente, al gruppo o al ruolo.

### Important

La policy IAM di AmazonSSMFullAccess concede autorizzazioni per le operazioni di Systems Manager. Tuttavia, alcuni runbook richiedono le autorizzazioni ad altri servizi, ad esempio il runbook di AWS-ReleaseElasticIP, che richiede autorizzazioni IAM per `ec2:ReleaseAddress`. Pertanto, devi esaminare le azioni intraprese in un runbook per assicurarti che al tuo utente, gruppo o ruolo siano assegnate le autorizzazioni necessarie per eseguire le azioni incluse nel runbook.

## Configurazione di un accesso al ruolo di servizio (ruolo presunto) per le automazioni

Le automazioni possono essere avviate nel contesto di un ruolo di servizio (o ruolo presunto). Ciò permette al servizio di eseguire operazioni per conto tuo. Se non specifichi un ruolo presunto, il servizio di automazione utilizza il contesto dell'utente che ha richiamato l'automazione.

Tuttavia, i seguenti scenari richiedono di specificare un ruolo di servizio di Automazione:

- Quando si desidera limitare le autorizzazioni di un utente per una risorsa, ma che permette all'utente di eseguire un'automazione che richiede autorizzazioni elevate. In questo scenario è possibile creare un ruolo di servizio con autorizzazioni elevate e permettere all'utente di eseguire l'automazione.
- Quando si crea un'associazione di Systems Manager State Manager che esegue un runbook.
- Quando disponi di operazioni che prevedi vengano eseguite per più di 12 ore.
- Quando esegui un runbook non di proprietà di Amazon che utilizza `aws:executeScriptazione` per chiamare un'operazione AWS API o per agire su una risorsa. AWS Per informazioni, consulta [Autorizzazioni per l'utilizzo di runbook](#).

Se devi creare un ruolo di servizio per il servizio di automazione, puoi utilizzare uno dei seguenti metodi.

## Crea ruoli di servizio per l'automazione utilizzando CloudFormation

Puoi creare un ruolo del servizio per l'automazione da un modello AWS CloudFormation . Dopo aver creato il ruolo di servizio, puoi specificare il ruolo di servizio nei runbook utilizzando il parametro `AutomationAssumeRole`.

### Crea il ruolo del servizio utilizzando CloudFormation

Utilizzare la procedura seguente per creare il ruolo AWS Identity and Access Management (IAM) richiesto per Systems Manager Automation utilizzando CloudFormation.

Per creare il ruolo IAM richiesto

1. scarica e decomprimi il file [AWS-SystemsManager-AutomationServiceRole.zip](#). Questo file include il file `AWS-SystemsManager-AutomationServiceRole.yaml` CloudFormation modello.
2. Apri la CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
3. Scegliere Create Stack (Crea stack).
4. Nella sezione Specify template (Specifica il modello) scegliere Upload a template file (Carica un file modello).
5. Scegli Sfoglia, quindi scegli il file `AWS-SystemsManager-AutomationServiceRole.yaml` CloudFormation modello.
6. Scegliere Next (Successivo).
7. Nella pagina Specify stack details (Specifica dettagli dello stack), inserire un nome nel campo Stack name (Nome stack).
8. Nella pagina Configure stack options (Configura opzioni stack) non è necessario effettuare alcuna selezione. Scegli Next (Successivo).
9. Nella pagina Revisione, scorri verso il basso e scegli l'opzione Riconosco che CloudFormation potrebbe creare risorse IAM.
10. Scegli Create (Crea).

CloudFormation mostra lo stato `CREATE_IN_PROGRESS` per circa tre minuti. Lo stato diventa `CREATE_COMPLETE` al termine della creazione dello stack e i ruoli sono pronti per essere utilizzati.

 Important

Se si esegue un flusso di lavoro di automazione che chiama altri servizi utilizzando un ruolo di servizio (IAM) AWS Identity and Access Management , tenere presente che tale ruolo di servizio deve essere configurato con l'autorizzazione per la chiamata di tali servizi. Questo requisito si applica a tutti i runbook (runbook) di AWS Automation come, e AWS - \* AWS-RestartEC2Instance runbook AWS-ConfigureS3BucketLoggingAWS-CreateDynamoDBBackup, solo per citarne alcuni. Questo requisito si applica anche a tutti i runbook di Automation personalizzati creati che richiamano altri utenti Servizi AWS utilizzando azioni che richiamano altri servizi. Ad esempio, se utilizzi le operazioni `aws:executeAwsApi`, `aws:createStack` o `aws:copyImage`, devi configurare il ruolo di servizio con l'autorizzazione per richiamare tali servizi. Puoi concedere le autorizzazioni ad altri Servizi AWS aggiungendo una policy inline IAM al ruolo. Per ulteriori informazioni, consulta [\(Facoltativo\) Aggiungi una policy in linea di Automation o una policy gestita dal cliente per richiamarne altre Servizi AWS](#).

## Copia delle informazioni sui ruoli per l'automazione

Utilizza la procedura seguente per copiare le informazioni sul ruolo del servizio di automazione dalla CloudFormation console. È necessario specificare questi ruoli quando si utilizza un runbook.

 Note

Non è necessario copiare le informazioni del ruolo per questa procedura se esegui i runbook di AWS-UpdateLinuxAmi o AWS-UpdateWindowsAmi. Questi runbook includono già i ruoli richiesti specificati come valori di default. I ruoli specificati in questi runbook utilizzano le policy IAM gestite.

## Per copiare i nomi dei ruoli

1. Apri la CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
2. Selezionare lo Stack name (Nome dello stack) di automazione creato nella procedura precedente.
3. Scegliere la scheda Resources (Risorse).

4. Scegli il link Physical ID per AutomationServiceRole. La console di IAM visualizza il riepilogo del ruolo di servizio dell'automazione.
5. Copiare l'Arn l'Amazon Resource Name (ARN) accanto a Role ARN (ARN ruolo). L'ARN è simile al seguente: `arn:aws:iam::12345678:role/AutomationServiceRole`
6. Incollare l'ARN in un file di testo da usare in un secondo momento.

La configurazione del ruolo di servizio per il servizio di automazione è stata completata. Ora puoi utilizzare l'Amazon Resource Name (ARN) del ruolo di servizio dell'automazione nei runbook.

Crea ruoli di servizio per l'automazione tramite la console

Se devi creare un ruolo di servizio per Automation, completa le seguenti attività. Per ulteriori informazioni su quando un ruolo di servizio è obbligatorio per l'automazione, consulta [Configurazione del servizio di automazione](#).

## Processi

- [Processo 1: creazione di un ruolo di servizio per il servizio di automazione](#)
- [Attività 2: Associa la PassRole policy iam: al tuo ruolo di automazione](#)

### Processo 1: creazione di un ruolo di servizio per il servizio di automazione

Utilizza la procedura seguente per creare un ruolo di servizio (o ruolo presunto) per il servizio di automazione di Systems Manager.

#### Note

Puoi anche utilizzare questo ruolo nei runbook, ad esempio il runbook AWS - CreateManagedLinuxInstance. L'utilizzo di questo ruolo, o dell'Amazon Resource Name (ARN) di un ruolo AWS Identity and Access Management (IAM), nei runbook consente ad Automation di eseguire azioni nel tuo ambiente, come lanciare nuove istanze ed eseguire azioni per tuo conto.

Per creare un ruolo IAM e consentire al servizio di automazione di usarlo

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, scegliere Roles (Ruoli) e quindi Create role (Crea ruolo).

3. In Select type of trusted entity (Seleziona tipo di entità attendibile), scegliere AWS service (Servizio).
4. Nella sezione Choose a use case (Scegli un caso d'uso), scegliere Systems Manager, e quindi scegliere Next: Permissions (Successivo: autorizzazioni).
5. Nella pagina della politica delle autorizzazioni allegata, cerca la AmazonSSMAutomationRole policy, sceglila, quindi scegli Avanti: Revisione.
6. Nella pagina Review (Rivedi) inserire un nome nella casella Role name (Nome ruolo), quindi inserire una descrizione.
7. Scegliere Create role (Crea ruolo). Il sistema visualizza di nuovo la pagina Roles (Ruoli).
8. Nella pagina Ruoli, scegli il ruolo appena creato per aprire la pagina Riepilogo. Annotare i valori per Role Name (Nome ruolo) e Role ARN (ARN ruolo). Specifica il ruolo ARN quando allegghi la PassRole policy iam: al tuo account IAM nella procedura successiva. È inoltre possibile specificare il nome di ruolo e l'ARN nei runbook.

#### Note

La AmazonSSMAutomationRole policy assegna l'autorizzazione del ruolo Automation a un sottoinsieme di AWS Lambda funzioni all'interno del tuo account. Queste funzioni iniziano con "Automation". Se si prevede di utilizzare il servizio di automazione con funzioni Lambda, l'ARN Lambda deve utilizzare il seguente formato:

**"arn:aws:lambda:\*:\*:function:Automation\*"**

Se disponi di funzioni Lambda esistenti i cui ARN non utilizzano questo formato, devi anche allegare una policy Lambda aggiuntiva al tuo ruolo di automazione, come la policy. AWSLambdaRole La policy o il ruolo aggiuntivo deve garantire un accesso più ampio alle funzioni Lambda all'interno dell' Account AWS.

Dopo aver creato il tuo ruolo di servizio, ti consigliamo di modificare la policy di attendibilità per evitare il problema del "confused deputy" tra servizi. 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. In AWS, l'impersonificazione tra servizi può causare il confuso problema del vice. Cross-service impersonification può avvenire quando un servizio (il servizio chiamante) chiama un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare che ciò accada, AWS fornisce strumenti che

consentono di proteggere i dati per tutti i servizi ai quali è stato concesso l'accesso alle risorse del proprio account.

Ti consigliamo di utilizzare le chiavi di contesto delle condizioni globali [aws:SourceArn](#) e [aws:SourceAccount](#) nelle policy delle risorse per limitare le autorizzazioni con cui Automation fornisce un altro servizio alla risorsa. Se il valore `aws:SourceArn` non contiene l'ID account, ad esempio un ARN del bucket Amazon S3, devi utilizzare entrambe le chiavi di contesto delle condizioni globali per limitare le autorizzazioni. 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` deve utilizzare lo stesso ID account nella stessa dichiarazione di policy. Utilizzare `aws:SourceArn` se si desidera consentire l'associazione di una sola risorsa all'accesso tra servizi. Utilizzare `aws:SourceAccount` se si desidera consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi. Il valore di `aws:SourceArn` deve essere l'ARN per l'esecuzione delle automazioni. Se non si conosce l'ARN completo della risorsa o se si sta specificando più risorse, utilizzare la chiave di condizione del contesto globale `aws:SourceArn` con caratteri speciali (\*) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:ssm:*:123456789012:automation-execution/*`.

L'esempio seguente mostra il modo in cui puoi utilizzare le chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` per l'automazione per prevenire il problema `confused deputy`.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": [
 "ssm.amazonaws.com"
]
 },
 "Action": "sts:AssumeRole",
 "Condition": {
 "StringEquals": {
 "aws:SourceAccount": "123456789012"
 },
 "ArnLike": {
```

```
 "aws:SourceArn": "arn:aws:ssm:*:123456789012:automation-execution/*"
 }
 }
 }
]
}
```

Per modificare una policy di attendibilità del ruolo

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, seleziona Ruoli.
3. Nell'elenco dei ruoli dell'account, scegliere il nome del ruolo di servizio di Automation.
4. Selezionare la scheda Trust relationships (Relazioni di trust) e scegliere Edit trust relationship (Modifica relazione di trust).
5. Modificare la policy di attendibilità utilizzando le chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` per fare in modo che Automation prevenga il problema del "confused deputy".
6. Per salvare le modifiche, scegliere Update Trust Policy (Aggiorna policy di attendibilità).

(Facoltativo) Aggiungi una policy in linea di Automation o una policy gestita dal cliente per richiamarne altre Servizi AWS

Se esegui un'automazione che ne richiama altri Servizi AWS utilizzando un ruolo del servizio IAM, il ruolo del servizio deve essere configurato con l'autorizzazione per richiamare tali servizi. Questo requisito si applica a tutti i runbook (AWS-\*runbook) di AWS Automation come, e i AWS-RestartEC2Instance runbook AWS-ConfigureS3BucketLoggingAWS-CreateDynamoDBBackup, solo per citarne alcuni. Questo requisito vale anche per i runbook personalizzati che utilizzano altri Servizi AWS tramite l'utilizzo di operazioni che chiamano altri servizi. Ad esempio, se utilizzi le operazioni `aws:executeAwsApi`, `aws:CreateStack` o `aws:copyImage`, per citarne alcune, devi configurare il ruolo di servizio con l'autorizzazione per richiamare questi servizi. Puoi concedere autorizzazioni ad altri Servizi AWS aggiungendo al ruolo una policy IAM in linea o una policy gestita dal cliente.

Per incorporare una policy inline per un ruolo di servizio (console IAM)

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

2. Nel pannello di navigazione, scegliere Roles (Ruoli).
3. Nell'elenco, scegliere il nome del ruolo da modificare.
4. Scegliere la scheda Permissions (Autorizzazioni).
5. Nell'elenco a discesa Aggiungi autorizzazioni, scegli Collega policy o Crea policy inline.
6. Se scegli Collega policy, seleziona la casella di controllo accanto alla policy che desideri aggiungere e scegli Aggiungi autorizzazioni.
7. Scegli Crea policy inline, quindi scegli la scheda JSON.
8. Inserisci il documento JSON Policy Servizi AWS che desideri richiamare. Di seguito sono riportati due documenti della policy JSON di esempio.

Amazon PutObject S3 ed esempio GetObject

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "s3:PutObject",
 "s3:GetObject"
],
 "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
 }
]
}
```

Amazon EC2 ed esempio CreateSnapshot DescribeSnapshots

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
```



```
 "Effect": "Allow",
 "Action": "ec2:CreateSnapshot",
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": "ec2:DescribeSnapshots",
 "Resource": "*"
 }
]
```

Per informazioni sul linguaggio della policy IAM consulta [Riferimento alle policy JSON IAM](#) nella Guida per l'utente IAM.

9. Al termine, seleziona Review policy (Rivedi policy). In [Policy Validator](#) (Validatore di policy) vengono segnalati eventuali errori di sintassi.
10. Nella pagina Review policy (Rivedi policy), inserire un Name (Nome) per la policy che stai creando. Consulta il Riepilogo della policy per visualizzare le autorizzazioni concesse dalla policy. Seleziona Create policy (Crea policy) per salvare il proprio lavoro.
11. Una volta creata, una policy inline viene automaticamente incorporata nel ruolo.

## Attività 2: Associa la PassRole policy iam: al tuo ruolo di automazione

Utilizza la procedura seguente per collegare la policy `iam:PassRole` al ruolo di servizio di Automazione. Ciò consente al servizio di automazione di passare il ruolo ad altri servizi o strumenti di Systems Manager durante l'esecuzione delle automazioni.

Per allegare la PassRole policy iam: al tuo ruolo Automation

1. Nella pagina Summary (Riepilogo) per il ruolo creato in precedenza, scegliere la scheda Permissions (Autorizzazioni).
2. Scegliere Add inline policy (Aggiungi policy inline).
3. Nella pagina Create Policy (Crea policy), scegliere la scheda Visual editor (Editor visivo).
4. Scegliere Service (Servizio), quindi IAM.
5. Scegliere Select actions (Seleziona operazioni).
6. Nella casella di testo Filtra azioni, digita **PassRole**, quindi scegli l'PassRole opzione.

7. Scegliere Resources (Risorse). Verifica che l'opzione Specific (Specifico) sia selezionata, quindi scegliere Add ARN (Aggiungi ARN).
8. Nel campo Specify ARN for role (Specifica ARN per il ruolo), incolla l'ARN del ruolo di automazione copiato alla fine del processo 1. Il sistema popola automaticamente i campi Account e Role name with path (Nome ruolo con percorso).

 Note

Se desideri che il ruolo di servizio dell'automazione alleggi un ruolo del profilo dell'istanza IAM a un'istanza EC2, è necessario aggiungere l'ARN del ruolo del profilo dell'istanza. Ciò consente al ruolo di servizio di dell'automazione di passare il ruolo del profilo dell'istanza IAM all'istanza EC2 di destinazione.

9. Scegliere Add (Aggiungi).
10. Scegliere Review policy (Rivedi policy).
11. Nella pagina Review Policy (Rivedi policy), inserire un nome, quindi scegliere Create Policy (Crea policy).

## Esempi di impostazione di politiche basate sull'identità

Le sezioni seguenti forniscono esempi di politiche basate sull'identità IAM per AWS Systems Manager il servizio di automazione. Per ulteriori informazioni su come creare una policy basata sull'identità IAM utilizzando questi esempi di documenti JSON Policy, consulta [Creating IAM policies nella IAM User Guide](#).

 Note

Tutti gli esempi contengono ID di account fittizi. L'ID dell'account non deve essere specificato nell'Amazon Resource Name (ARN) per i documenti pubblici AWS di proprietà.

## Esempi

- [Esempio 1: consentire a un utente di eseguire un documento di automazione e visualizzare l'esecuzione dell'automazione](#)
- [Esempio 2: consentire a un utente di eseguire una versione specifica di un documento di automazione](#)

- [Esempio 3: consentire a un utente di eseguire documenti di automazione con un tag specifico](#)
- [Esempio 4: consente a un utente di eseguire un documento di automazione quando viene fornito un parametro di tag specifico per l'esecuzione dell'automazione](#)

Esempio 1: consentire a un utente di eseguire un documento di automazione e visualizzare l'esecuzione dell'automazione

La seguente policy IAM di esempio permette a un utente di eseguire queste operazioni:

- Esegui il documento di automazione specificato nella politica. Il nome del documento è determinato dalla seguente voce:

```
arn:aws:ssm:*:111122223333:document/{{DocumentName}}
```

- Interrompi e invia segnali a un'esecuzione di automazione.
- Visualizza i dettagli sull'esecuzione dell'automazione dopo che è stata avviata.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Action": "ssm:StartAutomationExecution",
 "Effect": "Allow",
 "Resource": [
 "arn:aws:ssm:*:111122223333:document/{{DocumentName}}",
 "arn:aws:ssm:*:111122223333:automation-execution/*"
]
 },
 {
 "Action": [
 "ssm:StopAutomationExecution",
 "ssm:GetAutomationExecution",
 "ssm:DescribeAutomationExecutions",
 "ssm:DescribeAutomationStepExecutions",
 "ssm:SendAutomationSignal"
],
 "Resource": [
 "arn:aws:ssm:*:111122223333:automation-execution/*"
]
 }
]
}
```

```

],
 "Effect": "Allow"
 }
]
}

```

Esempio 2: consentire a un utente di eseguire una versione specifica di un documento di automazione

Il seguente esempio di policy IAM consente a un utente di eseguire una versione specifica di un documento di automazione:

- Il nome del documento di automazione è determinato dalla seguente voce.

```
arn:aws:ssm:*:111122223333:document/{{DocumentName}}
```

- La versione del documento di automazione è determinata dalla seguente voce.

```
"ssm:DocumentVersion": "5"
```

## JSON

```

{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Action": "ssm:StartAutomationExecution",
 "Effect": "Allow",
 "Resource": [
 "arn:aws:ssm:*:111122223333:document/{{DocumentName}}"
],
 "Condition": {
 "ForAnyValue:StringEquals": {
 "ssm:DocumentVersion": ["5"]
 }
 }
 },
 {
 "Action": [
 "ssm:StartAutomationExecution"

```

```

],
 "Resource": [
 "arn:aws:ssm:*:111122223333:automation-execution/*"
],
 "Effect": "Allow"
},
{
 "Action": [
 "ssm:StopAutomationExecution",
 "ssm:GetAutomationExecution",
 "ssm:DescribeAutomationExecutions",
 "ssm:DescribeAutomationStepExecutions",
 "ssm:SendAutomationSignal"
],
 "Resource": [
 "arn:aws:ssm:*:111122223333:automation-execution/*"
],
 "Effect": "Allow"
}
]
}

```

Esempio 3: consentire a un utente di eseguire documenti di automazione con un tag specifico

Il seguente esempio di policy IAM consente a un utente di eseguire qualsiasi documento di automazione che abbia un tag specifico:

- Il nome del documento di automazione è determinato dalla seguente voce.

```
arn:aws:ssm:*:111122223333:document/{{DocumentName}}
```

- Il tag del documento di automazione è determinato dalla seguente voce.

```
"ssm:DocumentVersion": "5"
```

## JSON

```

{
 "Version": "2012-10-17",
 "Statement": [

```

```

 {
 "Action": "ssm:StartAutomationExecution",
 "Effect": "Allow",
 "Resource": [
 "arn:aws:ssm:*:111122223333:document/*"
],
 "Condition": {
 "StringEquals": {
 "aws:ResourceTag/stage": "production"
 }
 }
 },
 {
 "Action": [
 "ssm:StartAutomationExecution"
],
 "Resource": [
 "arn:aws:ssm:*:111122223333:automation-execution/*"
],
 "Effect": "Allow"
 },
 {
 "Action": [
 "ssm:StopAutomationExecution",
 "ssm:GetAutomationExecution",
 "ssm:DescribeAutomationExecutions",
 "ssm:DescribeAutomationStepExecutions",
 "ssm:SendAutomationSignal"
],
 "Resource": [
 "arn:aws:ssm:*:111122223333:automation-execution/*"
],
 "Effect": "Allow"
 }
]
}

```

Esempio 4: consente a un utente di eseguire un documento di automazione quando viene fornito un parametro di tag specifico per l'esecuzione dell'automazione

L'esempio seguente di policy IAM concede le autorizzazioni a un utente per eseguire documenti di automazione quando viene fornito un parametro di tag specifico per l'esecuzione dell'automazione:

- Esegui il documento di automazione specificato nella policy. Il nome del documento è determinato dalla seguente voce:

```
arn:aws:ssm:*:111122223333:document/{{DocumentName}}
```

- È necessario fornire un parametro di tag specifico per l'esecuzione dell'automazione. Il parametro tag per la risorsa di esecuzione dell'automazione è determinato dalla voce seguente.

```
"aws:ResourceTag/stage": "production"
```

- Interrompi e invia segnali alle esecuzioni di automazione che hanno il tag specificato.
- Visualizza i dettagli sulle esecuzioni di automazione che hanno il tag specificato.
- Aggiungi il tag specificato alle risorse SSM.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Action": "ssm:StartAutomationExecution",
 "Effect": "Allow",
 "Resource": [
 "arn:aws:ssm:*:111122223333:document/{{DocumentName}}"
]
 },
 {
 "Action": [
 "ssm:StartAutomationExecution",
 "ssm:StopAutomationExecution",
 "ssm:GetAutomationExecution",
 "ssm:DescribeAutomationExecutions",
 "ssm:DescribeAutomationStepExecutions",
 "ssm:SendAutomationSignal"
],
 "Resource": [
 "arn:aws:ssm:*:111122223333:automation-execution/*"
],
 "Effect": "Allow",
 "Condition": {
```

```
 "StringEquals": {
 "aws:ResourceTag/environment": "beta"
 }
 },
 {
 "Action": "ssm:AddTagsToResource",
 "Effect": "Allow",
 "Resource": [
 "arn:aws:ssm:*:111122223333:automation-execution/*"
]
 }
]
```

Consentire ad Automation di adattarsi alle esigenze di simultaneità

Per impostazione predefinita, Automation consente di eseguire fino a 100 automazioni simultanee alla volta. Automation fornisce inoltre un'impostazione facoltativa da utilizzare per regolare automaticamente la quota di automazione simultanea. Grazie a questa impostazione, la quota di automazione simultanea può gestire fino a 500 automazioni simultanee, a seconda delle risorse disponibili.

#### Note

Se l'automazione chiama operazioni API, il dimensionamento adattivo agli obiettivi può comportare eccezioni di limitazione (della larghezza di banda della rete). Se si verificano eccezioni ricorrenti di limitazione (della larghezza di banda della rete) durante l'esecuzione di automazioni con la simultaneità adattiva attivata, potrebbe essere necessario richiedere un aumento delle quote per l'operazione API, se disponibile.

Per attivare la concorrenza adattiva utilizzando Console di gestione AWS

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Automazione.
3. Scegli la scheda Preferenze, quindi seleziona Modifica.
4. Seleziona la casella di controllo accanto a Attiva la simultaneità adattiva.



## 5. Selezionare Salva.

Per attivare la simultaneità adattiva utilizzando la riga di comando

- Apri AWS CLI o Strumenti per Windows PowerShell ed esegui il comando seguente per attivare la concorrenza adattiva per il tuo account nella regione richiedente.

### Linux & macOS

```
aws ssm update-service-setting \
 --setting-id /ssm/automation/enable-adaptive-concurrency \
 --setting-value True
```

### Windows

```
aws ssm update-service-setting ^
 --setting-id /ssm/automation/enable-adaptive-concurrency ^
 --setting-value True
```

### PowerShell

```
Update-SSMServiceSetting `
 -SettingId "/ssm/automation/enable-adaptive-concurrency" `
 -SettingValue "True"
```

Configurazione della ripetizione dei tentativi automatica per le operazioni di limitazione (della larghezza di banda della rete)

Esiste un limite nel numero di esecuzioni di automazione simultanee che eseguibili in ogni account. Il tentativo di eseguire numerose automazioni contemporaneamente in un account può causare problemi di limitazione (della larghezza di banda della rete). È possibile utilizzare la funzionalità di ripetizione dei tentativi di limitazione (della larghezza di banda della rete) automatica per configurare il relativo comportamento per i passaggi di automazione limitati.

La ripetizione dei tentativi di limitazione (della larghezza di banda della rete) automatica per le azioni di automazione offre un ambiente di esecuzione più resiliente per operazioni su larga scala. La funzionalità di ripetizione dei tentativi di limitazione (della larghezza di banda della rete) supporta tutte le [azioni di automazione](#) ad eccezione di `aws:executeScript`.

L'impostazione Throttling Retry funziona insieme alla proprietà `step.esistentemaxAttempts`. Quando entrambe sono configurate, il sistema tenta innanzitutto di ripetere i tentativi di limitazione (della larghezza di banda della rete) entro il limite di tempo specificato, quindi applica l'impostazione di `maxAttempts`, se il passaggio continua a fare errori.

Per configurare il throttling, riprova usando 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 Automazione.
3. Scegli la scheda Preferenze, quindi seleziona Modifica.
4. Nel campo Limite di tempo limitato per i tentativi, inserisci un valore compreso tra 0 e 3600 secondi. Questo specifica il tempo massimo durante il quale il sistema riprova un passaggio limitato.
5. Selezionare Salva.

Per configurare la ripetizione dei tentativi di limitazione (della larghezza di banda della rete) tramite la riga di comando

- Apri AWS CLI o Strumenti per Windows PowerShell ed esegui il comando seguente per configurare la limitazione dei tentativi per il tuo account nella regione richiedente.

#### Linux & macOS

```
aws ssm update-service-setting \
 --setting-id /ssm/automation/throttled-retry-time-limit \
 --setting-value 3600
```

#### Windows

```
aws ssm update-service-setting ^
 --setting-id /ssm/automation/throttled-retry-time-limit ^
 --setting-value 3600
```

#### PowerShell

```
Update-SSMServiceSetting `
 -SettingId "/ssm/automation/throttled-retry-time-limit" `
```

```
-SettingValue "3600"
```

## Implementazione dei controlli delle modifiche per Automazione

Per impostazione predefinita, Automation consente di utilizzare i runbook senza vincoli di data e ora. Integrando Automation con Change Calendar, puoi implementare i controlli delle modifiche a tutte le automazioni del tuo Account AWS. Con questa impostazione, i principali AWS Identity and Access Management (IAM) del tuo account possono eseguire automazioni solo durante i periodi di tempo consentiti. Per ulteriori informazioni sulle operazioni con Change Calendar, consulta la pagina [Utilizzo di Change Calendar](#).

### Attivazione dei controlli delle modifiche (console)

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Automazione.
3. Scegli la scheda Preferenze, quindi seleziona Modifica.
4. Seleziona la casella di controllo accanto a Attiva l'integrazione Change Calendar.
5. Nell'elenco a discesa Scegli un calendario delle modifiche, scegli il calendario delle modifiche che desideri che Automazione segua.
6. Scegli Salva.

## Esegui un'operazione automatizzata basata su Systems Manager Automation

Quando esegui un'automazione, per impostazione predefinita, l'automazione viene eseguita nel contesto dell'utente che ha avviato l'automazione. Ciò significa, ad esempio, che se l'utente dispone delle autorizzazioni di amministratore, l'automazione viene eseguita con le autorizzazioni di amministratore e con l'accesso completo alle risorse configurate dall'automazione. Come best practice di sicurezza, ti consigliamo di eseguire l'automazione utilizzando un ruolo del servizio IAM noto in questo caso come ruolo di assunzione configurato con la policy AmazonSSMAutomationRole gestita. Potrebbe essere necessario aggiungere ulteriori policy IAM al ruolo assunto per utilizzare diversi runbook. L'utilizzo di un ruolo di servizio IAM per l'esecuzione del servizio di automazione viene definito *delegated administration* (amministrazione delegata).

Quando utilizzi un ruolo di servizio, l'automazione può essere eseguita sulle risorse di AWS, ma l'utente che ha eseguito l'automazione ha un accesso limitato (o nessun accesso) a tali risorse. Ad

esempio, è possibile configurare un ruolo di servizio e utilizzarlo con il servizio di automazione per riavviare una o più istanze di Amazon Elastic Compute Cloud (Amazon EC2). L'automazione è uno strumento di AWS Systems Manager. L'automazione riavvia le istanze. Tuttavia, il ruolo del servizio non concede all'utente il permesso di accedere a tali istanze.

È possibile specificare un ruolo di servizio al runtime durante l'esecuzione di un'automazione oppure è possibile creare runbook personalizzati e specificare il ruolo di servizio direttamente nel runbook. Se specifichi un ruolo di servizio al runtime oppure in un runbook, il servizio viene eseguito nel contesto del ruolo di servizio specificato. Se non specifichi alcun ruolo di servizio, il sistema crea una sessione temporanea nel contesto dell'utente ed esegue l'automazione.

#### Note

È necessario specificare un ruolo di servizio per l'automazione con possibili tempi di esecuzione maggiori di 12 ore. Se si avvia un'automazione con tempi di esecuzione molto lunghi nel contesto di un utente, la sessione temporanea dell'utente scade dopo 12 ore.

L'amministrazione delegata garantisce livelli più elevati di sicurezza e il controllo delle risorse di AWS . Garantisce inoltre un'esperienza di controllo avanzata in quanto le operazioni vengono eseguite sulle risorse da un ruolo di servizio centralizzato anziché da più account IAM.

#### Prima di iniziare

Prima di completare le seguenti procedure, è necessario creare il ruolo del servizio IAM e configurare una relazione di fiducia per Automation. Per ulteriori informazioni, consulta [Processo 1: creazione di un ruolo di servizio per il servizio di automazione](#).

Le procedure riportate di seguito illustrano come utilizzare la console di Systems Manager o lo strumento a riga di comando preferito per eseguire un'automazione semplice.

#### Esecuzione di un'automazione semplice (console)

La procedura riportata di seguito illustra come utilizzare la console di Systems Manager per eseguire un'automazione semplice.

#### Per eseguire un'automazione semplice

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.

2. Nel pannello di navigazione, scegli Automazione, quindi Esegui automazione.
3. Nell'elenco Documento di automazione, scegli un runbook. Scegli una o più opzioni nel pannello Categorie di documenti per filtrare i documenti SSM in base al loro scopo. Per visualizzare un runbook di cui si è proprietari, scegliere la scheda Posseduto da me. Per visualizzare un runbook condiviso con l'account, scegliere la scheda Condiviso con me. Per visualizzare tutti i runbook, scegliere la scheda Tutti i documenti.

 Note

È possibile visualizzare informazioni su un runbook scegliendo il nome del runbook.

4. Nella sezione Dettagli documento verifica che l'opzione Versione documento sia impostata sulla versione che si desidera eseguire. Il sistema include le seguenti opzioni di versione:
  - Versione predefinita al runtime: scegli questa opzione se il runbook Automation viene aggiornato periodicamente e viene assegnata una nuova versione predefinita.
  - Ultima versione al runtime: scegli questa opzione se il runbook Automation viene aggiornato periodicamente e si desidera che venga eseguita la versione aggiornata più di recente.
  - 1 (predefinita): scegli questa opzione per eseguire la prima versione del documento (quella predefinita).
5. Scegli Avanti.
6. Nella sezione Execution Mode (Modalità esecuzione), scegliere Simple execution (Esecuzione semplice).
7. Nella sezione Input parameters (Parametri di input) specifica i parametri obbligatori. Facoltativamente, puoi scegliere un ruolo del servizio IAM dall'AutomationAssumeRoleelenco.
8. (Facoltativo) Scegli un CloudWatch allarme da applicare all'automazione per il monitoraggio. Se l'allarme entra in ALARM stato, l'automazione viene annullata e vengono eseguiti tutti onCancel i passaggi definiti. Se lo usi AWS CloudTrail, vedrai la chiamata StopAutomationExecution API nel tuo percorso. Per ulteriori informazioni, consulta [Configurazione delle automazioni per monitorare gli allarmi CloudWatch](#).
9. Scegliere Execute (Esegui).

La console visualizza lo stato dell'automazione. Se l'automazione non riesce, consulta [Risoluzione dei problemi di servizio di automazione di Systems Manager](#).

Una volta completata l'esecuzione di un'automazione, è possibile rieseguirila con gli stessi parametri o con parametri modificati. Per ulteriori informazioni, consulta [Ripetizione delle esecuzioni di automazione](#).

## Esecuzione di un'automazione semplice (riga di comando)

La procedura seguente descrive come utilizzare AWS CLI (su Linux o Windows) o AWS Strumenti per PowerShell eseguire una semplice automazione.

Per eseguire un'automazione semplice

1. Installa e configura il AWS CLI o il AWS Strumenti per PowerShell, se non l'hai già fatto.

Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

2. Esegui il comando seguente per avviare un'automazione semplice. Sostituisci ogni *example resource placeholder* con le tue informazioni.

### Linux & macOS

```
aws ssm start-automation-execution \
 --document-name runbook name \
 --parameters runbook parameters
```

### Windows

```
aws ssm start-automation-execution ^
 --document-name runbook name ^
 --parameters runbook parameters
```

### PowerShell

```
Start-SSMAutomationExecution `
 -DocumentName runbook name `
 -Parameter runbook parameters
```

Di seguito è riportato un esempio di utilizzo del runbook AWS-RestartEC2Instance per riavviare l'istanza EC2 specificata.

## Linux & macOS

```
aws ssm start-automation-execution \
 --document-name "AWS-RestartEC2Instance" \
 --parameters "InstanceId=i-02573cafcfEXAMPLE"
```

## Windows

```
aws ssm start-automation-execution ^
 --document-name "AWS-RestartEC2Instance" ^
 --parameters "InstanceId=i-02573cafcfEXAMPLE"
```

## PowerShell

```
Start-SSMAutomationExecution `
 -DocumentName AWS-RestartEC2Instance `
 -Parameter @{"InstanceId"="i-02573cafcfEXAMPLE"}
```

Il sistema restituisce informazioni simili alle seguenti.

## Linux & macOS

```
{
 "AutomationExecutionId": "4105a4fc-f944-11e6-9d32-0123456789ab"
}
```

## Windows

```
{
 "AutomationExecutionId": "4105a4fc-f944-11e6-9d32-0123456789ab"
}
```

## PowerShell

```
4105a4fc-f944-11e6-9d32-0123456789ab
```

3. Eseguire il comando seguente per recuperare lo stato dell'automazione.

## Linux & macOS

```
aws ssm describe-automation-executions \
 --filter "Key=ExecutionId,Values=4105a4fc-f944-11e6-9d32-0123456789ab"
```

## Windows

```
aws ssm describe-automation-executions ^
 --filter "Key=ExecutionId,Values=4105a4fc-f944-11e6-9d32-0123456789ab"
```

## PowerShell

```
Get-SSMAutomationExecutionList | `
 Where {$_.AutomationExecutionId -eq "4105a4fc-f944-11e6-9d32-0123456789ab"}
```

Il sistema restituisce informazioni simili alle seguenti.

## Linux & macOS

```
{
 "AutomationExecutionMetadataList": [
 {
 "AutomationExecutionStatus": "InProgress",
 "CurrentStepName": "stopInstances",
 "Outputs": {},
 "DocumentName": "AWS-RestartEC2Instance",
 "AutomationExecutionId": "4105a4fc-f944-11e6-9d32-0123456789ab",
 "DocumentVersion": "1",
 "ResolvedTargets": {
 "ParameterValues": [],
 "Truncated": false
 },
 "AutomationType": "Local",
 "Mode": "Auto",
 "ExecutionStartTime": 1564600648.159,
 "CurrentAction": "aws:changeInstanceState",
 "ExecutedBy": "arn:aws:sts::123456789012:assumed-role/Administrator/
Admin",
 "LogFile": "",
 "Targets": []
 }
]
}
```



```

 }
]
}

```

## Windows

```

{
 "AutomationExecutionMetadataList": [
 {
 "AutomationExecutionStatus": "InProgress",
 "CurrentStepName": "stopInstances",
 "Outputs": {},
 "DocumentName": "AWS-RestartEC2Instance",
 "AutomationExecutionId": "4105a4fc-f944-11e6-9d32-0123456789ab",
 "DocumentVersion": "1",
 "ResolvedTargets": {
 "ParameterValues": [],
 "Truncated": false
 },
 "AutomationType": "Local",
 "Mode": "Auto",
 "ExecutionStartTime": 1564600648.159,
 "CurrentAction": "aws:changeInstanceState",
 "ExecutedBy": "arn:aws:sts::123456789012:assumed-role/Administrator/Admin",
 "LogFile": "",
 "Targets": []
 }
]
}

```

## PowerShell

```

AutomationExecutionId : 4105a4fc-f944-11e6-9d32-0123456789ab
AutomationExecutionStatus : InProgress
AutomationType : Local
CurrentAction : aws:changeInstanceState
CurrentStepName : startInstances
DocumentName : AWS-RestartEC2Instance
DocumentVersion : 1
ExecutedBy : arn:aws:sts::123456789012:assumed-role/Administrator/Admin
ExecutionEndTime : 1/1/0001 12:00:00 AM

```

```
ExecutionStartTime : 7/31/2019 7:17:28 PM
FailureMessage :
LogFile :
MaxConcurrency :
MaxErrors :
Mode : Auto
Outputs : {}
ParentAutomationExecutionId :
ResolvedTargets :
 Amazon.SimpleSystemsManagement.Model.ResolvedTargets
Target :
TargetMaps : {}
TargetParameterName :
Targets : {}
```

## Ripetizione delle esecuzioni di automazione

È possibile eseguire nuovamente le esecuzioni di AWS Systems Manager automazione per ripetere attività con parametri identici o modificati. La funzionalità di riesecuzione consente di replicare in modo efficiente le esecuzioni di automazione senza ricreare manualmente le configurazioni di automazione, riducendo il sovraccarico operativo e i potenziali errori di configurazione.

Quando esegui nuovamente un'esecuzione di automazione, Systems Manager conserva i parametri del runbook originale, gli allarmi Amazon e i tag dell'esecuzione precedente. CloudWatch Il sistema crea una nuova esecuzione con il relativo nuovo ID e timestamp aggiornati. L'utente può ripetere qualsiasi tipo di esecuzione di automazione, incluse quelle semplici, quelle con controllo della velocità, quelle tra account e regioni e le esecuzioni manuali.

### Ripetere un'esecuzione di automazione (console)

La procedura riportata di seguito illustra come utilizzare la console di Systems Manager per ripetere un'esecuzione di automazione.

Per ripetere un'esecuzione di automazione dalla home page di Automazione

Apri la console all'indirizzo. AWS Systems Manager <https://console.aws.amazon.com/systems-manager/>

1. Nel pannello di navigazione, scegli Automazione.
2. Nell'elenco delle esecuzioni, seleziona quella che desideri ripetere.

3. Scegli Ripeti esecuzione.
4. Nella pagina del documento Esegui automazione, esamina i parametri precompilati, la modalità di esecuzione e la configurazione di destinazione dell'esecuzione originale.
5. (Facoltativo) Modifica i parametri, le destinazioni o le altre impostazioni necessarie per la ripetizione.
6. Scegli Esegui per avviare la ripetizione con un nuovo ID di esecuzione.

Per ripetere un'esecuzione di automazione dalla pagina dei dettagli dell'esecuzione

Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.

1. Nel pannello di navigazione, scegli Automazione.
2. Scegli l'ID di esecuzione dell'automazione che desideri ripetere.
3. Nella pagina dei dettagli dell'esecuzione, scegli Ripeti esecuzione.
4. Nella pagina del documento Esegui automazione, esamina i parametri precompilati, la modalità di esecuzione e la configurazione di destinazione dell'esecuzione originale.
5. (Facoltativo) Modifica i parametri, le destinazioni o le altre impostazioni necessarie per la ripetizione.
6. Scegli Esegui per avviare la ripetizione con un nuovo ID di esecuzione.

Per copiare un'esecuzione di automazione in una nuova esecuzione

Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.

1. Nel pannello di navigazione, scegli Automazione.
2. Scegli l'ID di esecuzione dell'automazione che desideri copiare.
3. Nella pagina dei dettagli di esecuzione, scegli Azioni, quindi scegli Copia su nuovo.
4. Nella pagina del documento Esegui automazione, esamina i parametri precompilati, la modalità di esecuzione e la configurazione di destinazione dell'esecuzione originale.
5. (Facoltativo) Modifica i parametri, le destinazioni o le altre impostazioni necessarie per la nuova esecuzione.
6. Scegli Esegui per avviare la nuova esecuzione.

## Esegui un'automazione che richiede approvazioni

Le procedure seguenti descrivono come utilizzare la AWS Systems Manager console e AWS Command Line Interface (AWS CLI) per eseguire un'automazione con approvazioni utilizzando un'esecuzione semplice. L'automazione usa l'operazione di automazione `aws:approve`, che sospende temporaneamente l'automazione finché i principali designati non approvano o rifiutano l'operazione. L'automazione viene eseguita nel contesto dell'utente corrente. Ciò significa che non è necessario configurare autorizzazioni IAM aggiuntive a condizione di disporre dell'autorizzazione necessaria per eseguire il runbook e qualsiasi operazione chiamata dal runbook. Se disponi delle autorizzazioni dell'amministratore in IAM, disponi già dell'autorizzazione per utilizzare questo runbook.

### Prima di iniziare

Oltre agli input standard richiesti dal runbook, l'`aws:approve` richiede i seguenti due parametri:

- un elenco di approvatori. L'elenco degli approvatori deve contenere almeno un approvatore sotto forma di un nome utente o di un ARN utente. Se vengono specificati più approvatori, all'interno del runbook deve essere specificato anche un numero minimo di approvazioni corrispondenti.
- Argomento ARN Amazon Simple Notification Service (Amazon SNS). Il nome dell'argomento Amazon SNS deve iniziare con `Automation`.

Questa procedura presuppone che tu abbia già creato un argomento Amazon SNS, necessario per inviare la richiesta di approvazione. Per ulteriori informazioni, consulta la pagina [Creazione di un argomento](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service.

### Esecuzione di un'automazione con approvatori (console)

#### Per eseguire un'automazione con approvatori

La procedura seguente descrive come utilizzare la console di Systems Manager per eseguire un'automazione con approvatori.

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Automazione, quindi Esegui automazione.
3. Nell'elenco Documento di automazione, scegli un runbook. Scegli una o più opzioni nel pannello Categorie di documenti per filtrare i documenti SSM in base al loro scopo. Per visualizzare un

runbook di cui si è proprietari, scegliere la scheda Posseduto da me. Per visualizzare un runbook condiviso con l'account, scegliere la scheda Condiviso con me. Per visualizzare tutti i runbook, scegliere la scheda Tutti i documenti.

 Note

È possibile visualizzare informazioni su un runbook scegliendo il nome del runbook.

4. Nella sezione Dettagli documento verifica che l'opzione Versione documento sia impostata sulla versione che si desidera eseguire. Il sistema include le seguenti opzioni di versione:
  - Versione predefinita al runtime: scegli questa opzione se il runbook Automation viene aggiornato periodicamente e viene assegnata una nuova versione predefinita.
  - Ultima versione al runtime: scegli questa opzione se il runbook Automation viene aggiornato periodicamente e si desidera che venga eseguita la versione aggiornata più di recente.
  - 1 (predefinita): scegli questa opzione per eseguire la prima versione del documento (quella predefinita).
5. Scegli Avanti.
6. Nella pagina Esecuzione documento di automazione, scegli Esecuzione semplice.
7. Nella sezione Parametri di input, specifica i parametri di input obbligatori.

Ad esempio, se hai scelto il **AWS-StartEC2InstanceWithApproval** runbook, devi specificare o scegliere gli ID di istanza per il `InstanceId` parametro.

8. Nella sezione Approvatori, specifica i nomi utenti o gli ARN utente degli approvatori per l'operazione di automazione.
9. Nella sezione SNSTopicARN, specifica l'ARN dell'argomento SNS da utilizzare per l'invio di una notifica di approvazione. Il nome dell'argomento SNS deve iniziare con Automation.
10. Facoltativamente, puoi scegliere un ruolo del servizio IAM dall'AutomationAssumeRoleelenco. Se hai come destinazione più di 100 account e Regioni, devi specificare `AWS-SystemsManager-AutomationAdministrationRole`.
11. Scegli Esegui automazione.

L'approvatore specificato riceve una notifica Amazon SNS con i dettagli per approvare o rifiutare l'automazione. Questa azione di approvazione è valida per 7 giorni dalla data di emissione e può essere emessa utilizzando la console Systems Manager o AWS Command Line Interface (AWS CLI).

Se si sceglie di approvarla, l'automazione continua a eseguire le fasi incluse nel runbook specificato. La console visualizza lo stato dell'automazione. Se l'automazione non riesce, consulta [Risoluzione dei problemi di servizio di automazione di Systems Manager](#).

Per approvare o rifiutare un servizio di automazione

1. Aprire la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegliere Automazione, quindi seleziona l'automazione eseguita nella procedura precedente.
3. Scegli Azioni, quindi scegli Approve/Deny.
4. Scegli Approva o Nega e, facoltativamente, aggiungi un commento.
5. Scegli Invia.

Esecuzione di un'automazione con approvatori (riga di comando)

La procedura seguente descrive come utilizzare AWS CLI (su Linux o Windows) o AWS Strumenti per PowerShell eseguire un'automazione con approvatori.

Per eseguire un'automazione con approvatori

1. Installa e configura il AWS CLI o il AWS Strumenti per PowerShell, se non l'hai già fatto.

Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

2. Esegui il seguente comando per eseguire un'automazione con approvatori. Sostituisci ogni *example resource placeholder* con le tue informazioni. Nella sezione del nome del documento, specifica un runbook che includa l'operazione di automazione `aws:approve`.

Per `Approvers`, specifica i nomi utente o gli ARN utente degli approvatori per l'operazione. Per `SNSTopic`, specifica l'ARN dell'argomento SNS da utilizzare per inviare una notifica di approvazione. Il nome dell'argomento Amazon SNS deve iniziare con `Automation`.

#### Note

I nomi specifici dei valori dei parametri per gli approvatori e l'argomento SNS dipendono dai valori specificati all'interno del runbook selezionato.

## Linux & macOS

```
aws ssm start-automation-execution \
 --document-name "AWS-StartEC2InstanceWithApproval" \
 --parameters
 "InstanceId=i-02573cafcfEXAMPLE,Approvers=arn:aws:iam::123456789012:role/
Administrator,SNSTopicArn=arn:aws:sns:region:123456789012:AutomationApproval"
```

## Windows

```
aws ssm start-automation-execution ^
 --document-name "AWS-StartEC2InstanceWithApproval" ^
 --parameters
 "InstanceId=i-02573cafcfEXAMPLE,Approvers=arn:aws:iam::123456789012:role/
Administrator,SNSTopicArn=arn:aws:sns:region:123456789012:AutomationApproval"
```

## PowerShell

```
Start-SSMAutomationExecution `
 -DocumentName AWS-StartEC2InstanceWithApproval `
 -Parameters @{
 "InstanceId"="i-02573cafcfEXAMPLE"
 "Approvers"="arn:aws:iam::123456789012:role/Administrator"
 "SNSTopicArn"="arn:aws:sns:region:123456789012:AutomationApproval"
 }
```

Il sistema restituisce informazioni simili alle seguenti.

## Linux & macOS

```
{
 "AutomationExecutionId": "df325c6d-b1b1-4aa0-8003-6cb7338213c6"
}
```

## Windows

```
{
 "AutomationExecutionId": "df325c6d-b1b1-4aa0-8003-6cb7338213c6"
```

```
}
```

## PowerShell

```
df325c6d-b1b1-4aa0-8003-6cb7338213c6
```

### Per approvare un'automazione

- Utilizza il comando seguente per approvare un'automazione. Sostituisci ogni *example resource placeholder* con le tue informazioni.

## Linux & macOS

```
aws ssm send-automation-signal \
 --automation-execution-id "df325c6d-b1b1-4aa0-8003-6cb7338213c6" \
 --signal-type "Approve" \
 --payload "Comment=your comments"
```

## Windows

```
aws ssm send-automation-signal ^
 --automation-execution-id "df325c6d-b1b1-4aa0-8003-6cb7338213c6" ^
 --signal-type "Approve" ^
 --payload "Comment=your comments"
```

## PowerShell

```
Send-SSMAutomationSignal `
 -AutomationExecutionId df325c6d-b1b1-4aa0-8003-6cb7338213c6 `
 -SignalType Approve `
 -Payload @{"Comment"="your comments"}
```

Se il comando va a buon fine, non viene generato output.

### Per rifiutare un'automazione

- Utilizza il comando seguente per rifiutare un'automazione. Sostituisci ogni *example resource placeholder* con le tue informazioni.



## Linux & macOS

```
aws ssm send-automation-signal \
 --automation-execution-id "df325c6d-b1b1-4aa0-8003-6cb7338213c6" \
 --signal-type "Deny" \
 --payload "Comment=your comments"
```

## Windows

```
aws ssm send-automation-signal ^
 --automation-execution-id "df325c6d-b1b1-4aa0-8003-6cb7338213c6" ^
 --signal-type "Deny" ^
 --payload "Comment=your comments"
```

## PowerShell

```
Send-SSMAutomationSignal `
 -AutomationExecutionId df325c6d-b1b1-4aa0-8003-6cb7338213c6 `
 -SignalType Deny `
 -Payload @{"Comment"="your comments"}
```

Se il comando va a buon fine, non viene generato output.

## Esegui operazioni automatizzate su larga scala

Con AWS Systems Manager Automation, puoi eseguire automazioni su una flotta di AWS risorse utilizzando obiettivi. Inoltre, è possibile controllare l'implementazione dell'automazione a livello di parco istanze specificando un valore di simultaneità e una soglia di errore. Le funzionalità di simultaneità e soglia di errore vengono definite collettivamente controlli di velocità. Il valore di simultaneità determina il numero di risorse autorizzate a eseguire l'automazione contemporaneamente. Automation permette di scegliere anche una modalità di simultaneità adattiva. La simultaneità adattiva dimensiona automaticamente la quota di automazione da 100 a 500 automazioni in esecuzione contemporaneamente. Una soglia di errore determina il numero di automazioni che possono avere esito negativo, superato il quale Systems Manager interrompe l'invio dell'automazione ad altre risorse.

Per ulteriori informazioni su simultaneità e soglie di errore, consulta [Controlla le automazioni su larga scala](#). Per ulteriori informazioni sulle destinazioni, consulta [Mappatura degli obiettivi per un'automazione](#).

Le procedure seguenti mostrano come attivare una simultaneità adattiva e come eseguire un'automazione con destinazioni e controlli di velocità utilizzando la console di Systems Manager e AWS Command Line Interface (AWS CLI).

Esecuzione di un'automazione con destinazioni e controlli di velocità (console)

La procedura seguente descrive come utilizzare la console di Systems Manager per eseguire un'automazione con destinazioni e controlli di velocità.

Per eseguire un'automazione con destinazioni e controlli di velocità

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Automazione, quindi Esegui automazione.
3. Nell'elenco Documento di automazione, scegli un runbook. Scegli una o più opzioni nel pannello Categorie di documenti per filtrare i documenti SSM in base al loro scopo. Per visualizzare un runbook di cui si è proprietari, scegliere la scheda Posseduto da me. Per visualizzare un runbook condiviso con l'account, scegliere la scheda Condiviso con me. Per visualizzare tutti i runbook, scegliere la scheda Tutti i documenti.

 Note

È possibile visualizzare informazioni su un runbook scegliendo il nome del runbook.

4. Nella sezione Dettagli documento verifica che l'opzione Versione documento sia impostata sulla versione che si desidera eseguire. Il sistema include le seguenti opzioni di versione:
  - Versione predefinita al runtime: scegli questa opzione se il runbook Automation viene aggiornato periodicamente e viene assegnata una nuova versione predefinita.
  - Ultima versione al runtime: scegli questa opzione se il runbook Automation viene aggiornato periodicamente e si desidera che venga eseguita la versione aggiornata più di recente.
  - 1 (predefinita): scegli questa opzione per eseguire la prima versione del documento (quella predefinita).
5. Scegli Avanti.

6. Nella sezione Execution Mode (Modalità di esecuzione) scegliere Rate Control (Controllo velocità). È necessario utilizzare questa modalità o Multi-account una regione se si desidera utilizzare gli obiettivi e i controlli delle tariffe.
7. Nella sezione Targets (Destinazioni) scegliere il modo in cui si desidera definire come destinazione le risorse di AWS in cui si desidera eseguire l'automazione. Queste opzioni sono obbligatorie.
  - a. Utilizza l'elenco Parameter (Parametro) per scegliere un parametro. Le voci nell'elenco Parameter (Parametro) sono determinate dai parametri presenti nel runbook del servizio di automazione selezionato all'inizio di questa procedura. È necessario scegliere un parametro per definire il tipo di risorsa su cui viene eseguito il flusso di lavoro del servizio di automazione.
  - b. Utilizza l'elenco Targets (Destinazioni) per scegliere come si desidera definire le risorse come destinazione.
    - i. Se è stato deciso di definire le risorse come destinazione mediante i valori dei parametri, inserire il valore del parametro per il parametro selezionato nella sezione Input parameters (Parametri di input).
    - ii. Se hai scelto di indirizzare le risorse utilizzando AWS Resource Groups, scegli il nome del gruppo dall'elenco dei gruppi di risorse.
    - iii. Se è stato deciso di definire le risorse come destinazione mediante i tag, inserire la chiave e (facoltativamente) il valore del tag nei campi disponibili. Scegli Add (Aggiungi).
    - iv. Se desideri eseguire un runbook di Automation su tutte le istanze del sistema operativo corrente Account AWS Regione AWS, scegli Tutte le istanze.
8. Nella sezione Input parameters (Parametri di input) specifica i parametri obbligatori. Facoltativamente, puoi scegliere un ruolo del servizio IAM dall'elenco. AutomationAssumeRole

 Note

Potrebbe non essere necessario scegliere alcune delle opzioni nella sezione Input parameters (Parametri di input). Ciò è dovuto al fatto che le risorse sono state definite come destinazione mediante i tag o un gruppo di risorse. Ad esempio, se è stato scelto il runbook AWS-RestartEC2Instance, non sarà necessario specificare o scegliere gli ID di istanza nella sezione Input parameters (Parametri di input). L'esecuzione dell'automazione individua le istanze da riavviare utilizzando i tag o i gruppi di risorse specificati.

9. Utilizza le opzioni nella sezione Rate control per limitare il numero di AWS risorse che possono eseguire l'automazione all'interno di ciascuna coppia account-regione.

Nella sezione Concurrency (Simultaneità) scegliere un'opzione:

- Scegliere Targets (Destinazioni) per inserire un numero assoluto di destinazioni che possono eseguire contemporaneamente il flusso di lavoro del servizio di automazione.
- Scegliere Percentage (Percentuale) per inserire la percentuale della serie di destinazioni che può eseguire contemporaneamente il flusso di lavoro del servizio di automazione.

10. Nella sezione Error threshold (Soglia di errore). scegliere un'opzione:

- Scegliere errors (errori) per inserire un numero assoluto di errori consentiti, raggiunto il quale il servizio di automazione interrompe l'invio del flusso di lavoro alle altre risorse.
- Scegli percentage (percentuale) per inserire una percentuale di errori consentiti, raggiunta la quale il servizio di automazione interrompe l'invio del flusso di lavoro alle altre risorse.

11. (Facoltativo) Scegli un CloudWatch allarme da applicare all'automazione per il monitoraggio. Se l'allarme entra in ALARM stato, l'automazione viene annullata e vengono eseguiti tutti onCancel i passaggi definiti. Se lo usi AWS CloudTrail, vedrai la chiamata StopAutomationExecution API nel tuo percorso. Per ulteriori informazioni, consulta [Configurazione delle automazioni per monitorare gli allarmi CloudWatch](#).

12. Scegliere Execute (Esegui).

Per visualizzare le automazioni avviate dall'automazione del controllo della velocità, nel pannello di navigazione scegliere Automation (Automazione), quindi selezionare Show child automations (Mostra automazioni figlio).

Una volta completata l'esecuzione di un'automazione, è possibile rieseguirla con gli stessi parametri o con parametri modificati. Per ulteriori informazioni, consulta [Ripetizione delle esecuzioni di automazione](#).

Esecuzione di un'automazione con destinazioni e controlli di velocità (riga di comando)

La procedura seguente descrive come utilizzare AWS CLI (su Linux o Windows) o AWS Strumenti per PowerShell eseguire un'automazione con obiettivi e controlli di frequenza.

Per eseguire un'automazione con destinazioni e controlli di velocità

1. Installa e configura il AWS CLI o il AWS Strumenti per PowerShell, se non l'hai già fatto.

Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

2. Eseguire il comando seguente per visualizzare un elenco di documenti.

#### Linux & macOS

```
aws ssm list-documents
```

#### Windows

```
aws ssm list-documents
```

#### PowerShell

```
Get-SSMDocumentList
```

Prendi nota del nome del runbook che desideri utilizzare.

3. Esegui il comando seguente per visualizzare i dettagli sul runbook. *runbook name* Sostituisci il nome del runbook di cui desideri visualizzare i dettagli. Inoltre, prendi nota di un nome di parametro (ad esempio, InstanceId) che desideri utilizzare per l'opzione `--target-parameter-name`. Questo parametro determina il tipo di risorsa su cui viene eseguita l'automazione.

#### Linux & macOS

```
aws ssm describe-document \
 --name runbook name
```

#### Windows

```
aws ssm describe-document ^
 --name runbook name
```

#### PowerShell

```
Get-SSMDocumentDescription `
```

-Name *runbook name*

4. Crea un comando che utilizza le opzioni relative alle destinazioni e ai controlli di velocità da eseguire. Sostituisci ogni *example resource placeholder* con le tue informazioni.

## Definizione di destinazioni mediante tag

### Linux & macOS

```
aws ssm start-automation-execution \
 --document-name runbook name \
 --targets Key=tag:key name,Values=value \
 --target-parameter-name parameter name \
 --parameters "input parameter name=input parameter value,input parameter 2
name=input parameter 2 value" \
 --max-concurrency 10 \
 --max-errors 25%
```

### Windows

```
aws ssm start-automation-execution ^
 --document-name runbook name ^
 --targets Key=tag:key name,Values=value ^
 --target-parameter-name parameter name ^
 --parameters "input parameter name=input parameter value,input parameter 2
name=input parameter 2 value" ^
 --max-concurrency 10 ^
 --max-errors 25%
```

### PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "tag:key name"
$Targets.Values = "value"

Start-SSMAutomationExecution `
 DocumentName "runbook name" `
 -Targets $Targets `
 -TargetParameterName "parameter name" `
 -Parameter @{"input parameter name"="input parameter value";"input parameter
2 name"="input parameter 2 value"} `
 -MaxConcurrency "10" `
```

```
-MaxError "25%"
```

## Definizione di destinazioni mediante valori di parametro

### Linux & macOS

```
aws ssm start-automation-execution \
 --document-name runbook name \
 --targets Key=ParameterValues,Values=value,value 2,value 3 \
 --target-parameter-name parameter name \
 --parameters "input parameter name=input parameter value" \
 --max-concurrency 10 \
 --max-errors 25%
```

### Windows

```
aws ssm start-automation-execution ^
 --document-name runbook name ^
 --targets Key=ParameterValues,Values=value,value 2,value 3 ^
 --target-parameter-name parameter name ^
 --parameters "input parameter name=input parameter value" ^
 --max-concurrency 10 ^
 --max-errors 25%
```

### PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "ParameterValues"
$Targets.Values = "value","value 2","value 3"

Start-SSMAutomationExecution `
 -DocumentName "runbook name" `
 -Targets $Targets `
 -TargetParameterName "parameter name" `
 -Parameter @{"input parameter name"="input parameter value"} `
 -MaxConcurrency "10" `
 -MaxError "25%"
```

## Targeting utilizzando AWS Resource Groups

## Linux & macOS

```
aws ssm start-automation-execution \
 --document-name runbook name \
 --targets Key=ResourceGroup,Values=Resource group name \
 --target-parameter-name parameter name \
 --parameters "input parameter name=input parameter value" \
 --max-concurrency 10 \
 --max-errors 25%
```

## Windows

```
aws ssm start-automation-execution ^
 --document-name runbook name ^
 --targets Key=ResourceGroup,Values=Resource group name ^
 --target-parameter-name parameter name ^
 --parameters "input parameter name=input parameter value" ^
 --max-concurrency 10 ^
 --max-errors 25%
```

## PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "ResourceGroup"
$Targets.Values = "Resource group name"

Start-SSMAutomationExecution `
 -DocumentName "runbook name" `
 -Targets $Targets `
 -TargetParameterName "parameter name" `
 -Parameter @{"input parameter name"="input parameter value"} `
 -MaxConcurrency "10" `
 -MaxError "25%"
```

Rivolto a tutte le istanze Amazon EC2 nell'attuale e Account AWS Regione AWS

## Linux & macOS

```
aws ssm start-automation-execution \
 --document-name runbook name \
 --target-parameter-name parameter name \
 --parameters "input parameter name=input parameter value" \
 --max-concurrency 10 \
 --max-errors 25%
```



```
--targets "Key=AWS::EC2::Instance,Values=*" \
--target-parameter-name instanceId \
--parameters "input parameter name=input parameter value" \
--max-concurrency 10 \
--max-errors 25%
```

## Windows

```
aws ssm start-automation-execution ^
--document-name runbook name ^
--targets Key=AWS::EC2::Instance,Values=* ^
--target-parameter-name instanceId ^
--parameters "input parameter name=input parameter value" ^
--max-concurrency 10 ^
--max-errors 25%
```

## PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "AWS::EC2::Instance"
$Targets.Values = "*"

Start-SSMAutomationExecution `
-DocumentName "runbook name" `
-Targets $Targets `
-TargetParameterName "instanceId" `
-Parameter @{"input parameter name"="input parameter value"} `
-MaxConcurrency "10" `
-MaxError "25%"
```

Il comando restituisce un ID di esecuzione. Copia questo ID negli appunti. È possibile usare questo ID per visualizzare lo stato dell'automazione.

## Linux & macOS

```
{
 "AutomationExecutionId": "a4a3c0e9-7efd-462a-8594-01234EXAMPLE"
}
```

## Windows

```
{
 "AutomationExecutionId": "a4a3c0e9-7efd-462a-8594-01234EXAMPLE"
}
```

## PowerShell

```
a4a3c0e9-7efd-462a-8594-01234EXAMPLE
```

5. Esegui il comando seguente per visualizzare l'automazione. Sostituisci ogni *automation execution ID* con le tue informazioni.

## Linux & macOS

```
aws ssm describe-automation-executions \
 --filter Key=ExecutionId,Values=automation execution ID
```

## Windows

```
aws ssm describe-automation-executions ^
 --filter Key=ExecutionId,Values=automation execution ID
```

## PowerShell

```
Get-SSMAutomationExecutionList | `
 Where {$_.AutomationExecutionId -eq "automation execution ID"}
```

6. Eseguire il comando seguente per visualizzare i dettagli relativi al progresso dell'automazione. Sostituisci ogni *automation execution ID* con le tue informazioni.

## Linux & macOS

```
aws ssm get-automation-execution \
 --automation-execution-id automation execution ID
```

## Windows

```
aws ssm get-automation-execution ^
```

```
--automation-execution-id automation execution ID
```

## PowerShell

```
Get-SSMAutomationExecution `
-AutomationExecutionId automation execution ID
```

Il sistema restituisce informazioni simili alle seguenti.

## Linux & macOS

```
{
 "AutomationExecution": {
 "StepExecutionsTruncated": false,
 "AutomationExecutionStatus": "Success",
 "MaxConcurrency": "1",
 "Parameters": {},
 "MaxErrors": "1",
 "Outputs": {},
 "DocumentName": "AWS-StopEC2Instance",
 "AutomationExecutionId": "a4a3c0e9-7efd-462a-8594-01234EXAMPLE",
 "ResolvedTargets": {
 "ParameterValues": [
 "i-02573cafcfEXAMPLE"
],
 "Truncated": false
 },
 "ExecutionEndTime": 1564681619.915,
 "Targets": [
 {
 "Values": [
 "DEV"
],
 "Key": "tag:ENV"
 }
],
 "DocumentVersion": "1",
 "ExecutionStartTime": 1564681576.09,
 "ExecutedBy": "arn:aws:sts::123456789012:assumed-role/Administrator/
Admin",
 "StepExecutions": [
 {
```

```

 "Inputs": {
 "InstanceId": "i-02573cafcfEXAMPLE"
 },
 "Outputs": {},
 "StepName": "i-02573cafcfEXAMPLE",
 "ExecutionEndTime": 1564681619.093,
 "StepExecutionId": "86c7b811-3896-4b78-b897-01234EXAMPLE",
 "ExecutionStartTime": 1564681576.836,
 "Action": "aws:executeAutomation",
 "StepStatus": "Success"
 }
],
"TargetParameterName": "InstanceId",
"Mode": "Auto"
}
}

```

## Windows

```

{
 "AutomationExecution": {
 "StepExecutionsTruncated": false,
 "AutomationExecutionStatus": "Success",
 "MaxConcurrency": "1",
 "Parameters": {},
 "MaxErrors": "1",
 "Outputs": {},
 "DocumentName": "AWS-StopEC2Instance",
 "AutomationExecutionId": "a4a3c0e9-7efd-462a-8594-01234EXAMPLE",
 "ResolvedTargets": {
 "ParameterValues": [
 "i-02573cafcfEXAMPLE"
],
 "Truncated": false
 },
 "ExecutionEndTime": 1564681619.915,
 "Targets": [
 {
 "Values": [
 "DEV"
],
 "Key": "tag:ENV"
 }
]
 }
}

```

```

],
 "DocumentVersion": "1",
 "ExecutionStartTime": 1564681576.09,
 "ExecutedBy": "arn:aws:sts::123456789012:assumed-role/Administrator/
Admin",
 "StepExecutions": [
 {
 "Inputs": {
 "InstanceId": "i-02573cafcfEXAMPLE"
 },
 "Outputs": {},
 "StepName": "i-02573cafcfEXAMPLE",
 "ExecutionEndTime": 1564681619.093,
 "StepExecutionId": "86c7b811-3896-4b78-b897-01234EXAMPLE",
 "ExecutionStartTime": 1564681576.836,
 "Action": "aws:executeAutomation",
 "StepStatus": "Success"
 }
],
 "TargetParameterName": "InstanceId",
 "Mode": "Auto"
 }
}

```

## PowerShell

```

AutomationExecutionId : a4a3c0e9-7efd-462a-8594-01234EXAMPLE
AutomationExecutionStatus : Success
CurrentAction :
CurrentStepName :
DocumentName : AWS-StopEC2Instance
DocumentVersion : 1
ExecutedBy : arn:aws:sts::123456789012:assumed-role/
Administrator/Admin
ExecutionEndTime : 8/1/2019 5:46:59 PM
ExecutionStartTime : 8/1/2019 5:46:16 PM
FailureMessage :
MaxConcurrency : 1
MaxErrors : 1
Mode : Auto
Outputs : {}
Parameters : {}
ParentAutomationExecutionId :

```

```
ProgressCounters :
ResolvedTargets :
 Amazon.SimpleSystemsManagement.Model.ResolvedTargets
StepExecutions : {i-02573cafcfEXAMPLE}
StepExecutionsTruncated : False
Target :
TargetLocations : {}
TargetMaps : {}
TargetParameterName : InstanceId
Targets : {tag:Name}
```

#### Note

È inoltre possibile monitorare lo stato dell'automazione nella console. Nell'elenco delle Esecuzioni di automazione, scegli l'automazione appena eseguita e quindi scegli la scheda Fasi di esecuzione. In questa scheda viene mostrato lo stato delle operazioni di automazione.

## Mappatura degli obiettivi per un'automazione

Utilizza il parametro `Targets` per definire velocemente quali risorse possono essere destinate a un'automazione. Ad esempio, se vuoi eseguire un'automazione che riavvii le istanze gestite, anziché selezionare manualmente decine di ID di istanza nella console o digitarli in un comando, puoi definire le istanze come destinazione specificando i tag di Amazon Elastic Compute Cloud (Amazon EC2) con il parametro `Targets`.

Quando esegui un'automazione che utilizza un obiettivo, AWS Systems Manager crea un'automazione figlio per ogni destinazione. Ad esempio, se come destinazione utilizzi i volumi di Amazon Elastic Block Store (Amazon EBS) mediante la specifica di tag e se tali tag restituiscono 100 volumi di Amazon EBS, Systems Manager crea 100 automazioni figlio. L'automazione padre risulta completa quando tutte le automazioni figlio raggiungono lo stato finale.

#### Note

Qualsiasi opzione `input parameters` specificata nel runtime (tempo di esecuzione) (nella sezione `Input parameters` (Parametri di input) della console oppure utilizzando l'opzione

`parameters` nella riga di comando) viene elaborata automaticamente da tutte le automazioni figlio.

Per definire le risorse come destinazione per un'automazione, puoi usare i tag, Resource Groups, e i valori dei parametri. Puoi inoltre utilizzare l'opzione `TargetMaps` per utilizzare come destinazione più valori di parametro nella riga di comando o in un file. La sezione seguente descrive con maggiore dettaglio ciascuna di queste opzioni.

### Definizione di un tag come destinazione

Puoi specificare un singolo tag come destinazione di un'automazione. Molte risorse di AWS supportano i tag, tra cui istanze di Amazon Elastic Compute Cloud (Amazon EC2) e di Amazon Relational Database Service (Amazon RDS), volumi e snapshot di Amazon Elastic Block Store (Amazon EBS), Resource Groups e bucket Amazon Simple Storage Service (Amazon S3), per citarne alcune. Puoi eseguire rapidamente l'automazione sulle tue AWS risorse scegliendo come target un tag. Un tag è una coppia chiave-valore, ad esempio: `Linux o. Operating_System` `Department:Finance` Se assigni un nome specifico a una risorsa, puoi anche possibile utilizzare la parola "Nome" come chiave e il nome della risorsa come valore.

Quando specifichi un tag come destinazione di un'automazione, devi specificare anche un parametro di destinazione. Il parametro di destinazione utilizza l'opzione `TargetParameterName`. Scegliendo un parametro di destinazione, definisci il tipo di risorsa su cui viene eseguita l'automazione. Il parametro di destinazione specificato con il tag deve essere un parametro valido definito nel runbook. Ad esempio, se vuoi definire come destinazione molte istanze di EC2 utilizzando i tag, devi scegliere il parametro di destinazione `InstanceId`. Quando scegli questo parametro, definisci le instances (istanze) come il tipo di risorsa per l'automazione. Durante la creazione di un runbook personalizzato è necessario specificare, per Tipo di distanza, il valore `/AWS::EC2::Instance` per garantire che vengano utilizzate solo le istanze. Altrimenti, verranno definite come destinazione tutte le risorse con lo stesso tag. Quando definisci come destinazione le istanze con un tag, potrebbero essere incluse anche le istanze terminate.

Lo screenshot seguente utilizza il runbook di `AWS-DetachEBSVolume`. Il parametro di destinazione logico è `VolumeId`.

**Targets**  
Select the targets on which the automation document will run.

**Parameter**  
Choose the parameter that will define how your automation will branch out.  

Volumeld

**Targets**  

Tags

**Tags**  
Specify a tag key/value pair.  

Finance

Test Env

Add

  
Enter a tag key and optional value applied to the instances you want to target, and then choose Add.

Il runbook di `AWS-DetachEBSVolume` include anche una proprietà speciale chiamata Tipo di destinazione, impostata su `/AWS::EC2::Volume`. Ciò significa che se la coppia tag-chiave `Finance:TestEnv` restituisce tipi diversi di risorse, (ad esempio istanze di EC2, volumi di Amazon EBS e snapshot di Amazon EBS), verranno utilizzati solo i volumi di Amazon EBS.

### Important

I nomi dei parametri di destinazione fanno distinzione tra maiuscole e minuscole. Se esegui automazioni utilizzando AWS Command Line Interface (AWS CLI) o AWS Tools for Windows PowerShell, devi inserire il nome del parametro di destinazione esattamente come definito nel runbook. In caso contrario, il sistema restituisce un errore di `InvalidAutomationExecutionParametersException`. Puoi utilizzare l'operazione [DescribeDocument](#) API per visualizzare le informazioni sui parametri di destinazione disponibili in un runbook specifico. Di seguito è riportato un esempio di comando di AWS CLI che fornisce informazioni su documento di `AWS-DeleteSnapshot` non valido.

```
aws ssm describe-document \
 --name AWS-DeleteSnapshot
```

Ecco alcuni AWS CLI comandi di esempio che indirizzano le risorse utilizzando un tag.

Esempio 1: definizione di un tag come destinazione mediante l'uso di una coppia chiave-valore per riavviare le istanze Amazon EC2

Questo esempio riavvia tutte le istanze Amazon EC2 contrassegnate con una chiave `Department` e un valore di `HumanResources`. Il parametro `target` utilizza il `InstanceId` parametro del runbook.

Servizio di automazione

1212



L'esempio utilizza un parametro aggiuntivo per eseguire l'automazione utilizzando un ruolo di servizio di automazione, definito anche ruolo presunto.

```
aws ssm start-automation-execution \
 --document-name AWS-RestartEC2Instance \
 --targets Key=tag:Department,Values=HumanResources \
 --target-parameter-name InstanceId \
 --parameters "AutomationAssumeRole=arn:aws:iam::111122223333:role/
AutomationServiceRole"
```

Esempio 2: definizione di un tag come destinazione mediante l'uso di una coppia chiave-valore per eliminare gli snapshot di Amazon EBS

L'esempio seguente utilizza il runbook di AWS-DeleteSnapshot per eliminare tutti gli snapshot con la chiave Nome e il valore January2018Backups. Il parametro target utilizza il VolumeId parametro.

```
aws ssm start-automation-execution \
 --document-name AWS-DeleteSnapshot \
 --targets Key=tag:Name,Values=January2018Backups \
 --target-parameter-name VolumeId
```

## Definizione del target AWS Resource Groups

È possibile specificare un singolo gruppo di AWS risorse come destinazione di un'automazione. Systems Manager crea un'automazione figlio per ogni oggetto nel gruppo di risorse di destinazione.

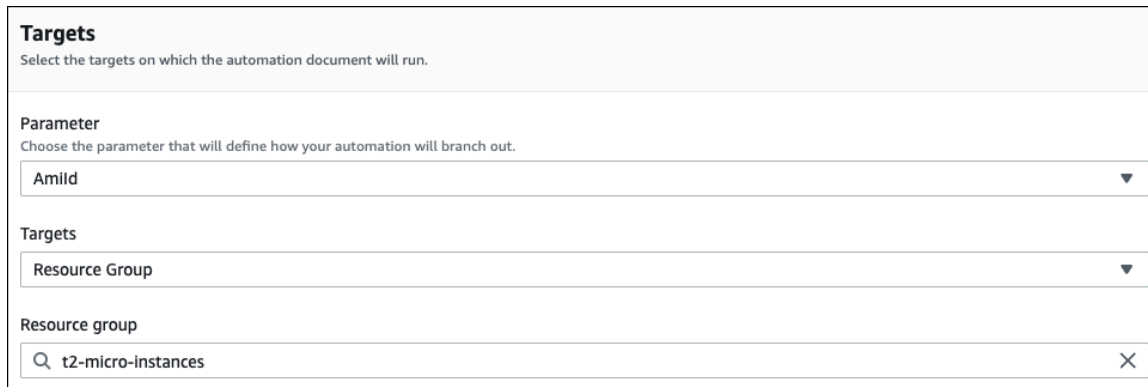
Si supponga, ad esempio, che il nome del Resource Groups sia PatchedAMIs. Questo gruppo di risorse include un elenco di 25 Amazon Machine Images (AMIs) Windows a cui vengono regolarmente applicate patch. Se esegui un'automazione che utilizza il runbook di AWS-CreateManagedWindowsInstance e che ha questo gruppo di risorse come destinazione, Systems Manager creerà un'automazione figlio per ciascuna delle 25 AMIs. Ciò significa che definendo il gruppo di risorse PatchedAMIs come destinazione, l'automazione crea 25 istanze da un elenco di AMIs a cui sono state applicate patch. L'automazione padre risulta completa quando tutte le automazioni figlio hanno ultimato l'elaborazione o hanno raggiunto lo stato finale.

Il AWS CLI comando seguente si applica all'esempio di PatchAMIs Resource Group. Il comando accetta il Amild parametro dell'opzione. --target-parameter-name Il comando non include un parametro aggiuntivo che definisce il tipo di istanza da creare da ciascuna AMI. Il runbook di AWS-CreateManagedWindowsInstance usa per impostazione predefinita il tipo di istanza t2.medium;

per tale motivo, questo comando crea 25 istanze t2.medium di Amazon EC2 instances per Windows Server.

```
aws ssm start-automation-execution \
 --document-name AWS-CreateManagedWindowsInstance \
 --targets Key=ResourceGroup,Values=PatchedAMIs \
 --target-parameter-name AmiId
```

La seguente console di esempio utilizza un gruppo di risorse denominato t2-micro-instances.



**Targets**  
Select the targets on which the automation document will run.

**Parameter**  
Choose the parameter that will define how your automation will branch out.

AmiId ▼

**Targets**

Resource Group ▼

Resource group

t2-micro-instances X

### Definizione dei valori di parametro come destinazione

È anche possibile definire come destinazione un valore di parametro. A tale scopo, devi specificare `ParameterValues` come chiave e quindi inserire il valore specifico di risorsa in cui vuoi eseguire l'automazione. Se specifichi più valori, Systems Manager esegue un'automazione figlio su ciascun valore specificato.

Supponiamo, ad esempio, che il runbook includa un parametro `InstanceId`. Se definisci i valori del parametro `InstanceId` come destinazione quando esegui l'automazione, Systems Manager esegue un'automazione figlio per ogni valore di ID di istanza specificato. L'automazione padre risulta completa quando l'automazione termina l'esecuzione di ciascuna istanza specificata oppure se l'automazione ha esito negativo. Puoi definire come destinazione un massimo di 50 valori di parametro.

Nell'esempio seguente viene utilizzato il runbook di `AWS-CreateImage`. Il nome del parametro di destinazione specificato è `InstanceId`. La chiave utilizza `ParameterValues`. I valori sono due ID di istanza di Amazon EC2. Questo comando crea un'automazione per ogni istanza, che genera un'AMI da ciascuna istanza.

```
aws ssm start-automation-execution
```

```
--document-name AWS-CreateImage \
--target-parameter-name InstanceId \
--targets Key=ParameterValues,Values=i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE
```

#### Note

AutomationAssumeRole non è un parametro valido. Non scegliere questo elemento quando si esegue un'automazione che definisce un valore di parametro come destinazione.

## Definizione delle mappe di valori di parametro come destinazione

L'opzione TargetMaps potenzia la capacità di definire ParameterValues come destinazione. Puoi inserire una serie di valori di parametro utilizzando TargetMaps nella riga di comando. Puoi infine specificare un massimo di 50 valori di parametro nella riga di comando. Per eseguire comandi che specificano più di 50 valori di parametro, puoi inserire i valori in un file in formato JSON. Potrai quindi richiamare il file dalla riga di comando.

#### Note

L'opzione TargetMaps non è supportata nella console.

Usa il seguente formato per specificare più valori di parametro mediante l'opzione TargetMaps in un comando. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
aws ssm start-automation-execution \
 --document-name runbook name \
 --target-maps "parameter=value, parameter 2=value, parameter 3=value" "parameter
4=value, parameter 5=value, parameter 6=value"
```

Se vuoi immettere più di 50 valori di parametro per l'opzione TargetMaps, specifica i valori in un file utilizzando il seguente formato JSON. L'utilizzo di un file in formato JSON migliora inoltre la leggibilità quando vengono specificati più valori di parametro.

```
[

 {"parameter": "value", "parameter 2": "value", "parameter 3": "value"},
```

```
 {"parameter 4": "value", "parameter 5": "value", "parameter 6": "value"}
]
```

Salva il file con l'estensione .json. Puoi chiamare il file utilizzando il comando seguente. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
aws ssm start-automation-execution \
 --document-name runbook name \
 --parameters input parameters \
 --target-maps path to file/file name.json
```

Puoi inoltre scaricare il file da un bucket Amazon Simple Storage Service (Amazon S3), a condizione che tu disponga dell'autorizzazione necessaria per leggere i dati dal bucket. Utilizza il seguente formato di comando. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
aws ssm start-automation-execution \
 --document-name runbook name \
 --target-maps http://amzn-s3-demo-bucket.s3.amazonaws.com/file_name.json
```

Ecco uno scenario di esempio che illustra l'opzione TargetMaps. In questo scenario, un utente desidera creare istanze di Amazon EC2 di vari tipi da AMIs diverse. Per eseguire questa attività, l'utente crea un runbook denominato AMI\_Testing. Questo runbook definisce due parametri di input: `instanceType` e `imageId`.

```
{
 "description": "AMI Testing",
 "schemaVersion": "0.3",
 "assumeRole": "{{assumeRole}}",
 "parameters": {
 "assumeRole": {
 "type": "String",
 "description": "Role under which to run the automation",
 "default": ""
 },
 "instanceType": {
 "type": "String",
 "description": "Type of EC2 Instance to launch for this test"
 },
 "imageId": {
```

```
 "type": "String",
 "description": "Source AMI id from which to run instance"
 },
 "mainSteps": [
 {
 "name": "runInstances",
 "action": "aws:runInstances",
 "maxAttempts": 1,
 "onFailure": "Abort",
 "inputs": {
 "ImageId": "{{imageId}}",
 "InstanceType": "{{instanceType}}",
 "MinInstanceCount": 1,
 "MaxInstanceCount": 1
 }
 }
],
 "outputs": [
 "runInstances.InstanceIds"
]
}
```

L'utente specifica quindi i seguenti valori di parametro di destinazione in un file denominato `AMI_instance_types.json`.

```
[
 {
 "instanceType" : ["t2.micro"],
 "imageId" : ["ami-b70554c8"]
 },
 {
 "instanceType" : ["t2.small"],
 "imageId" : ["ami-b70554c8"]
 },
 {
 "instanceType" : ["t2.medium"],
 "imageId" : ["ami-cfe4b2b0"]
 },
 {
 "instanceType" : ["t2.medium"],
 "imageId" : ["ami-cfe4b2b0"]
 },
]
```

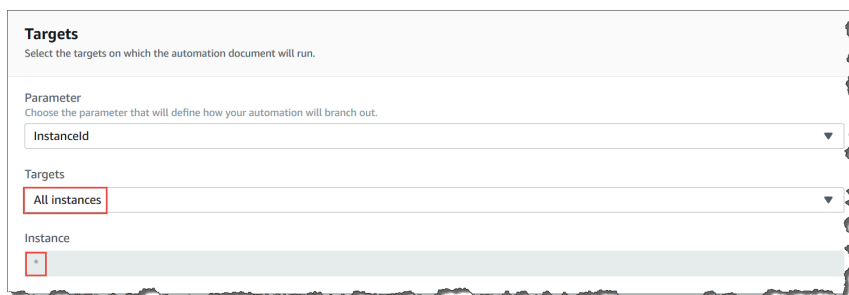
```
{
 "instanceType" : ["t2.medium"],
 "imageId" : ["ami-cfe4b2b0"]
}
```

L'utente può eseguire l'automazione e creare le cinque istanze di EC2 definite nel file `AMI_instance_types.json` con il comando seguente.

```
aws ssm start-automation-execution \
 --document-name AMI_Testing \
 --target-parameter-name imageId \
 --target-maps file:///home/TestUser/workspace/runinstances/AMI_instance_types.json
```

## Definizione di tutte le istanze Amazon EC2 come destinazione

Puoi eseguire un'automazione su tutte le istanze di Amazon EC2 nella versione corrente Account AWS e Regione AWS selezionando **Tutte le istanze** nell'elenco **Targets**. Ad esempio, se desideri riavviare tutte le istanze di Amazon EC2, tua Account AWS e corrente Regione AWS, puoi scegliere il **AWS-RestartEC2Instance** runbook e quindi scegliere **Tutte le istanze** dall'elenco **Targets**.



**Targets**  
Select the targets on which the automation document will run.

**Parameter**  
Choose the parameter that will define how your automation will branch out.

InstanceId

**Targets**  
All instances

Instance  
\*

Dopo aver scelto **Tutte le istanze**, Systems Manager popola il campo **Istanza** con un asterisco (\*) e rende il campo non disponibile per le modifiche (il campo è disabilitato). Systems Manager rende inoltre il **InstanceId** campo nel campo dei parametri di input non disponibile per le modifiche. Rendi questi campi non disponibili per le modifiche è un comportamento previsto se scegli di definire tutte le istanze come destinazione.

## Controlla le automazioni su larga scala

Puoi controllare l'implementazione di un'automazione su un parco di AWS risorse specificando un valore di concorrenza e una soglia di errore. Le caratteristiche di simultaneità e soglia di errore vengono collettivamente definite controlli di velocità.

## Concurrency (Simultaneità)

La simultaneità permette di specificare il numero di risorse autorizzate a eseguire un'automazione contemporaneamente. La simultaneità consente quindi di limitare l'impatto o il tempo di inattività a livello di risorse durante l'elaborazione di un'automazione. Puoi specificare un numero assoluto di risorse, ad esempio 20, oppure una percentuale della serie di destinazione, ad esempio 10%.

Il sistema di accodamento invia l'automazione a una singola risorsa e attende il completamento della chiamata iniziale prima di inviare l'automazione ad altre due risorse. Il sistema invia in modo esponenziale l'automazione a più risorse fino al raggiungimento del valore definito per la simultaneità.

## Soglie di errore

Utilizza una soglia di errore per specificare quante automazioni possono fallire prima di AWS Systems Manager interrompere l'invio dell'automazione ad altre risorse. Puoi specificare un numero assoluto di errori, ad esempio 10, oppure una percentuale della serie di destinazioni, ad esempio 10%.

Se specifichi un numero assoluto pari a 3 errori, ad esempio, il sistema interrompe l'esecuzione dell'automazione alla ricezione del quarto errore. Se specifichi 0, il sistema smette di eseguire l'automazione su altre destinazioni non appena viene restituito il risultato del primo errore.

Se, ad esempio, se invii un'automazione a 50 istanze e imposti la soglia di errore su 10%, il sistema smette di inviare il comando alle altre istanze quando viene ricevuto il quinto errore. Sarà consentito il completamento delle chiamate che già eseguono un'automazione quando viene raggiunta la soglia di errore. Tuttavia, è possibile che alcune di queste automazioni abbiano esito negativo. Se devi assicurarti che non ci siano più errori del numero specificato per la soglia di errore, imposta il valore di `Concurrency` su 1 in modo che le automazioni procedano una alla volta.

## Esecuzione di automazioni in più Regioni AWS e account

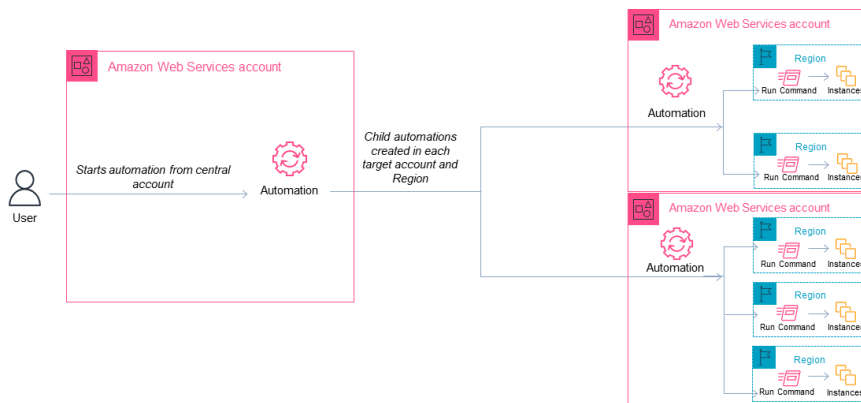
Puoi eseguire AWS Systems Manager automazioni su più Regioni AWS unità Account AWS e/o AWS Organizations organizzative (OU) da un account centrale. L'automazione è uno strumento di AWS Systems Manager. L'esecuzione delle automazioni in più regioni e account o unità organizzative riduce il tempo necessario per amministrare le AWS risorse migliorando al contempo la sicurezza dell'ambiente informatico.

Ad esempio, è possibile eseguire le operazioni seguenti utilizzando i runbook di Automazione:

- Implementa l'applicazione di patch e gli aggiornamenti di sicurezza a livello centrale.
- Correggi gli errori di conformità nelle configurazioni di VPC o nelle policy di bucket di Amazon S3.

- Gestisci risorse, come istanze EC2 di Amazon Elastic Compute Cloud (Amazon EC2), su larga scala.

Il diagramma riportato di seguito mostra un esempio di utente che sta eseguendo il runbook AWS - RestartEC2Instances in più Regioni e account da un account centrale. Il servizio di automazione individua le istanze mediante l'uso dei tag specificati nelle Regioni e negli account di destinazione.



## Scelta di un account centrale per l'automazione

Se desideri eseguire automazioni tra le unità organizzative, l'account centrale deve avere le autorizzazioni per elencare tutti gli account nelle unità. È possibile solo da un account amministratore delegato o dall'account di gestione dell'organizzazione. Ti consigliamo di seguire le AWS Organizations best practice e di utilizzare un account amministratore delegato. Per ulteriori informazioni sulle AWS Organizations best practice, consulta [Best practice per l'account di gestione](#) nella Guida per l'AWS Organizations utente. Per creare un account amministratore delegato per Systems Manager, è possibile utilizzare il `register-delegated-administrator` comando con il comando AWS CLI come mostrato nell'esempio seguente.

```
aws organizations register-delegated-administrator \
 --account-id delegated admin account ID \
 --service-principal ssm.amazonaws.com
```

Se desideri eseguire automazioni su più account non gestiti da AWS Organizations, ti consigliamo di creare un account dedicato per la gestione dell'automazione. L'esecuzione di tutte le automazioni tra account da un account dedicato semplifica la gestione delle autorizzazioni IAM, le operazioni di



risoluzione dei problemi e crea un livello di separazione tra operazioni e amministrazione. Questo approccio è consigliato anche se si utilizzano AWS Organizations, ma si desidera utilizzare solo account individuali e non unità organizzative.

Come funziona l'esecuzione delle automazioni

L'esecuzione delle automazioni in più Regioni e account o nelle UO funziona nel modo descritto di seguito:

1. Accedere all'account da configurare come account centrale dell'automazione.
2. Utilizzare la procedura [Configurazione delle autorizzazioni degli account di gestione per le automazioni in più Regioni e account](#) descritta in questo argomento per creare i seguenti ruoli IAM.
  - **AWS-SystemsManager-AutomationAdministrationRole**: questo ruolo concede all'utente l'autorizzazione necessaria per eseguire le automazioni in più account e nelle UO.
  - **AWS-SystemsManager-AutomationExecutionRole**: questo ruolo concede all'utente l'autorizzazione necessaria per eseguire le automazioni in più account di destinazione.
3. Scegliere il runbook, le Regioni e gli account o le UO in cui eseguire l'automazione.

 Note

Assicurarsi che l'unità organizzativa di destinazione contenga gli account desiderati. Se si sceglie un runbook personalizzato, il runbook deve essere condiviso con tutti gli account di destinazione. Per informazioni sulla condivisione di runbook, consulta [Condivisione di documenti SSM](#). Per informazioni sull'uso di runbook condivisi, consulta [Utilizzo di documenti SSM condivisi](#).

4. Esecuzione dell'automazione.
5. Utilizza le operazioni [GetAutomationExecution](#), [DescribeAutomationStepExecutions](#), e [DescribeAutomationExecutions](#) API dalla AWS Systems Manager console o dalla console AWS CLI per monitorare l'avanzamento dell'automazione. L'output delle fasi per l'automazione nell'account primario sarà AutomationExecutionId delle automazioni figlio. Per visualizzare l'output delle automazioni figlio create negli account di destinazione, assicurarsi di specificare l'account appropriato, la regione e AutomationExecutionId nella richiesta.

## Configurazione delle autorizzazioni degli account di gestione per le automazioni in più Regioni e account

Utilizzare la procedura seguente per creare i ruoli IAM richiesti per il servizio di automazione di Systems Manager in più regioni e account mediante l'uso di AWS CloudFormation. Questa procedura descrive come creare il ruolo `AWS-SystemsManager-AutomationAdministrationRole`. È sufficiente creare questo ruolo nell'account centrale del servizio di automazione. Questa procedura illustra inoltre come creare il ruolo `AWS-SystemsManager-AutomationExecutionRole`. È necessario creare questo ruolo in ogni account da definire come destinazione per l'esecuzione delle automazioni in più regioni e account. Ti consigliamo di CloudFormation StackSets utilizzarlo per creare il `AWS-SystemsManager-AutomationExecutionRole` ruolo negli account a cui desideri assegnare come target le automazioni per più regioni e più account.

Per creare il ruolo di amministrazione IAM richiesto per le automazioni in più regioni e più account utilizzando CloudFormation

1. Scarica e decomprimi il file [AWS-SystemsManager-AutomationAdministrationRole.zip](#).

oppure

Se i tuoi account sono gestiti da AWS Organizations [AWS-SystemsManager-AutomationAdministrationRole \(org\).zip](#)

Questi file contengono rispettivamente i file `AWS-SystemsManager-AutomationAdministrationRole (org).yaml` CloudFormation modello `AWS-SystemsManager-AutomationAdministrationRole.yaml` e i file modello.

2. Apri la CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
3. Seleziona Crea stack.
4. Nella sezione Specifica il modello, scegli Carica un modello.
5. Scegli il file, quindi scegli il file `AWS-SystemsManager-AutomationAdministrationRole.yaml` o il `AWS-SystemsManager-AutomationAdministrationRole (org).yaml` CloudFormation modello, a seconda della selezione effettuata nel passaggio 1.
6. Scegli Successivo.
7. Nella pagina Specificare dettagli dello stack, inserisci un nome nel campo Nome dello stack.
8. Scegli Avanti.

9. Nella pagina Configurazione delle opzioni dello stack, inserisci i valori per le opzioni che desideri utilizzare. Scegli Avanti.
10. Nella pagina Revisione, scorri verso il basso e scegli l'opzione Riconosco che CloudFormation potrebbe creare risorse IAM con nomi personalizzati.
11. Seleziona Crea stack.

CloudFormation mostra lo stato `CREATE_IN_PROGRESS` per circa tre minuti. Lo stato cambia in `CREATE_COMPLETE`.

È necessario ripetere questa procedura per ogni account da definire come destinazione per l'esecuzione delle automazioni in più regioni e account.

Per creare il ruolo di automazione IAM richiesto per le automazioni in più regioni e più account utilizzando CloudFormation

1. Scarica [AWS-SystemsManager-AutomationExecutionRole.zip](#).

oppure

Se i tuoi account sono gestiti da AWS Organizations [AWS-SystemsManager-AutomationExecutionRole \(org\).zip](#)

Questi file contengono rispettivamente i file modello `AWS-SystemsManager-AutomationExecutionRole.yaml` e `AWS-SystemsManager-AutomationExecutionRole (org).yaml` CloudFormation.

2. Apri la CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
3. Seleziona Crea stack.
4. Nella sezione Specifica il modello, scegli Carica un modello.
5. Scegli il file, quindi scegli il file `AWS-SystemsManager-AutomationExecutionRole.yaml` o il `AWS-SystemsManager-AutomationExecutionRole (org).yaml` CloudFormation modello, a seconda della selezione effettuata nel passaggio 1.
6. Scegli Successivo.
7. Nella pagina Specificare dettagli dello stack, inserisci un nome nel campo Nome dello stack.
8. Nella sezione Parametri, nel `AdminAccountId` campo, inserisci l'ID per l'account centrale di Automation.

9. Se stai configurando questo ruolo per un AWS Organizations ambiente, c'è un altro campo nella sezione chiamato `OrganizationID`. Inserisci l'ID della tua AWS organizzazione.
10. Scegli Avanti.
11. Nella pagina Configurazione delle opzioni dello stack, inserisci i valori per le opzioni che desideri utilizzare. Scegli Avanti.
12. Nella pagina Revisione, scorri verso il basso e scegli l'opzione Riconosco che CloudFormation potrebbe creare risorse IAM con nomi personalizzati.
13. Seleziona Crea stack.

CloudFormation mostra lo stato `CREATE_IN_PROGRESS` per circa tre minuti. Lo stato cambia in `CREATE_COMPLETE`.

Esecuzione di un'automazione in più regioni e account (console)

La procedura seguente descrive come utilizzare la console di Systems Manager per eseguire un'automazione in più regioni e account dall'account di gestione del servizio di automazione.

Prima di iniziare

Prima di completare la procedura seguente, prendi nota delle informazioni riportate di seguito:

- L'utente o il ruolo utilizzato per eseguire un'automazione tra più Regioni o tra più account deve disporre dell'autorizzazione `iam:PassRole` per il ruolo `AWS-SystemsManager-AutomationAdministrationRole`.
- Account AWS ID o unità organizzative in cui si desidera eseguire l'automazione.
- [Regioni supportate da Systems Manager](#) dove si desidera eseguire l'automazione.
- La chiave tag e il valore di tag, oppure il nome del gruppo di risorse, in cui eseguire l'automazione.

Per eseguire un'automazione in più regioni e account

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Automazione, quindi Esegui automazione.
3. Nell'elenco Documento di automazione, scegli un runbook. Scegli una o più opzioni nel pannello Categorie di documenti per filtrare i documenti SSM in base al loro scopo. Per visualizzare un runbook di cui si è proprietari, scegliere la scheda Posseduto da me. Per visualizzare un runbook

condiviso con l'account, scegliere la scheda Condiviso con me. Per visualizzare tutti i runbook, scegliere la scheda Tutti i documenti.

 Note

È possibile visualizzare informazioni su un runbook scegliendo il nome del runbook.

4. Nella sezione Dettagli documento verifica che l'opzione Versione documento sia impostata sulla versione che si desidera eseguire. Il sistema include le seguenti opzioni di versione:
  - Versione predefinita al runtime: scegli questa opzione se il runbook Automation viene aggiornato periodicamente e viene assegnata una nuova versione predefinita.
  - Ultima versione al runtime: scegli questa opzione se il runbook Automation viene aggiornato periodicamente e si desidera che venga eseguita la versione aggiornata più di recente.
  - 1 (predefinita): scegli questa opzione per eseguire la prima versione del documento (quella predefinita).
5. Scegli Avanti.
6. Nella pagina del documento Esegui automazione, scegli Multi-account una regione.
7. Nella sezione Account e regioni di Target, utilizza il campo Account, unità organizzative (OU) e root per specificare le diverse Account AWS unità AWS organizzative (OU) in cui desideri eseguire l'automazione. Separare i vari account o UO con virgole.
  - a. (Facoltativo) Seleziona la casella di controllo Includi UO figlie per includere tutte le unità organizzative figlie all'interno delle UO specificate.
  - b. (Facoltativo) Nel campo Escludi account e unità organizzative (UO), inserisci un elenco separato da virgole di ID account e ID UO che desideri escludere dalle entità espase inserite sopra.
8. Utilizzare l'elenco delle Regioni per scegliere una o più Regioni in cui eseguire l'automazione.
9. Utilizza le opzioni di controllo del tasso Multi-Region e dell'account per limitare l'automazione a un numero limitato di account in esecuzione in un numero limitato di regioni. Queste opzioni non limitano il numero di risorse di AWS in grado di eseguire le automazioni.
  - a. Nella sezione Location (account-Region pair) concurrency (Posizione (coppia account-regione) simultanea) scegliere un'opzione per limitare il numero di automazioni che possono essere eseguite contemporaneamente in più account e regioni. Ad esempio, se scegli di eseguire un'automazione in cinque (5) Account AWS, che si trovano in quattro

(4) Regioni AWS, Systems Manager esegue le automazioni in un totale di 20 coppie account-regione. È possibile utilizzare questa opzione per specificare un numero assoluto, ad esempio **2**, in modo che l'automazione venga eseguita solo in due coppie account-regione nello stesso momento. In alternativa, è possibile specificare una percentuale delle coppie account-regione in grado di eseguire l'automazione nello stesso momento. Ad esempio, con 20 coppie account-regione, se si specifica 20%, l'automazione verrà eseguita contemporaneamente in un massimo di cinque (5) coppie account-regione.

- Scegliere targets (destinazioni) per inserire un numero assoluto di coppie account-regione che possono eseguire contemporaneamente l'automazione.
- Scegliere percent (percentuale) per inserire una percentuale del numero totale di coppie account-regione che possono eseguire contemporaneamente l'automazione.

b. Nella sezione Error threshold (Soglia di errore) scegliere un'opzione:

- Scegliere errors (errori) per inserire un numero assoluto di errori consentiti, raggiunto il quale il servizio di automazione interrompe l'invio dell'automazione alle altre risorse.
- Scegliere percent (percentuale) per inserire la percentuale di errori consentiti, raggiunta la quale il servizio di automazione interrompe l'invio dell'automazione alle altre risorse.

10. Nella sezione Targets (Destinazioni) scegliere il modo in cui si desidera definire le risorse di AWS come destinazione in cui si desidera eseguire il servizio di automazione. Queste opzioni sono obbligatorie.

- Utilizza l'elenco Parameter (Parametro) per scegliere un parametro. Le voci nell'elenco Parameter (Parametro) sono determinate dai parametri presenti nel runbook del servizio di automazione selezionato all'inizio di questa procedura. È necessario scegliere un parametro per definire il tipo di risorsa su cui viene eseguito il flusso di lavoro del servizio di automazione.
- Utilizza l'elenco Targets (Destinazioni) per scegliere come si desidera definire le risorse come destinazione.
  - Se è stato deciso di definire le risorse come destinazione mediante i valori dei parametri, inserire il valore del parametro per il parametro selezionato nella sezione Input parameters (Parametri di input).
  - Se hai scelto di indirizzare le risorse utilizzando AWS Resource Groups, scegli il nome del gruppo dall'elenco dei gruppi di risorse.

- iii. Se è stato deciso di definire le risorse come destinazione mediante i tag, inserire la chiave e (facoltativamente) il valore del tag nei campi disponibili. Scegli Add (Aggiungi).
  - iv. Se desideri eseguire un runbook di Automation su tutte le istanze del sistema operativo corrente Account AWS Regione AWS, scegli Tutte le istanze.
11. Nella sezione Input parameters (Parametri di input) specifica i parametri obbligatori. Scegli il ruolo del servizio AWS-SystemsManager-AutomationAdministrationRole IAM dall'elenco. AutomationAssumeRole

 Note

Potrebbe non essere necessario scegliere alcune delle opzioni nella sezione Input parameters (Inserisci Parametri). Ciò è dovuto al fatto che le risorse sono state definite come destinazione in più regioni e account mediante i tag o un gruppo di risorse. Ad esempio, se è stato scelto il runbook AWS-RestartEC2Instance, non sarà necessario specificare o scegliere gli ID di istanza nella sezione Input parameters (Parametri di input). L'automazione individua le istanze da riavviare utilizzando i tag specificati.

12. (Facoltativo) Scegli un CloudWatch allarme da applicare all'automazione per il monitoraggio. Se l'allarme entra in ALARM stato, l'automazione viene annullata e vengono eseguiti tutti onCancel i passaggi definiti. Se lo usi AWS CloudTrail, vedrai la chiamata StopAutomationExecution API nel tuo percorso. Per ulteriori informazioni, consulta [Configurazione delle automazioni per monitorare gli allarmi CloudWatch](#).
13. Utilizza le opzioni nella sezione Rate control per limitare il numero di AWS risorse che possono eseguire l'automazione all'interno di ciascuna coppia account-regione.

Nella sezione Concurrency (Simultaneità) scegliere un'opzione:

- Scegliere Targets (Destinazioni) per inserire un numero assoluto di destinazioni che possono eseguire contemporaneamente il flusso di lavoro del servizio di automazione.
- Scegliere Percentage (Percentuale) per inserire la percentuale della serie di destinazioni che può eseguire contemporaneamente il flusso di lavoro del servizio di automazione.

14. Nella sezione Error threshold (Soglia di errore). scegliere un'opzione:

- Scegliere errors (errori) per inserire un numero assoluto di errori consentiti, raggiunto il quale il servizio di automazione interrompe l'invio del flusso di lavoro alle altre risorse.
- Scegli percentage (percentuale) per inserire una percentuale di errori consentiti, raggiunta la quale il servizio di automazione interrompe l'invio del flusso di lavoro alle altre risorse.

## 15. Scegliere Execute (Esegui).

Una volta completata l'esecuzione di un'automazione, è possibile rieseguirla con gli stessi parametri o con parametri modificati. Per ulteriori informazioni, consulta [Ripetizione delle esecuzioni di automazione](#).

Esecuzione di un'automazione in più Regioni e account (riga di comando)

La procedura seguente descrive come utilizzare AWS CLI (su Linux o Windows) o AWS Strumenti per PowerShell eseguire un'automazione in più regioni e account dall'account di gestione dell'automazione.

Prima di iniziare

Prima di completare la procedura seguente, prendi nota delle informazioni riportate di seguito:

- Account AWS ID o unità organizzative in cui si desidera eseguire l'automazione.
- [Regioni supportate da Systems Manager](#) dove si desidera eseguire l'automazione.
- La chiave tag e il valore di tag, oppure il nome del gruppo di risorse, in cui eseguire l'automazione.

Per eseguire un'automazione in più regioni e account

1. Installa e configura il AWS CLI o il AWS Strumenti per PowerShell, se non l'hai già fatto.

Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

2. Utilizzare il formato seguente per creare un comando per eseguire un'automazione in più regioni e account. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux & macOS

```
aws ssm start-automation-execution \
 --document-name runbook name \
 --parameters AutomationAssumeRole=arn:aws:iam::management account
ID:role/AWS-SystemsManager-AutomationAdministrationRole \
 --target-parameter-name parameter name \
 --targets Key=tag key,Values=value \

```



```
--target-locations Accounts=account ID,account ID
2,Regions=Region,Region 2,ExecutionRoleName=AWS-SystemsManager-
AutomationExecutionRole
```

## Windows

```
aws ssm start-automation-execution ^
 --document-name runbook name ^
 --parameters AutomationAssumeRole=arn:aws:iam::management account
ID:role/AWS-SystemsManager-AutomationAdministrationRole ^
 --target-parameter-name parameter name ^
 --targets Key=tag key,Values=value ^
 --target-locations Accounts=account ID,account ID
2,Regions=Region,Region 2,ExecutionRoleName=AWS-SystemsManager-
AutomationExecutionRole
```

## PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "tag key"
$Targets.Values = "value"

Start-SSMAutomationExecution `
 -DocumentName "runbook name" `
 -Parameter @{
 "AutomationAssumeRole"="arn:aws:iam::management account ID:role/AWS-
SystemsManager-AutomationAdministrationRole" } `
 -TargetParameterName "parameter name" `
 -Target $Targets `
 -TargetLocation @{
 "Accounts"="account ID","account ID 2";
 "Regions"="Region","Region 2";
 "ExecutionRoleName"="AWS-SystemsManager-AutomationExecutionRole" }
```

Esempi: esecuzione di un'automazione in più Regioni e account

Di seguito sono riportati alcuni esempi che dimostrano come utilizzare AWS CLI e PowerShell eseguire automazioni in più account e regioni con un solo comando.

Esempio 1: questo esempio riavvia le istanze EC2 in tre regioni di un'intera organizzazione. AWS Organizations Ciò si ottiene scegliendo come obiettivo l'ID root dell'organizzazione e includendo le unità organizzative secondarie.

## Linux & macOS

```
aws ssm start-automation-execution \
 --document-name "AWS-RestartEC2Instance" \
 --target-parameter-name InstanceId \
 --targets '[{"Key":"AWS::EC2::Instance","Values":["*"]}]' \
 --target-locations '[{
 "Accounts": ["r-example"],
 "IncludeChildOrganizationUnits": true,
 "Regions": ["us-east-1", "us-east-2", "us-west-2"]
 }]'
```

## Windows

```
aws ssm start-automation-execution \
 --document-name "AWS-RestartEC2Instance" ^
 --target-parameter-name InstanceId ^
 --targets '[{"Key":"AWS::EC2::Instance","Values":["*"]}]' ^
 --target-locations '[{
 "Accounts": ["r-example"],
 "IncludeChildOrganizationUnits": true,
 "Regions": ["us-east-1", "us-east-2", "us-west-2"]
 }]'
```

## PowerShell

```
Start-SSMAutomationExecution `
 -DocumentName "AWS-RestartEC2Instance" `
 -TargetParameterName "InstanceId" `
 -Targets '[{"Key":"AWS::EC2::Instance","Values":["*"]}]'
 -TargetLocation @{
 "Accounts"="r-example";
 "Regions"="us-east-1", "us-east-2", "us-west-2";
 "IncludeChildOrganizationUnits"=true}
```

Esempio 2: questo esempio riavvia istanze EC2 specifiche in diversi account e regioni.

 Note

L'opzione `TargetLocationMaxConcurrency` è disponibile utilizzando gli SDK e AWS CLI . AWS

## Linux &amp; macOS

```
aws ssm start-automation-execution \
 --document-name "AWS-RestartEC2Instance" \
 --target-parameter-name InstanceId \
 --target-locations '[{
 "Accounts": ["123456789012"],
 "Targets": [{
 "Key": "ParameterValues",
 "Values": ["i-02573cafcfEXAMPLE", "i-0471e04240EXAMPLE"]
 }],
 "TargetLocationMaxConcurrency": "100%",
 "Regions": ["us-east-1"]
 }, {
 "Accounts": ["987654321098"],
 "Targets": [{
 "Key": "ParameterValues",
 "Values": ["i-07782c72faEXAMPLE"]
 }],
 "TargetLocationMaxConcurrency": "100%",
 "Regions": ["us-east-2"]
 }]'
```

## Windows

```
aws ssm start-automation-execution ^
 --document-name "AWS-RestartEC2Instance" ^
 --target-parameter-name InstanceId ^
 --target-locations '[{
 "Accounts": ["123456789012"],
 "Targets": [{
 "Key": "ParameterValues",
 "Values": ["i-02573cafcfEXAMPLE", "i-0471e04240EXAMPLE"]
 }],
 "TargetLocationMaxConcurrency": "100%",
```

```

 "Regions": ["us-east-1"]
 }, {
 "Accounts": ["987654321098"],
 "Targets": [{
 "Key": "ParameterValues",
 "Values": ["i-07782c72faEXAMPLE"]
 }],
 "TargetLocationMaxConcurrency": "100%",
 "Regions": ["us-east-2"]
 }]
}
```

## PowerShell

```

Start-SSMAutomationExecution `
 -DocumentName "AWS-RestartEC2Instance" `
 -TargetParameterName "InstanceId" `
 -Targets '["Key": "AWS::EC2::Instance", "Values": ["*"]]'
 -TargetLocation @(
 "Accounts"="123456789012",
 "Targets"= @(
 "Key": "ParameterValues",
 "Values": ["i-02573cafcfEXAMPLE", "i-0471e04240EXAMPLE"]
),
 "TargetLocationMaxConcurrency"="100%",
 "Regions"=["us-east-1"]
), {
 "Accounts"="987654321098",
 "Targets": @(
 "Key": "ParameterValues",
 "Values": ["i-07782c72faEXAMPLE"]
),
 "TargetLocationMaxConcurrency": "100%",
 "Regions"=["us-east-2"]
 })
```

Esempio 3: questo esempio dimostra la specificazione di più Account AWS regioni in cui l'automazione deve essere eseguita utilizzando l'opzione. `--target-locations-url` Il valore di questa opzione deve essere un file JSON in un [URL Amazon S3 prefirmato](#) accessibile pubblicamente.

 Note

`--target-locations-url` è disponibile quando si utilizzano gli SDK AWS CLI e AWS .

## Linux &amp; macOS

```
aws ssm start-automation-execution \
 --document-name "MyCustomAutomationRunbook" \
 --target-locations-url "https://amzn-s3-demo-bucket.s3.amazonaws.com/target-
locations.json"
```

## Windows

```
aws ssm start-automation-execution ^
 --document-name "MyCustomAutomationRunbook" ^
 --target-locations-url "https://amzn-s3-demo-bucket.s3.amazonaws.com/target-
locations.json"
```

## PowerShell

```
Start-SSMAutomationExecution `
 -DocumentName "MyCustomAutomationRunbook" `
 -TargetLocationsUrl "https://amzn-s3-demo-bucket.s3.amazonaws.com/target-
locations.json"
```

## Contenuto esemplificativo per il file JSON:

```
[
{
 "Accounts": ["123456789012", "987654321098", "456789123012"],
 "ExcludeAccounts": ["111222333444", "999888444666"],
 "ExecutionRoleName": "MyAutomationExecutionRole",
 "IncludeChildOrganizationUnits": true,
 "Regions": ["us-east-1", "us-west-2", "ap-south-1", "ap-northeast-1"],
 "Targets": [{"Key": "AWS::EC2::Instance", "Values": ["i-2"]}],
 "TargetLocationMaxConcurrency": "50%",
 "TargetLocationMaxErrors": "10",
}
```

```

 "TargetsMaxConcurrency": "20",
 "TargetsMaxErrors": "12"
 }
]

```

Esempio 4: questo esempio riavvia le istanze EC2 negli account 123456789012 e 987654321098, che si trovano nelle Regioni us-east-2 e us-west-1. Le istanze devono essere contrassegnate con il valore Env-PROD della coppia di chiavi di tag.

## Linux & macOS

```

aws ssm start-automation-execution \
 --document-name AWS-RestartEC2Instance \
 --parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole \
 --target-parameter-name InstanceId \
 --targets Key=tag:Env,Values=PROD \
 --target-locations Accounts=123456789012,987654321098,Regions=us-
east-2,us-west-1,ExecutionRoleName=AWS-SystemsManager-AutomationExecutionRole

```

## Windows

```

aws ssm start-automation-execution ^
 --document-name AWS-RestartEC2Instance ^
 --parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole ^
 --target-parameter-name InstanceId ^
 --targets Key=tag:Env,Values=PROD ^
 --target-locations Accounts=123456789012,987654321098,Regions=us-
east-2,us-west-1,ExecutionRoleName=AWS-SystemsManager-AutomationExecutionRole

```

## PowerShell

```

$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "tag:Env"
$Targets.Values = "PROD"

Start-SSMAutomationExecution `
 -DocumentName "AWS-RestartEC2Instance" `
 -Parameter @{

```

```

 "AutomationAssumeRole"="arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole" } `
 -TargetParameterName "InstanceId" `
 -Target $Targets `
 -TargetLocation @{
 "Accounts"="123456789012","987654321098";
 "Regions"="us-east-2","us-west-1";
 "ExecutionRoleName"="AWS-SystemsManager-AutomationExecutionRole" }

```

Esempio 5: questo esempio riavvia le istanze EC2 negli account 123456789012 e 987654321098, che si trovano nella Regione eu-central-1. Le istanze devono essere membri del gruppo di prod-instances AWS risorse.

## Linux & macOS

```

aws ssm start-automation-execution \
 --document-name AWS-RestartEC2Instance \
 --parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole \
 --target-parameter-name InstanceId \
 --targets Key=ResourceGroup,Values=prod-instances \
 --target-locations Accounts=123456789012,987654321098,Regions=eu-
central-1,ExecutionRoleName=AWS-SystemsManager-AutomationExecutionRole

```

## Windows

```

aws ssm start-automation-execution ^
 --document-name AWS-RestartEC2Instance ^
 --parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole ^
 --target-parameter-name InstanceId ^
 --targets Key=ResourceGroup,Values=prod-instances ^
 --target-locations Accounts=123456789012,987654321098,Regions=eu-
central-1,ExecutionRoleName=AWS-SystemsManager-AutomationExecutionRole

```

## PowerShell

```

$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "ResourceGroup"
$Targets.Values = "prod-instances"

```

```
Start-SSMAutomationExecution `
 -DocumentName "AWS-RestartEC2Instance" `
 -Parameter @{
 "AutomationAssumeRole"="arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole" } `
 -TargetParameterName "InstanceId" `
 -Target $Targets `
 -TargetLocation @{
 "Accounts"="123456789012","987654321098";
 "Regions"="eu-central-1";
 "ExecutionRoleName"="AWS-SystemsManager-AutomationExecutionRole" }
```

Esempio 6: questo esempio riavvia le istanze EC2 nell'unità ou-1a2b3c-4d5e6c AWS organizzativa (OU). Le istanze si trovano nelle regioni us-west-1 e us-west-2. Le istanze devono essere membri del gruppo di risorse. WebServices AWS

## Linux & macOS

```
aws ssm start-automation-execution \
 --document-name AWS-RestartEC2Instance \
 --parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole \
 --target-parameter-name InstanceId \
 --targets Key=ResourceGroup,Values=WebServices \
 --target-locations Accounts=ou-1a2b3c-4d5e6c,Regions=us-west-1,us-
west-2,ExecutionRoleName=AWS-SystemsManager-AutomationExecutionRole
```

## Windows

```
aws ssm start-automation-execution ^
 --document-name AWS-RestartEC2Instance ^
 --parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole ^
 --target-parameter-name InstanceId ^
 --targets Key=ResourceGroup,Values=WebServices ^
 --target-locations Accounts=ou-1a2b3c-4d5e6c,Regions=us-west-1,us-
west-2,ExecutionRoleName=AWS-SystemsManager-AutomationExecutionRole
```

## PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
```



```

$Targets.Key = "ResourceGroup"
$Targets.Values = "WebServices"

Start-SSMAutomationExecution `
 -DocumentName "AWS-RestartEC2Instance" `
 -Parameter @{
 "AutomationAssumeRole"="arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole" } `
 -TargetParameterName "InstanceId" `
 -Target $Targets `
 -TargetLocation @{
 "Accounts"="ou-1a2b3c-4d5e6c";
 "Regions"="us-west-1";
 "ExecutionRoleName"="AWS-SystemsManager-AutomationExecutionRole" }

```

Questo sistema restituisce informazioni simili alle seguenti.

#### Linux & macOS

```

{
 "AutomationExecutionId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE"
}

```

#### Windows

```

{
 "AutomationExecutionId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE"
}

```

#### PowerShell

```
4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE
```

3. Eseguire il comando seguente per visualizzare i dettagli relativi all'automazione. *automation execution ID* Sostituiscile con le tue informazioni.

#### Linux & macOS

```

aws ssm describe-automation-executions \
 --filters Key=ExecutionId,Values=automation execution ID

```

## Windows

```
aws ssm describe-automation-executions ^
 --filters Key=ExecutionId,Values=automation execution ID
```

## PowerShell

```
Get-SSMAutomationExecutionList | `
 Where {$_.AutomationExecutionId -eq "automation execution ID"}
```

4. Eseguire il comando seguente per visualizzare i dettagli relativi allo stato di avanzamento dell'automazione.

## Linux & macOS

```
aws ssm get-automation-execution \
 --automation-execution-id 4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE
```

## Windows

```
aws ssm get-automation-execution ^
 --automation-execution-id 4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE
```

## PowerShell

```
Get-SSMAutomationExecution `
 -AutomationExecutionId a4a3c0e9-7efd-462a-8594-01234EXAMPLE
```

### Note

È inoltre possibile monitorare lo stato dell'automazione nella console. Nell'elenco delle Esecuzioni di automazione, scegli l'automazione appena eseguita e quindi scegli la scheda Fasi di esecuzione. In questa scheda viene mostrato lo stato delle operazioni di automazione.

## Ulteriori informazioni

[Applicazione di patch centralizzata per più account e Regioni con il servizio di Automazione di AWS Systems Manager](#)

## Esegui automazioni basate sugli eventi EventBridge

Puoi avviare un'automazione specificando un runbook come destinazione di un evento Amazon. EventBridge È possibile avviare le automazioni in base a una pianificazione oppure quando si verifica un determinato evento di sistema di AWS . Ad esempio, supponiamo che tu crei un runbook denominato `BootstrapInstances` che installa il software su un'istanza all'avvio di un'istanza. Per specificare il `BootstrapInstances` runbook (e l'automazione corrispondente) come destinazione di un EventBridge evento, devi prima creare una nuova regola. EventBridge (Ecco una regola di esempio: Nome del servizio: EC2, Tipo di evento: State-change Notifica dell'istanza EC2, Stati specifici: in esecuzione, Qualsiasi istanza.) Quindi si utilizzano le seguenti procedure per specificare il `BootstrapInstances` runbook come destinazione dell'evento utilizzando la EventBridge console e AWS Command Line Interface ().AWS CLI All'avvio di una nuova istanza, il sistema eseguirà l'automazione e installerà il software.

Per ulteriori informazioni sulla creazione di runbook, consulta [Creazione di runbook personalizzati](#).

### Creazione di un EventBridge evento che utilizza un runbook (console)

Utilizzate la procedura seguente per configurare un runbook come destinazione di un EventBridge evento.

Per configurare un runbook come destinazione di una regola di evento EventBridge

1. Apri la EventBridge console Amazon all'indirizzo. <https://console.aws.amazon.com/events/>
2. Nel pannello di navigazione, scegli Regole.
3. Scegli Crea regola.
4. Inserisci un nome e una descrizione per la regola.

Una regola non può avere lo stesso nome di un'altra regola nella stessa Regione e sullo stesso router di eventi.

5. Per Router di eventi, seleziona il router di eventi che desideri associare a questa regola. Se desideri che questa regola risponda agli eventi corrispondenti che provengono dai tuoi Account AWS, seleziona predefinito. Quando un Servizio AWS utente del tuo account emette un evento, viene sempre indirizzato al bus eventi predefinito del tuo account.

## 6. Scegli come attivare la regola.

| Per creare una regola basata su... | Esegui questa operazione...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |  |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Event                              | <p>a. Per Tipo di regola, scegli Regola con un modello di eventi.</p> <p>b. Scegli Avanti.</p> <p>c. Per Origine degli eventi, scegli AWS eventi o eventi EventBridge partner.</p> <p>d. Nella sezione Modello di eventi, procedi come segue:</p> <ul style="list-style-type: none"><li>• Per utilizzare un modello per creare lo schema di eventi, scegli Modulo del modello di eventi, quindi scegli Origine evento, Servizio AWS e Tipo di evento. Se scegli Tutti gli eventi come tipo di evento, tutti gli eventi emessi da Servizio AWS rispecchi erano la regola.</li></ul> <p>Per personalizzare il modello, scegli Modello personalizzato (editor JSON) e apporta le modifiche.</p> <ul style="list-style-type: none"><li>• Per utilizzare un modello di eventi personalizzato, scegli Modello personalizzato</li></ul> |  |

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |  |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Per creare una regola basata su... | Esegui questa operazione...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  |
|                                    | (editor JSON) e crea il tuo modello di evento.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |  |
| Schedule                           | <p>a. Per Tipo di regola, scegli Pianifica.</p> <p>b. Scegli Avanti.</p> <p>c. Per Modello di pianificazione, esegui una delle seguenti operazioni:</p> <ul style="list-style-type: none"> <li>• Per utilizzare un'espressione Cron per definire la pianificazione, scegli Una pianificazione con granularità fine che viene eseguita in un orario specifico , ad esempio le 8:00 PST il primo lunedì di ogni mese e inserisci l'espressione Cron.</li> <li>• Per utilizzare un'espressione della frequenza per definire la pianificazione, scegli Una pianificazione che viene eseguita con una frequenza regolare, ad esempio ogni 10 minuti e inserisci l'espressione della frequenza.</li> </ul> |  |

7. Scegli Avanti.

8. Per Tipi di destinazione, scegli servizio AWS .

9. Per Seleziona destinazione, scegli Automazione di Systems Manager.
10. Per Documento, scegli un runbook da usare quando viene chiamata la destinazione.
11. Nella sezione Configura parametri automazione non modificare i valori predefiniti dei parametri (se disponibili) oppure inserisci i valori desiderati.

#### Note

Per creare una destinazione, è necessario specificare un valore per ciascun parametro obbligatorio. In caso contrario, la regola verrà creata dal sistema ma non verrà eseguita.

12. Per molti tipi di target, EventBridge sono necessarie le autorizzazioni per inviare eventi al target. In questi casi, EventBridge può creare il ruolo IAM necessario per l'esecuzione della regola. Esegui una delle seguenti operazioni:

- Per creare un ruolo IAM automaticamente, seleziona Crea un nuovo ruolo per questa risorsa specifica.
- Per utilizzare un ruolo IAM creato in precedenza, seleziona Utilizza un ruolo esistente e seleziona il ruolo esistente dal menu a discesa. Tieni presente che potresti dover aggiornare la policy di fiducia da includere nel tuo ruolo IAM EventBridge. Di seguito è riportato un esempio:

#### JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "",
 "Effect": "Allow",
 "Principal": {
 "Service": [
 "events.amazonaws.com",
 "ssm.amazonaws.com"
]
 },
 "Action": "sts:AssumeRole"
 }
]
}
```

13. Scegli Avanti.
14. (Facoltativo) Inserire uno o più tag per la regola. Per ulteriori informazioni, consulta [Tagging Your Amazon EventBridge Resources](#) nella Amazon EventBridge User Guide.
15. Scegli Avanti.
16. Rivedi i dettagli della regola e scegli Crea regola.

Crea un EventBridge evento che utilizza un runbook (riga di comando)

La procedura seguente descrive come utilizzare AWS CLI (su Linux o Windows) o AWS Strumenti per PowerShell creare una regola di EventBridge evento e configurare un runbook come destinazione.

Per configurare un runbook come destinazione di una regola di evento EventBridge

1. Installa e configura il AWS CLI o il AWS Strumenti per PowerShell, se non l'hai già fatto.

Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

2. Crea un comando per specificare una nuova regola di EventBridge evento. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Attivazioni basate su una pianificazione

Linux & macOS

```
aws events put-rule \
--name "rule name" \
--schedule-expression "cron or rate expression"
```

Windows

```
aws events put-rule ^
--name "rule name" ^
--schedule-expression "cron or rate expression"
```

PowerShell

```
Write-CWRule `
-Name "rule name" `
```



```
-ScheduleExpression "cron or rate expression"
```

L'esempio seguente crea una regola di EventBridge evento che inizia ogni giorno alle 9:00 AM (UTC).

## Linux & macOS

```
aws events put-rule \
--name "DailyAutomationRule" \
--schedule-expression "cron(0 9 * * ? *)"
```

## Windows

```
aws events put-rule ^
--name "DailyAutomationRule" ^
--schedule-expression "cron(0 9 * * ? *)"
```

## PowerShell

```
Write-CWERule `\
-Name "DailyAutomationRule" `\
-ScheduleExpression "cron(0 9 * * ? *)"
```

## Attivazioni basate su un evento

### Linux & macOS

```
aws events put-rule \
--name "rule name" \
--event-pattern "{\"source\": [\"aws.service\"], \"detail-type\": [\"service event detail type\"]}"
```

### Windows

```
aws events put-rule ^
--name "rule name" ^
--event-pattern "{\"source\": [\"aws.service\"], \"detail-type\": [\"service event detail type\"]}"
```

## PowerShell

```
Write-CWRule `
-Name "rule name" `
-EventPattern '{"source":["aws.service"],"detail-type":["service event detail type"]}'
```

L'esempio seguente crea una regola di EventBridge evento che inizia quando una qualsiasi istanza EC2 nella regione cambia stato.

## Linux & macOS

```
aws events put-rule \
--name "EC2InstanceStateChanges" \
--event-pattern '{"source":["aws.ec2"],"detail-type":["EC2 Instance State-change Notification"]}'
```

## Windows

```
aws events put-rule ^
--name "EC2InstanceStateChanges" ^
--event-pattern '{"source":["aws.ec2"],"detail-type":["EC2 Instance State-change Notification"]}'
```

## PowerShell

```
Write-CWRule `
-Name "EC2InstanceStateChanges" `
-EventPattern '{"source":["aws.ec2"],"detail-type":["EC2 Instance State-change Notification"]}'
```

Il comando restituisce dettagli per la nuova EventBridge regola simili ai seguenti.

## Linux & macOS

```
{
 "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/automationrule"
}
```

## Windows

```
{
 "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/automationrule"
}
```

## PowerShell

```
arn:aws:events:us-east-1:123456789012:rule/EC2InstanceStateChanges
```

3. Create un comando per specificare un runbook come destinazione della regola dell' EventBridge evento creata nel passaggio 2. Sostituisci ogni *example resource placeholder* con le tue informazioni.

## Linux & macOS

```
aws events put-targets \
--rule rule name \
--targets '{"Arn": " arn:aws:ssm:region:account ID:automation-definition/runbook name","Input":{"Message\":[\{"Key\":"key name\","Values\":[\value\]]\}}","Id": "target ID","RoleArn": "arn:aws:iam::123456789012:role/service-role/EventBridge service role"}'
```

## Windows

```
aws events put-targets ^
--rule rule name ^
--targets '{"Arn": "arn:aws:ssm:region:account ID:automation-definition/runbook name","Input":{"Message\":[\{"Key\":"key name\","Values\":[\value\]]\}}","Id": "target ID","RoleArn": "arn:aws:iam::123456789012:role/service-role/EventBridge service role"}'
```

## PowerShell

```
$Target = New-Object Amazon.CloudWatchEvents.Model.Target
$Target.Id = "target ID"
$Target.Arn = "arn:aws:ssm:region:account ID:automation-definition/runbook name"
$Target.RoleArn = "arn:aws:iam::123456789012:role/service-role/EventBridge service role"
```

```
$Target.Input = '{"input parameter":["value"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/AutomationServiceRole"]}'

Write-CWETarget `
-Rule "rule name" `
-Target $Target
```

L'esempio seguente crea un target di EventBridge evento che avvia l'ID di istanza specificato utilizzando il AWS-StartEC2Instance runbook.

## Linux & macOS

```
aws events put-targets \
--rule DailyAutomationRule \
--targets '{"Arn": "arn:aws:ssm:region*:automation-definition/AWS-
StartEC2Instance", "Input": "{\\"InstanceId\\": [\\"i-02573cafcfEXAMPLE\\"],
\\"AutomationAssumeRole\\": [\\"arn:aws:iam::123456789012:role/AutomationServiceRole
\\"]}", "Id": "Target1", "RoleArn": "arn:aws:iam::123456789012:role/service-role/
AWS_Events_Invoke_Start_Automation_Execution_1213609520"}'
```

## Windows

```
aws events put-targets ^
--rule DailyAutomationRule ^
--targets '{"Arn": "arn:aws:ssm:region*:automation-definition/AWS-
StartEC2Instance", "Input": "{\\"InstanceId\\": [\\"i-02573cafcfEXAMPLE\\"],
\\"AutomationAssumeRole\\": [\\"arn:aws:iam::123456789012:role/AutomationServiceRole
\\"]}", "Id": "Target1", "RoleArn": "arn:aws:iam::123456789012:role/service-role/
AWS_Events_Invoke_Start_Automation_Execution_1213609520"}'
```

## PowerShell

```
$Target = New-Object Amazon.CloudWatchEvents.Model.Target
$Target.Id = "Target1"
$Target.Arn = "arn:aws:ssm:region*:automation-definition/AWS-StartEC2Instance"
$Target.RoleArn = "arn:aws:iam::123456789012:role/service-role/
AWS_Events_Invoke_Start_Automation_Execution_1213609520"
$Target.Input = '{"InstanceId":["i-02573cafcfEXAMPLE"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/AutomationServiceRole"]}'

Write-CWETarget `
```

```
-Rule "DailyAutomationRule" `
-Target $Target
```

Il sistema restituisce informazioni simili alle seguenti.

## Linux & macOS

```
{
 "FailedEntries": [],
 "FailedEntryCount": 0
}
```

## Windows

```
{
 "FailedEntries": [],
 "FailedEntryCount": 0
}
```

## PowerShell

Non viene prodotto alcun risultato se il comando ha esito positivo. PowerShell

## Esegui un'automazione passo dopo passo

Le procedure seguenti descrivono come utilizzare la AWS Systems Manager console e AWS Command Line Interface (AWS CLI) per eseguire un'automazione utilizzando la modalità di esecuzione manuale. Con questa modalità manuale, l'automazione viene avviata in stato Waiting (Attesa) e torna in stato Waiting (Attesa) nelle pause tra una fase e l'altra. Ciò consente di controllare quando l'automazione procede, il che è utile se è necessario esaminare il risultato di un passaggio prima di continuare.

L'automazione viene eseguita nel contesto dell'utente corrente. Ciò significa che non è necessario configurare autorizzazioni IAM aggiuntive a condizione di disporre dell'autorizzazione necessaria per eseguire il runbook e qualsiasi operazione chiamata dal runbook. Se disponi delle autorizzazioni dell'amministratore in IAM, disponi già dell'autorizzazione per eseguire l'automazione.

## Procedura dettagliata per l'esecuzione di un'automazione (console)

La procedura seguente mostra come utilizzare la console Systems Manager per eseguire manualmente un'automazione passo dopo passo.

Per eseguire un'automazione passo dopo passo

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Automazione, quindi Esegui automazione.
3. Nell'elenco Documento di automazione, scegli un runbook. Scegli una o più opzioni nel pannello Categorie di documenti per filtrare i documenti SSM in base al loro scopo. Per visualizzare un runbook di cui si è proprietari, scegliere la scheda Posseduto da me. Per visualizzare un runbook condiviso con l'account, scegliere la scheda Condiviso con me. Per visualizzare tutti i runbook, scegliere la scheda Tutti i documenti.

### Note

È possibile visualizzare informazioni su un runbook scegliendo il nome del runbook.

4. Nella sezione Dettagli documento verifica che l'opzione Versione documento sia impostata sulla versione che si desidera eseguire. Il sistema include le seguenti opzioni di versione:
  - Versione predefinita al runtime: scegli questa opzione se il runbook Automation viene aggiornato periodicamente e viene assegnata una nuova versione predefinita.
  - Ultima versione al runtime: scegli questa opzione se il runbook Automation viene aggiornato periodicamente e si desidera che venga eseguita la versione aggiornata più di recente.
  - 1 (predefinita): scegli questa opzione per eseguire la prima versione del documento (quella predefinita).
5. Scegli Avanti.
6. Nella sezione Execution Mode (Modalità esecuzione), scegliere Manual Execution (Esecuzione manuale).
7. Nella sezione Input parameters (Parametri di input) specifica i parametri obbligatori. Facoltativamente, puoi scegliere un ruolo del servizio IAM dall'AutomationAssumeRoleelenco.
8. Scegliere Execute (Esegui).
9. Scegliere Execute this step (Esegui questa fase) per avviare la prima fase dell'automazione. L'automazione procede con la fase uno e si interrompe prima di eseguire le fasi di automazione

successive specificate nel runbook scelto nella fase 3 di questa procedura. Se il runbook include più fasi, è necessario selezionare **Execute this step** (Esegui questa fase) per ogni fase per consentire all'automazione di continuare. Ogni volta che si sceglie **Execute this step** (Esegui questa fase) l'operazione viene eseguita.

#### Note

La console visualizza lo stato dell'automazione. Se l'automazione non è in grado di eseguire una fase, consulta [Risoluzione dei problemi di servizio di automazione di Systems Manager](#).

10. Dopo aver completato tutte le fasi indicate nel runbook, scegliere **Complete and view results** (Completa e visualizza i risultati) per completare l'automazione e visualizzare i risultati.

Una volta completata l'esecuzione di automazione, è possibile ripetere l'esecuzione con gli stessi parametri o con quelli modificati. Per ulteriori informazioni, consulta [Ripetizione delle esecuzioni di automazione](#).

Procedura dettagliata per l'esecuzione di un'automazione (riga di comando)

La procedura seguente descrive come utilizzare AWS CLI (su Linux o Windows) o AWS Strumenti per PowerShell eseguire manualmente un'automazione passo dopo passo. macOS

Per eseguire un'automazione passo dopo passo

1. Installa e configura AWS CLI o AWS Strumenti per PowerShell, se non l'hai già fatto.

Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

2. Esegui il comando seguente per avviare un'automazione manuale. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux & macOS

```
aws ssm start-automation-execution \
 --document-name runbook name \
 --mode Interactive \
 --parameters runbook parameters
```

## Windows

```
aws ssm start-automation-execution ^
 --document-name runbook name ^
 --mode Interactive ^
 --parameters runbook parameters
```

## PowerShell

```
Start-SSMAutomationExecution `
 -DocumentName runbook name `
 -Mode Interactive `
 -Parameter runbook parameters
```

Di seguito è riportato un esempio di utilizzo del runbook AWS-RestartEC2Instance per riavviare l'istanza EC2 specificata.

## Linux & macOS

```
aws ssm start-automation-execution \
 --document-name "AWS-RestartEC2Instance" \
 --mode Interactive \
 --parameters "InstanceId=i-02573cafcfEXAMPLE"
```

## Windows

```
aws ssm start-automation-execution ^
 --document-name "AWS-RestartEC2Instance" ^
 --mode Interactive ^
 --parameters "InstanceId=i-02573cafcfEXAMPLE"
```

## PowerShell

```
Start-SSMAutomationExecution `
 -DocumentName AWS-RestartEC2Instance `
 -Mode Interactive
 -Parameter @{"InstanceId"="i-02573cafcfEXAMPLE"}
```



Il sistema restituisce informazioni simili alle seguenti.

## Linux & macOS

```
{
 "AutomationExecutionId": "ba9cd881-1b36-4d31-a698-0123456789ab"
}
```

## Windows

```
{
 "AutomationExecutionId": "ba9cd881-1b36-4d31-a698-0123456789ab"
}
```

## PowerShell

```
ba9cd881-1b36-4d31-a698-0123456789ab
```

3. Esegui il comando seguente quando hai tutto pronto per avviare la prima fase dell'automazione. Sostituisci ogni *example resource placeholder* con le tue informazioni. L'automazione procede con la fase uno e si interrompe prima di eseguire le fasi successive specificate nel runbook scelto nella fase 1 di questa procedura. Se il runbook dispone di più fasi, è necessario eseguire il comando seguente per ogni fase affinché proceda l'automazione.

## Linux & macOS

```
aws ssm send-automation-signal \
 --automation-execution-id ba9cd881-1b36-4d31-a698-0123456789ab \
 --signal-type StartStep \
 --payload StepName="stopInstances"
```

## Windows

```
aws ssm send-automation-signal ^
 --automation-execution-id ba9cd881-1b36-4d31-a698-0123456789ab ^
 --signal-type StartStep ^
 --payload StepName="stopInstances"
```

## PowerShell

```
Send-SSMAutomationSignal `
 -AutomationExecutionId ba9cd881-1b36-4d31-a698-0123456789ab `
 -SignalType StartStep
 -Payload @{"StepName"="stopInstances"}
```

Se il comando va a buon fine, non viene generato output.

4. Esegui il comando seguente per recuperare lo stato di ciascuna esecuzione di fase nell'automazione.

## Linux & macOS

```
aws ssm describe-automation-step-executions \
 --automation-execution-id ba9cd881-1b36-4d31-a698-0123456789ab
```

## Windows

```
aws ssm describe-automation-step-executions ^
 --automation-execution-id ba9cd881-1b36-4d31-a698-0123456789ab
```

## PowerShell

```
Get-SSMAutomationStepExecution `
 -AutomationExecutionId ba9cd881-1b36-4d31-a698-0123456789ab
```

Il sistema restituisce informazioni simili alle seguenti.

## Linux & macOS

```
{
 "StepExecutions": [
 {
 "StepName": "stopInstances",
 "Action": "aws:changeInstanceState",
 "ExecutionStartTime": 1557167178.42,
 "ExecutionEndTime": 1557167220.617,
 "StepStatus": "Success",
```

```

 "Inputs": {
 "DesiredState": "\"stopped\"",
 "InstanceIds": "[\"i-02573cafcfEXAMPLE\"]"
 },
 "Outputs": {
 "InstanceStates": [
 "stopped"
]
 },
 "StepExecutionId": "654243ba-71e3-4771-b04f-0123456789ab",
 "OverriddenParameters": {},
 "ValidNextSteps": [
 "startInstances"
]
 },
 {
 "StepName": "startInstances",
 "Action": "aws:changeInstanceState",
 "ExecutionStartTime": 1557167273.754,
 "ExecutionEndTime": 1557167480.73,
 "StepStatus": "Success",
 "Inputs": {
 "DesiredState": "\"running\"",
 "InstanceIds": "[\"i-02573cafcfEXAMPLE\"]"
 },
 "Outputs": {
 "InstanceStates": [
 "running"
]
 },
 "StepExecutionId": "8a4a1e0d-dc3e-4039-a599-0123456789ab",
 "OverriddenParameters": {}
 }
]
}

```

## Windows

```

{
 "StepExecutions": [
 {
 "StepName": "stopInstances",
 "Action": "aws:changeInstanceState",

```

```

 "ExecutionStartTime": 1557167178.42,
 "ExecutionEndTime": 1557167220.617,
 "StepStatus": "Success",
 "Inputs": {
 "DesiredState": "\"stopped\"",
 "InstanceIds": "[\"i-02573cafcfEXAMPLE\"]"
 },
 "Outputs": {
 "InstanceStates": [
 "stopped"
]
 },
 "StepExecutionId": "654243ba-71e3-4771-b04f-0123456789ab",
 "OverriddenParameters": {},
 "ValidNextSteps": [
 "startInstances"
]
 },
 {
 "StepName": "startInstances",
 "Action": "aws:changeInstanceState",
 "ExecutionStartTime": 1557167273.754,
 "ExecutionEndTime": 1557167480.73,
 "StepStatus": "Success",
 "Inputs": {
 "DesiredState": "\"running\"",
 "InstanceIds": "[\"i-02573cafcfEXAMPLE\"]"
 },
 "Outputs": {
 "InstanceStates": [
 "running"
]
 },
 "StepExecutionId": "8a4a1e0d-dc3e-4039-a599-0123456789ab",
 "OverriddenParameters": {}
 }
]
}

```

## PowerShell

```

Action: aws:changeInstanceState
ExecutionEndTime : 5/6/2019 19:45:46

```

```

ExecutionStartTime : 5/6/2019 19:45:03
FailureDetails :
FailureMessage :
Inputs : {[DesiredState, "stopped"], [InstanceIds,
["i-02573cafcfEXAMPLE"]]}
IsCritical : False
IsEnd : False
MaxAttempts : 0
NextStep :
OnFailure :
Outputs : {[InstanceStates,
Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
OverriddenParameters : {}
Response :
ResponseCode :
StepExecutionId : 8fcc9641-24b7-40b3-a9be-0123456789ab
StepName : stopInstances
StepStatus : Success
TimeoutSeconds : 0
ValidNextSteps : {startInstances}

```

5. Esegui il comando seguente per completare l'automazione al termine di tutte le fasi specificate all'interno del runbook scelto. Sostituisci ogni *example resource placeholder* con le tue informazioni.

### Linux & macOS

```

aws ssm stop-automation-execution \
 --automation-execution-id ba9cd881-1b36-4d31-a698-0123456789ab \
 --type Complete

```

### Windows

```

aws ssm stop-automation-execution ^
 --automation-execution-id ba9cd881-1b36-4d31-a698-0123456789ab ^
 --type Complete

```

### PowerShell

```

Stop-SSMAutomationExecution `
 -AutomationExecutionId ba9cd881-1b36-4d31-a698-0123456789ab `

```

## -Type Complete

Se il comando va a buon fine, non viene generato output.

## Pianificazione delle automazioni con State Manager associazioni

È possibile avviare un'automazione creando un'associazione State Manager con un runbook. State Manager è uno strumento di AWS Systems Manager. Creando un'associazione State Manager con un runbook, puoi scegliere come target diversi tipi di AWS risorse. Ad esempio, è possibile creare associazioni che impongono lo stato desiderato a una AWS risorsa, tra cui:

- assegna un ruolo Systems Manager alle istanze di Amazon Elastic Compute Cloud (Amazon EC2) per renderle managed instances (istanze gestite);
- applica le regole di ingresso e di uscita desiderate per un gruppo di sicurezza;
- crea o elimina i backup di Amazon DynamoDB;
- crea o elimina gli snapshot di Amazon Elastic Block Store (Amazon EBS);
- Disattiva le autorizzazioni di lettura e scrittura per i bucket Amazon Simple Storage Service (Amazon S3);
- avvia, riavvia o arresta le istanze gestite e le istanze di Amazon Relational Database Service (Amazon RDS);
- applicare patch a Linux, macOS e alla finestra AMIs;

Utilizzate le seguenti procedure per creare un'associazione State Manager che esegue un'automazione utilizzando la AWS Systems Manager console e AWS Command Line Interface (AWS CLI). Per informazioni generali sulle associazioni e informazioni sulla creazione di un'associazione che utilizza un documento SSM Command o un documento Policy, consulta [Creazione di associazioni](#).

### Prima di iniziare

Tieni presente le informazioni importanti seguenti prima di eseguire un'automazione con State Manager:

- Prima di poter creare un'associazione che utilizza un runbook, verifica di aver configurato le autorizzazioni per l'automazione. Per ulteriori informazioni, consulta [Configurazione del servizio di automazione](#).

- Le associazioni di State Manager che utilizzano i runbook contribuiscono al raggiungimento del numero massimo per l'esecuzione di automazioni simultanee nell' Account AWS. Il numero massimo di esecuzioni simultanee del servizio di automazione è 100. Per informazioni, consulta [Service Quotas di Systems Manager](#) nella Riferimenti generali di Amazon Web Services.
- Quando si esegue un'automazione, State Manager non registra le operazioni API avviate dall'automazione in AWS CloudTrail.
- Systems Manager crea automaticamente un ruolo collegato al servizio affinché State Manager disponga dell'autorizzazione per chiamare le operazioni API del servizio di automazione di Systems Manager. Se lo desideri, puoi creare tu stesso il ruolo collegato al servizio eseguendo il seguente comando da o. AWS CLI AWS Strumenti per PowerShell

#### Linux & macOS

```
aws iam create-service-linked-role \
--aws-service-name ssm.amazonaws.com
```

#### Windows

```
aws iam create-service-linked-role ^
--aws-service-name ssm.amazonaws.com
```

#### PowerShell

```
New-IAMServiceLinkedRole `\
-AWSServiceName ssm.amazonaws.com
```

Per ulteriori informazioni sui ruoli collegati al servizio, consulta [Utilizzo di ruoli collegati ai servizi per Systems Manager](#).

#### Creazione di un'associazione che esegue un'automazione (console)

La procedura seguente descrive come utilizzare la console di Systems Manager per creare un'associazione di State Manager che esegue un'automazione.

Per creare un State Manager associazione che esegue un'automazione

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.

2. Nel pannello di navigazione, scegliere State Manager, quindi Create association (Crea associazione).
3. Nel campo Name (Nome), specifica un nome. Questo passaggio è facoltativo, ma è consigliato.
4. Nell'elenco Document (Documento), scegliere un runbook. Utilizza la barra di ricerca per filtrare per runbook Document type : Equal : Automation (Tipo documento: Uguale: Automazione). È possibile utilizzare i numeri a destra della barra di ricerca per visualizzare ulteriori runbook.

 Note

È possibile visualizzare informazioni su un runbook scegliendo il nome del runbook.

5. Scegli Simple execution (Esecuzione semplice) per eseguire l'automazione su una o più destinazioni specificando l'ID di risorsa per tali destinazioni. Scegli Rate control per eseguire l'automazione su una flotta di AWS risorse specificando un'opzione di targeting come tag o. AWS Resource Groups. È anche possibile controllare l'operazione dell'automazione nelle risorse specificando la simultaneità e le soglie di errore.

Se si sceglie Rate control (Controllo velocità), viene visualizzata la sezione Targets (Destinazioni).

6. Nella sezione Targets (Destinazioni), scegliere un metodo per definire le risorse come destinazione.
  - a. (Obbligatorio) Nell'elenco Parameter (Parametro), scegliere un parametro. Le voci nell'elenco Parameter (Parametro) sono determinate dai parametri presenti nel runbook selezionato all'inizio di questa procedura. Scegliendo un parametro, si definisce il tipo di risorsa su cui viene eseguita l'automazione.
  - b. (Obbligatorio) Nell'elenco Targets (Destinazioni), scegliere un metodo per definire le risorse come destinazione.
    - Resource Group (Gruppo di risorse): scegliere il nome del gruppo dall'elenco Resource Group (Gruppo di risorse). Per ulteriori informazioni sul targeting AWS Resource Groups nei runbook, consulta [Definizione del target AWS Resource Groups](#)
    - Tags (Tag): inserire la chiave del tag e, facoltativamente, il valore del tag nei campi disponibili. Scegli Add (Aggiungi). Per ulteriori informazioni sulla definizione dei tag come destinazione nei runbook, consulta [Definizione di un tag come destinazione](#).



- **Parameter Values (Valori parametro):** inserire i valori nella sezione Input parameters (Parametri di input). Se specifichi più valori, Systems Manager esegue un'automazione figlio su ciascun valore specificato.

Supponiamo, ad esempio, che il runbook includa un parametro InstanceID. Se definisci i valori del parametro InstanceID (IDistanza) come destinazione quando esegui l'automazione, il Systems Manager esegue un'automazione figlio per ogni valore di ID di istanza specificato. L'automazione padre risulta completa quando l'automazione termina l'esecuzione di ciascuna istanza specificata oppure se l'automazione ha esito negativo. È possibile definire come destinazione un massimo di 50 valori di parametro. Per ulteriori informazioni sulla definizione dei valori dei parametri come destinazione nei runbook, vedi [Definizione dei valori di parametro come destinazione](#).

7. Nella sezione Input parameters (Parametri di input), specificare i parametri di input obbligatori.

Se hai deciso di definire le risorse come destinazione mediante i tag o un gruppo di risorse, potrebbe non essere necessario scegliere alcune delle opzioni nella sezione Input parameters (Parametri di input). Ad esempio, se hai scelto il runbook AWS-RestartEC2Instance ed hai deciso di definire le istanze come destinazione mediante i tag, non sarà necessario specificare o scegliere gli ID di istanza nella sezione Input parameters (Parametri di input). Il servizio di automazione individua le istanze da riavviare utilizzando i tag specificati.

 **Important**

È necessario specificare un ruolo ARN nel campo. AutomationAssumeRole State Manager utilizza il ruolo di assunzione per chiamare Servizi AWS specificato nel runbook ed eseguire le associazioni di automazione per conto dell'utente.

8. Nella sezione Specify schedule (Specifica pianificazione), scegliere On Schedule (In base a pianificazione) per eseguire l'associazione a intervalli regolari. Se si sceglie questa opzione, utilizzare le opzioni fornite per creare la pianificazione con le espressioni Cron o della frequenza. Per ulteriori informazioni sulle espressioni Cron e della frequenza per State Manager, consulta [Espressioni Cron e della frequenza per le associazioni](#).

 **Note**

Le espressioni della frequenza sono il meccanismo di programmazione preferito per le associazioni State Manager che utilizzano i runbook. Le espressioni di frequenza consentono una maggiore flessibilità per l'esecuzione delle associazioni se si raggiunge

il numero massimo di automazioni in esecuzione simultanea. Con una pianificazione Rate, Systems Manager può riprovare l'automazione subito dopo aver ricevuto la notifica relativa al raggiungimento del numero massimo di automazioni simultanee e alla conseguente limitazione.

Scegliere No Schedule (Nessuna pianificazione) per eseguire l'associazione una sola volta.

9. (Facoltativo) Nella sezione Rate Control, scegli le opzioni Concurrency e Error threshold per controllare la distribuzione dell'automazione tra le tue risorse. AWS

a. Nella sezione Concurrency (Simultaneità) scegliere un'opzione:

- Scegliere Targets (Destinazioni) per inserire il numero assoluto di destinazioni che può eseguire contemporaneamente il servizio di automazione.
- Scegliere Percentage (Percentuale) per inserire la percentuale della serie di destinazioni che può eseguire contemporaneamente il servizio di automazione.

b. Nella sezione Error threshold (Soglia di errore) scegliere un'opzione:

- Scegliere errors (errori) per inserire il numero assoluto di errori consentiti, raggiunto il quale il servizio di automazione interrompe l'invio dell'automazione alle altre risorse;
- Scegliere percentage (percentuale) per inserire la percentuale di errori consentiti, raggiunta la quale il servizio di automazione interrompe l'invio dell'automazione alle altre risorse.

Per ulteriori informazioni sull'utilizzo delle destinazioni e dei controlli di velocità con l'automazione, vedi [Esegui operazioni automatizzate su larga scala](#).

10. Scegli Crea associazione.

 Important

Quando viene creata un'associazione, questa viene eseguita immediatamente in base alle destinazioni specificate. L'associazione quindi viene eseguita in base all'espressione Cron o della frequenza scelta. Se si sceglie No schedule (Nessuna pianificazione), l'associazione non viene eseguita di nuovo.

## Creazione di un'associazione che esegue un'automazione (riga di comando)

La procedura seguente descrive come utilizzare AWS CLI (su Linux o Windows Server) o creare un'associazione che AWS Strumenti per PowerShell esegua un'automazione.

### Prima di iniziare

Prima di completare la procedura seguente, assicurati di aver creato un ruolo del servizio IAM che contenga le autorizzazioni necessarie per eseguire il runbook e di aver configurato una relazione di fiducia per Automation. Per ulteriori informazioni, consulta [Processo 1: creazione di un ruolo di servizio per il servizio di automazione](#).

Per creare un'associazione che esegue un'automazione

1. Installa e configura il AWS CLI o il AWS Strumenti per PowerShell, se non l'hai già fatto.

Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

2. Eseguire il comando seguente per visualizzare un elenco di documenti.

#### Linux & macOS

```
aws ssm list-documents
```

#### Windows

```
aws ssm list-documents
```

#### PowerShell

```
Get-SSMDocumentList
```

Prendere nota del nome del runbook che desideri utilizzare per l'associazione.

3. Eseguire il comando seguente per visualizzare i dettagli sul runbook. Nel comando seguente, sostituisci *runbook name* con le tue informazioni.

#### Linux & macOS

```
aws ssm describe-document \
```

```
--name runbook name
```

Prendere nota di un nome di parametro (ad esempio, InstanceId) che si desidera utilizzare per l'opzione `--automation-target-parameter-name`. Questo parametro determina il tipo di risorsa su cui viene eseguita l'automazione.

## Windows

```
aws ssm describe-document ^
--name runbook name
```

Prendere nota di un nome di parametro (ad esempio, InstanceId) che si desidera utilizzare per l'opzione `--automation-target-parameter-name`. Questo parametro determina il tipo di risorsa su cui viene eseguita l'automazione.

## PowerShell

```
Get-SSMDocumentDescription `
-Name runbook name
```

Prendere nota di un nome di parametro (ad esempio, InstanceId) che si desidera utilizzare per l'opzione `AutomationTargetParameterName`. Questo parametro determina il tipo di risorsa su cui viene eseguita l'automazione.

4. Creare un comando che esegue un'automazione utilizzando un'associazione di State Manager. Sostituisci ogni *example resource placeholder* con le tue informazioni.

## Definizione di destinazioni mediante tag

## Linux & macOS

```
aws ssm create-association \
--association-name association name \
--targets Key=tag:key name,Values=value \
--name runbook name \
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/RunbookAssumeRole \
--automation-target-parameter-name target parameter \
--schedule "cron or rate expression"
```

 Note

Se create un'associazione utilizzando il AWS CLI, utilizzate il `--targets` parametro per indirizzare le istanze per l'associazione. Non utilizzare il parametro `--instance-id`. Il parametro `--instance-id` è un parametro legacy.

## Windows

```
aws ssm create-association ^
--association-name association name ^
--targets Key=tag:key name,Values=value ^
--name runbook name ^
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/RunbookAssumeRole ^
--automation-target-parameter-name target parameter ^
--schedule "cron or rate expression"
```

 Note

Se create un'associazione utilizzando il AWS CLI, utilizzate il `--targets` parametro per indirizzare le istanze per l'associazione. Non utilizzare il parametro `--instance-id`. Il parametro `--instance-id` è un parametro legacy.

## PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "tag:key name"
$Targets.Values = "value"

New-SSMAssociation `
-AssociationName "association name" `
-Target $Targets `
-Name "runbook name" `
-Parameters @{
"AutomationAssumeRole"="arn:aws:iam::123456789012:role/RunbookAssumeRole" } `
-AutomationTargetParameterName "target parameter" `
```

```
-ScheduleExpression "cron or rate expression"
```

### Note

Se create un'associazione utilizzando il AWS Strumenti per PowerShell, utilizzate il Target parametro per indirizzare le istanze per l'associazione. Non utilizzare il parametro InstanceId. Il parametro InstanceId è un parametro legacy.

## Definizione di destinazioni mediante valori di parametro

### Linux & macOS

```
aws ssm create-association \
--association-name association name \
--targets Key=ParameterValues,Values=value,value 2,value 3 \
--name runbook name \
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/RunbookAssumeRole \
--automation-target-parameter-name target parameter \
--schedule "cron or rate expression"
```

### Windows

```
aws ssm create-association ^
--association-name association name ^
--targets Key=ParameterValues,Values=value,value 2,value 3 ^
--name runbook name ^
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/RunbookAssumeRole ^
--automation-target-parameter-name target parameter ^
--schedule "cron or rate expression"
```

### PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "ParameterValues"
$Targets.Values = "value,value 2,value 3"

New-SSMAssociation `
```

```
-AssociationName "association name" `
-Target $Targets `
-Name "runbook name" `
-Parameters @{
 "AutomationAssumeRole"="arn:aws:iam::123456789012:role/RunbookAssumeRole" } `
-AutomationTargetParameterName "target parameter" `
-ScheduleExpression "cron or rate expression"
```

## Targeting utilizzando AWS Resource Groups

### Linux & macOS

```
aws ssm create-association \
--association-name association name \
--targets Key=ResourceGroup,Values=resource group name \
--name runbook name \
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/RunbookAssumeRole \
--automation-target-parameter-name target parameter \
--schedule "cron or rate expression"
```

### Windows

```
aws ssm create-association ^
--association-name association name ^
--targets Key=ResourceGroup,Values=resource group name ^
--name runbook name ^
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/RunbookAssumeRole ^
--automation-target-parameter-name target parameter ^
--schedule "cron or rate expression"
```

### PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "ResourceGroup"
$Targets.Values = "resource group name"

New-SSMAssociation `
-AssociationName "association name" `
-Target $Targets `
```

```
-Name "runbook name" `
-Parameters @{
 "AutomationAssumeRole"="arn:aws:iam::123456789012:role/RunbookAssumeRole" } `
-AutomationTargetParameterName "target parameter" `
-ScheduleExpression "cron or rate expression"
```

## Definizione di più account e regioni come destinazione

### Linux & macOS

```
aws ssm create-association \
--association-name association name \
--targets Key=ResourceGroup,Values=resource group name \
--name runbook name \
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/RunbookAssumeRole \
--automation-target-parameter-name target parameter \
--schedule "cron or rate expression" \
--target-locations
Accounts=111122223333,444455556666,444455556666,Regions=region,region
```

### Windows

```
aws ssm create-association ^
--association-name association name ^
--targets Key=ResourceGroup,Values=resource group name ^
--name runbook name ^
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/RunbookAssumeRole ^
--automation-target-parameter-name target parameter ^
--schedule "cron or rate expression" ^
--target-locations
Accounts=111122223333,444455556666,444455556666,Regions=region,region
```

### PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "ResourceGroup"
$Targets.Values = "resource group name"

New-SSMAssociation `
```



```
-AssociationName "association name" `
-Target $Targets `
-Name "runbook name" `
-Parameters @{
 "AutomationAssumeRole"="arn:aws:iam::123456789012:role/RunbookAssumeRole" } `
-AutomationTargetParameterName "target parameter" `
-ScheduleExpression "cron or rate expression" `
-TargetLocations @{
 "Accounts"=["111122223333,444455556666,444455556666"],
 "Regions"=["region,region"]
}
```

Il comando restituisce i dettagli per la nuova associazione simili ai seguenti.

## Linux & macOS

```
{
 "AssociationDescription": {
 "ScheduleExpression": "cron(0 7 ? * MON *)",
 "Name": "AWS-StartEC2Instance",
 "Parameters": {
 "AutomationAssumeRole": [
 "arn:aws:iam::123456789012:role/RunbookAssumeRole"
]
 },
 "Overview": {
 "Status": "Pending",
 "DetailedStatus": "Creating"
 },
 "AssociationId": "1450b4b7-bea2-4e4b-b340-01234EXAMPLE",
 "DocumentVersion": "$DEFAULT",
 "AutomationTargetParameterName": "InstanceId",
 "LastUpdateAssociationDate": 1564686638.498,
 "Date": 1564686638.498,
 "AssociationVersion": "1",
 "AssociationName": "CLI",
 "Targets": [
 {
 "Values": [
 "DEV"
],
 "Key": "tag:ENV"
 }
]
 }
}
```

```

]
 }
}

```

## Windows

```

{
 "AssociationDescription": {
 "ScheduleExpression": "cron(0 7 ? * MON *)",
 "Name": "AWS-StartEC2Instance",
 "Parameters": {
 "AutomationAssumeRole": [
 "arn:aws:iam::123456789012:role/RunbookAssumeRole"
]
 },
 "Overview": {
 "Status": "Pending",
 "DetailedStatus": "Creating"
 },
 "AssociationId": "1450b4b7-bea2-4e4b-b340-01234EXAMPLE",
 "DocumentVersion": "$DEFAULT",
 "AutomationTargetParameterName": "InstanceId",
 "LastUpdateAssociationDate": 1564686638.498,
 "Date": 1564686638.498,
 "AssociationVersion": "1",
 "AssociationName": "CLI",
 "Targets": [
 {
 "Values": [
 "DEV"
],
 "Key": "tag:ENV"
 }
]
 }
}

```

## PowerShell

```

Name : AWS-StartEC2Instance
InstanceId :
Date : 8/1/2019 7:31:38 PM
Status.Name :

```

```
Status.Date :
Status.Message :
Status.AdditionalInfo :
```

### Note

Se utilizzi i tag per creare un'associazione su una o più istanze di destinazione e quindi rimuovi i tag da un'istanza, tale istanza non eseguirà più l'associazione. L'istanza viene dissociata dal documento di State Manager.

## Risoluzione dei problemi relativi alle automazioni eseguite da State Manager associazioni

Il servizio di automazione di Systems Manager applica un limite di 100 automazioni simultanee e di 1.000 automazioni in coda per ogni account e per ogni regione. Se un'associazione che utilizza un runbook mostra lo stato `Non riuscito` e uno stato dettagliato di `AutomationExecutionLimitExceeded`, l'automazione potrebbe aver raggiunto il limite. Di conseguenza, Systems Manager limita le automazioni. Per risolvere il problema, procedere come segue:

- utilizzare un'altra espressione Cron o Rate per l'associazione. Ad esempio, se l'associazione è pianificata per l'esecuzione ogni 30 minuti, modifica l'espressione in modo che venga eseguita ogni ora o ogni due ore;
- eliminare le automazioni esistenti con stato Pending (In attesa). Eliminando queste automazioni, si cancella la coda corrente.

## Pianificazione delle automazioni con finestre di manutenzione

Puoi avviare un'automazione configurando un runbook come processo registrato per una finestra di manutenzione. Impostando il runbook come processo registrato, la finestra di manutenzione esegue l'automazione durante il periodo di manutenzione pianificato.

Ad esempio, supponiamo di creare un runbook denominato `CreateAMI` che crea un Amazon Machine Image (AMI) delle istanze registrate come destinazioni nella finestra di manutenzione. Per specificare il runbook `CreateAMI` (e la corrispondente automazione) come processo registrato di una finestra di manutenzione, creare innanzitutto una finestra di manutenzione e registra le destinazioni. Quindi puoi utilizzare la procedura seguente per specificare il documento `CreateAMI` come processo registrato all'interno della finestra di manutenzione. Quando la finestra di

manutenzione viene avviata durante il periodo programmato, il sistema esegue l'automazione e crea un'AMI delle destinazioni registrate.

Per informazioni sulla creazione dei runbook Automation, consulta [Creazione di runbook personalizzati](#). Automazione è uno strumento di AWS Systems Manager.

Utilizza le seguenti procedure per configurare un'automazione come attività registrata per una finestra di manutenzione utilizzando la AWS Systems Manager console, AWS Command Line Interface (AWS CLI) o AWS Tools for Windows PowerShell.

### Registrazione di un processo di automazione in una finestra di manutenzione (console)

La procedura seguente descrive come utilizzare la console di Systems Manager per configurare un'automazione come processo registrato per una finestra di manutenzione.

#### Prima di iniziare

Prima di completare la procedura seguente, è necessario creare una finestra di manutenzione e registrare almeno una destinazione. Per ulteriori informazioni, consulta le procedure seguenti:

- [Creare una finestra di manutenzione utilizzando la console](#).
- [Assegnazione di destinazioni a una finestra di manutenzione utilizzando la console](#)

Per configurare un'automazione come processo registrato per una finestra di manutenzione

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione a sinistra, scegliere Maintenance Windows, quindi selezionare la finestra di manutenzione all'interno della quale si desidera registrare un processo del servizio di automazione.
3. Scegliere Actions (Operazioni). Scegliere quindi Register Automation task (Registra processo di automazione) per eseguire un'automazione nelle destinazioni utilizzando un runbook.
4. In Name (Nome), inserire un nome per il processo.
5. In Description (Descrizione), inserire una descrizione.
6. In Document (Documento), scegliere il runbook che definisce i processi da eseguire.
7. In Document version (Versione del documento), scegliere la versione del runbook da utilizzare.

8. In Task priority (Priorità dei processi) scegliere una priorità. 1 è la priorità massima. I processi in una finestra di manutenzione vengono pianificati in ordine di priorità, pianificando in parallelo i processi che hanno la stessa priorità.
9. Nella sezione Targets (Destinazioni), se il runbook scelto esegue i processi in base alle risorse, identificare le destinazioni su cui eseguire l'automazione specificando i tag o selezionando le istanze manualmente.

#### Note

Se si desidera passare le risorse attraverso i parametri di input anziché le destinazioni, non è necessario specificare una destinazione per la finestra di manutenzione. In molti casi, non è necessario specificare in modo esplicito una destinazione per un processo di automazione. Ad esempio, supponiamo che tu stia creando un' Automation-type attività per aggiornare un Amazon Machine Image (AMI) per Linux usando il AWS-UpdateLinuxAmi runbook. Quando l'attività viene eseguita, AMI viene aggiornato con gli ultimi pacchetti di distribuzione Linux disponibili e il software Amazon. Nuove istanze create da AMI hanno già questi aggiornamenti installati. Perché l'ID dell'AMI da aggiornare è specificato nei parametri di input per il runbook, non è necessario specificare nuovamente una destinazione nel processo della finestra di manutenzione.

Per informazioni sui processi della finestra di manutenzione che non richiedono destinazioni, vedi [the section called “Registrazione delle attività della finestra di manutenzione senza destinazioni”](#).

10. (Facoltativo) In Controllo velocità:

#### Note

se il processo in esecuzione non specifica le destinazioni, non è necessario specificare i controlli della velocità.

- In Concurrency (Simultaneità), specificare un numero o una percentuale di destinazioni su cui eseguire contemporaneamente l'automazione.

Se le destinazioni vengono selezionate tramite coppie chiave-valore di tag e non si conosce il numero preciso delle destinazioni che utilizzano i tag selezionati, limitare il numero di automazioni che può essere eseguito simultaneamente specificando una percentuale.

Quando viene eseguita la finestra di manutenzione, viene avviata una nuova automazione per ogni destinazione. C'è un limite di 100 automazioni simultanee per Account AWS. Se si specifica una quota di simultaneità maggiore di 100, le automazioni simultanee superiori a 100 vengono automaticamente aggiunte alla coda di automazione. Per informazioni, consulta [Service Quotas di Systems Manager](#) nella Riferimenti generali di Amazon Web Services.

- In Error threshold (Soglia di errore), specificare quando interrompere l'esecuzione dell'automazione nelle altre destinazioni in seguito a errori su un certo numero o percentuale di destinazioni. Ad esempio, se si specificano tre errori, Systems Manager smette di eseguire le automazioni quando si verifica il quarto errore. Anche le destinazioni stanno ancora elaborando l'automazione potrebbero inviare errori.
11. Nella sezione Input parameters (Parametri di input), specifica i parametri per il runbook. Per i runbook, il sistema compila automaticamente alcuni dei valori. È possibile mantenere o sostituire tali valori.

 Important

Per i runbook, è possibile specificare facoltativamente un ruolo presunto di automazione. Se non specifichi un ruolo per questo parametro, l'automazione presume l'utilizzo del ruolo di servizio della finestra di manutenzione scelto nella fase 11. Pertanto, è necessario assicurarsi che il ruolo del servizio di finestra di manutenzione scelto disponga delle autorizzazioni AWS Identity and Access Management (IAM) appropriate per eseguire le azioni definite all'interno del runbook.

Ad esempio, il ruolo collegato al servizio per Systems Manager non ha l'autorizzazione IAM `ec2:CreateSnapshot`, obbligatoria per utilizzare il runbook `AWS-CopySnapshot`. In questo scenario, devi utilizzare un ruolo di servizio personalizzato della finestra di manutenzione o specificare un ruolo presunto di automazione che disponga delle autorizzazioni `ec2:CreateSnapshot`. Per informazioni, consulta [Configurazione del servizio di automazione](#).

12. Nell'area IAM service role (Ruolo di servizio IAM), scegli un ruolo per concedere a Systems Manager le autorizzazioni per avviare l'automazione.

Per creare un ruolo di servizio per le attività della finestra di manutenzione, consulta la sezione [Configurazione Intervallo di manutenzione](#).

13. Scegli Register Automation task (Registra processi di automazione).

## Registrazione di un processo di automazione in una finestra di manutenzione (riga di comando)

La procedura seguente descrive come utilizzare AWS CLI (su Linux o Windows Server) o AWS Strumenti per PowerShell configurare un'automazione come attività registrata per una finestra di manutenzione.

### Prima di iniziare

Prima di completare la procedura seguente, è necessario creare una finestra di manutenzione e registrare almeno una destinazione. Per ulteriori informazioni, consulta le procedure seguenti:

- [Fase 1: Creare la finestra di manutenzione utilizzando AWS CLI.](#)
- [Fase 2: Registrare un nodo di destinazione nella finestra di manutenzione utilizzando AWS CLI](#)

Per configurare un'automazione come processo registrato per una finestra di manutenzione

1. Installa e configura AWS CLI o AWS Strumenti per PowerShell, se non l'hai già fatto.

Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

2. Creare un comando per configurare un'automazione come processo registrato per una finestra di manutenzione Sostituisci ogni *example resource placeholder* con le tue informazioni.

### Linux & macOS

```
aws ssm register-task-with-maintenance-window \
--window-id window ID \
--name task name \
--task-arn runbook name \
--targets Key=targets,Values=value \
--service-role-arn IAM role arn \
--task-type AUTOMATION \
--task-invocation-parameters task parameters \
--priority task priority \
--max-concurrency 10% \
--max-errors 5
```

 Note

Se configuri un'automazione come attività registrata utilizzando il AWS CLI, utilizza il `--Task-Invocation-Parameters` parametro per specificare i parametri da passare a un'attività quando viene eseguita. Non utilizzare il parametro `--Task-Parameters`. Il parametro `--Task-Parameters` è un parametro legacy.

Per i processi della finestra di manutenzione senza una destinazione specificata, non è possibile fornire valori per `--max-errors` e `--max-concurrency`. Invece, il sistema inserisce un valore segnaposto pari a 1, che potrebbe essere segnalato nella risposta a comandi come [describe-maintenance-window-tasks](#) e [get-maintenance-window-task](#). Questi valori non influiscono sull'esecuzione del processo e possono essere ignorati.

Per informazioni sui processi della finestra di manutenzione che non richiedono destinazioni, vedi [Registrazione delle attività della finestra di manutenzione senza destinazioni](#).

## Windows

```
aws ssm register-task-with-maintenance-window ^
--window-id window ID ^
--name task name ^
--task-arn runbook name ^
--targets Key=targets,Values=value ^
--service-role-arn IAM role arn ^
--task-type AUTOMATION ^
--task-invocation-parameters task parameters ^
--priority task priority ^
--max-concurrency 10% ^
--max-errors 5
```

 Note

Se configuri un'automazione come attività registrata utilizzando il AWS CLI, utilizza il `--task-invocation-parameters` parametro per specificare i parametri da passare a un'attività quando viene eseguita. Non utilizzare il parametro `--task-parameters`. Il parametro `--task-parameters` è un parametro legacy.



Per i processi della finestra di manutenzione senza una destinazione specificata, non è possibile fornire valori per `--max-errors` e `--max-concurrency`. Invece, il sistema inserisce un valore segnaposto pari a 1, che potrebbe essere segnalato nella risposta a comandi come [describe-maintenance-window-tasks](#) e [get-maintenance-window-task](#). Questi valori non influiscono sull'esecuzione del processo e possono essere ignorati.

Per informazioni sui processi della finestra di manutenzione che non richiedono destinazioni, vedi [Registrazione delle attività della finestra di manutenzione senza destinazioni](#).

## PowerShell

```
Register-SSMTaskWithMaintenanceWindow `
-WindowId window ID `
-Name "task name" `
-TaskArn "runbook name" `
-Target @{ Key="targets";Values="value" } `
-ServiceRoleArn "IAM role arn" `
-TaskType "AUTOMATION" `
-Automation_Parameter @{ "task parameter"="task parameter value"} `
-Priority task priority `
-MaxConcurrency 10% `
-MaxError 5
```

### Note

Se configuri un'automazione come attività registrata utilizzando il AWS Strumenti per PowerShell, utilizza il `-Automation_Parameter` parametro per specificare i parametri da passare a un'attività quando l'operazione viene eseguita. Non utilizzare il parametro `-TaskParameters`. Il parametro `-TaskParameters` è un parametro legacy.

Per i processi della finestra di manutenzione senza una destinazione specificata, non è possibile fornire valori per `-MaxError` e `-MaxConcurrency`. Invece, il sistema inserisce un valore segnaposto pari a 1, che potrebbe essere segnalato nella risposta a comandi come `Get-SSMMaintenanceWindowTaskList` e `Get-SSMMaintenanceWindowTask`. Questi valori non influiscono sull'esecuzione del processo e possono essere ignorati.

Per informazioni sui processi della finestra di manutenzione che non richiedono destinazioni, vedi [Registrazione delle attività della finestra di manutenzione senza destinazioni](#).

L'esempio seguente configura un'automazione come processo registrato in una finestra di manutenzione con priorità 1. Dimostra inoltre l'omissione delle opzioni di `--targets`, `--max-errors`, e `--max-concurrency` per un processo della una finestra di manutenzione senza destinazione. L'automazione utilizza il runbook `AWS-StartEC2Instance` e il ruolo presunto del servizio di automazione specificato per avviare le istanze di EC2 registrate come destinazioni nella finestra di manutenzione. La finestra di manutenzione esegue l'automazione simultaneamente su un massimo di 5 istanze in qualsiasi momento. Inoltre, l'esecuzione del processo registrato viene arrestata su più istanze per un determinato intervallo se il conteggio degli errori supera 1.

## Linux & macOS

```
aws ssm register-task-with-maintenance-window \
--window-id mw-0c50858d01EXAMPLE \
--name StartEC2Instances \
--task-arn AWS-StartEC2Instance \
--service-role-arn arn:aws:iam::123456789012:role/MaintenanceWindowRole \
--task-type AUTOMATION \
--task-invocation-parameters "{\"Automation\":{\"Parameters\":{\"InstanceId\":\n\"{{TARGET_ID}}\"},\"AutomationAssumeRole\":[\"arn:aws:iam::123456789012:role/AutomationAssumeRole\"]}}\" \
--priority 1
```

## Windows

```
aws ssm register-task-with-maintenance-window ^
--window-id mw-0c50858d01EXAMPLE ^
--name StartEC2Instances ^
--task-arn AWS-StartEC2Instance ^
--service-role-arn arn:aws:iam::123456789012:role/MaintenanceWindowRole ^
--task-type AUTOMATION ^
--task-invocation-parameters "{\"Automation\":{\"Parameters\":{\"InstanceId\":\n\"{{TARGET_ID}}\"},\"AutomationAssumeRole\":[\"arn:aws:iam::123456789012:role/AutomationAssumeRole\"]}}\" ^
--priority 1
```

## PowerShell

```
Register-SSMTaskWithMaintenanceWindow `
-WindowId mw-0c50858d01EXAMPLE `
-Name "StartEC2" `
-TaskArn "AWS-StartEC2Instance" `
-ServiceRoleArn "arn:aws:iam::123456789012:role/MaintenanceWindowRole" `
-TaskType "AUTOMATION" `
-Automation_Parameter
@{ "InstanceId"="{{TARGET_ID}}";"AutomationAssumeRole"="arn:aws:iam::123456789012:role/
AutomationAssumeRole" } `
-Priority 1
```

Il comando restituisce i dettagli per il nuovo processo registrato simili ai seguenti.

## Linux & macOS

```
{
 "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE"
}
```

## Windows

```
{
 "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE"
}
```

## PowerShell

```
4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE
```

3. Per visualizzare il processo registrato, esegui il comando seguente. Sostituisci *maintenance windows ID* con le tue informazioni.

## Linux & macOS

```
aws ssm describe-maintenance-window-tasks \
--window-id maintenance window ID
```

## Windows

```
aws ssm describe-maintenance-window-tasks ^
--window-id maintenance window ID
```

## PowerShell

```
Get-SSMMaintenanceWindowTaskList `
-WindowId maintenance window ID
```

Il sistema restituisce informazioni simili alle seguenti.

## Linux & macOS

```
{
 "Tasks": [
 {
 "ServiceRoleArn": "arn:aws:iam::123456789012:role/
MaintenanceWindowRole",
 "MaxErrors": "1",
 "TaskArn": "AWS-StartEC2Instance",
 "MaxConcurrency": "1",
 "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
 "TaskParameters": {},
 "Priority": 1,
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Type": "AUTOMATION",
 "Targets": [
],
 "Name": "StartEC2"
 }
]
}
```

## Windows

```
{
 "Tasks": [
 {
```

```

 "ServiceRoleArn": "arn:aws:iam::123456789012:role/
MaintenanceWindowRole",
 "MaxErrors": "1",
 "TaskArn": "AWS-StartEC2Instance",
 "MaxConcurrency": "1",
 "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
 "TaskParameters": {},
 "Priority": 1,
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Type": "AUTOMATION",
 "Targets": [
],
 "Name": "StartEC2"
 }
]
}

```

## PowerShell

```

Description :
LoggingInfo :
MaxConcurrency : 5
MaxErrors : 1
Name : StartEC2
Priority : 1
ServiceRoleArn : arn:aws:iam::123456789012:role/MaintenanceWindowRole
Targets : {}
TaskArn : AWS-StartEC2Instance
TaskParameters : {}
Type : AUTOMATION
WindowId : mw-0c50858d01EXAMPLE
WindowTaskId : 4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE

```

## Configurazione delle automazioni per monitorare gli allarmi CloudWatch

È possibile configurare le esecuzioni del runbook di Automation per monitorare gli allarmi.

CloudWatch Se un allarme specificato entra in ALARM stato, Automation ne interrompe l'esecuzione.

Per le esecuzioni che utilizzano la modalità di controllo della frequenza o eseguite su più account,

Automation annulla tutte le esecuzioni in sospeso. Se definisci `onCancel` i passaggi nel tuo runbook,

questi passaggi vengono eseguiti prima del termine dell'esecuzione. Ciò impedisce che i runbook

continuino quando le risorse monitorate non sono intatte.

## Prima di iniziare

Completa questi prerequisiti prima di configurare CloudWatch il monitoraggio degli allarmi:

- Crea un CloudWatch allarme: crea un allarme che monitora le risorse interessate dall'esecuzione dell'automazione. Per ulteriori informazioni, consulta [Utilizzo degli CloudWatch allarmi](#) Amazon.
- Configurazione delle autorizzazioni dell'identità di esecuzione: l'identità di esecuzione utilizzata da Automation deve disporre delle seguenti autorizzazioni affinché il monitoraggio degli CloudWatch allarmi funzioni correttamente:
  - `cloudwatch:DescribeAlarms`— Necessario per monitorare gli stati di allarme.
  - `ssm:StopAutomationExecution`— Necessario per interrompere l'esecuzione quando si attiva un allarme.

L'identità di esecuzione è determinata dal ruolo IAM ARN specificato nel `assumeRole` campo del runbook di Automation. Se non viene specificato alcun `assumeRole` valore, il runbook viene eseguito utilizzando l'identità del principale IAM che ha chiamato `StartAutomationExecution`.

L'esempio seguente mostra una policy IAM minima che concede le autorizzazioni necessarie per il monitoraggio degli allarmi: CloudWatch

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "cloudwatch:DescribeAlarms",
 "ssm:StopAutomationExecution"
],
 "Resource": "*"
 }
]
}
```

## Configurazione del monitoraggio degli allarmi (console)

Utilizzare la seguente procedura per configurare il monitoraggio degli CloudWatch allarmi all'avvio di un'automazione dalla console di Systems Manager.

## Per configurare il monitoraggio degli allarmi

Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.

1. Nel pannello di navigazione, scegli Automazione.
2. Scegli Esegui automazione.
3. Seleziona un runbook e configura i parametri di input per la tua esecuzione.
4. Nella sezione degli CloudWatch allarmi, scegli un allarme da monitorare durante l'esecuzione.

**Input parameters**

**InstanceId**  
(Required) The ID of the EC2 instance on which you want to enable CloudWatch monitoring.

String

**AutomationAssumeRole**  
(Optional) The Amazon Resource Name (ARN) of the role that allows SSM Automation to perform the actions on your behalf.

Choose IAMRole

**status**  
(Optional) Specifies whether to enable or disable CloudWatch. Valid values: "Enabled" | "Disabled"

Enabled

**properties**  
(Optional) This parameter is not supported. It is listed here for backwards compatibility.

String

**CloudWatch alarm - optional**  
Control your automation by adding a CloudWatch alarm. If the alarm activates while the automation is running, the automation stops.

**Alarm name**  
The name of the CloudWatch alarm that you want to apply to this automation. [Create CloudWatch alarm](#)

my-alarm

☐ Continue automation if alarm status is unavailable  
If automation is unable to retrieve information about the state of your CloudWatch alarm, the automation continues to run.

5. (Facoltativo) Attiva Continua l'automazione se lo stato di allarme non è disponibile per controllare il comportamento quando Automation non è in grado di recuperare lo stato di allarme. Se abilitata, l'esecuzione continua anche se non è possibile determinare lo stato di allarme. Se disabilitato (impostazione predefinita), l'esecuzione si interrompe se non è possibile recuperare lo stato di allarme.
6. Scegli Esegui.

## Configurazione del monitoraggio degli allarmi (AWS CLI)

Utilizzate il `--alarm-configuration` parametro con il `aws ssm start-automation-execution` comando per specificare gli CloudWatch allarmi da monitorare.

Il `--alarm-configuration` parametro accetta una struttura JSON con i seguenti campi:

- **Alarms**(obbligatorio) — Un oggetto di allarme con un `Name` campo che identifica l' CloudWatch allarme da monitorare.
- **IgnorePollAlarmFailure**(opzionale, booleano) — Controlla il comportamento quando Automation non è in grado di recuperare lo stato di allarme. Impostato su `false` (impostazione

predefinita) per interrompere l'esecuzione se non è possibile determinare lo stato di allarme o `true` per continuare l'esecuzione a prescindere.

L'esempio seguente avvia un'automazione che monitora un CloudWatch allarme denominato `my-alarm`. Poiché `IgnorePollAlarmFailure` è impostata su `false`, l'automazione si interrompe se non riesce a recuperare lo stato di allarme:

```
aws ssm start-automation-execution \
 --document-name "AWS-RestartEC2Instance" \
 --parameters '{"InstanceId":["i-02573cafcfEXAMPLE"]}' \
 --alarm-configuration '{"IgnorePollAlarmFailure":false,"Alarms":[{"Name":"my-
alarm"}]}'
```

## Cross-account e monitoraggio degli allarmi interregionale

Per le automazioni eseguite su più account e regioni, puoi configurare il monitoraggio degli allarmi per località target utilizzando il `TargetLocationAlarmConfiguration` campo all'interno. `TargetLocations` Il ruolo di esecuzione in ogni account di destinazione (ad esempio `AWS-SystemsManager-AutomationExecutionRole`) deve disporre delle `ssm:StopAutomationExecution` autorizzazioni `cloudwatch:DescribeAlarms` necessarie.

Per ulteriori informazioni sulla configurazione dei ruoli tra account, vedere. [Configurazione delle autorizzazioni degli account di gestione per le automazioni in più Regioni e account](#)

## Riferimento alle operazioni del servizio di automazione di Systems Manager

In questa sezione di riferimento sono descritte le operazioni del servizio di automazione che è possibile specificare in un runbook del servizio di automazione. L'automazione è uno strumento di AWS Systems Manager. Queste operazioni non possono essere utilizzate in altri tipi di documenti di Systems Manager (SSM). Per informazioni sui plugin per gli altri tipi di documenti di SSM, consulta [Documentazione di riferimento del plugin per i documenti di comando](#).

Il servizio di automazione di Systems Manager esegue le fasi definite nei runbook del servizio di automazione. Ogni passaggio è associato a un'operazione specifica. L'operazione determina gli input, il comportamento e l'output della fase. Le fasi vengono definite nella sezione `mainSteps` del runbook.

Non è necessario specificare gli output di un'operazione o una fase. Gli output sono definiti dall'operazione associata alla fase. Quando si specifica gli input delle fasi nei runbook, è possibile



fare riferimento a uno o più output di una fase precedente. Ad esempio, è possibile rendere disponibile l'output di `aws:runInstances` a una successiva operazione `aws:runCommand`. È anche possibile fare riferimento agli output delle fasi precedenti nella sezione `Output` del runbook.

### Important

Se si esegue un flusso di lavoro di automazione che chiama altri servizi utilizzando un ruolo di servizio (IAM) di AWS Identity and Access Management, tenere presente che tale ruolo di servizio deve essere configurato con l'autorizzazione per la chiamata di tali servizi. Questo requisito si applica a tutti i runbook (AWS-\*runbook) di AWS Automation come `AWS-ConfigureS3BucketLogging`, e `AWS-RestartEC2Instance` runbook `AWS-CreateDynamoDBBackup`, solo per citarne alcuni. Questo requisito si applica anche a tutti i runbook di Automation personalizzati creati che richiamano altri utenti Servizi AWS utilizzando azioni che richiamano altri servizi. Ad esempio, se utilizzi le operazioni `aws:executeAwsApi`, `aws:createStack` o `aws:copyImage`, devi configurare il ruolo di servizio con l'autorizzazione per richiamare tali servizi. Puoi concedere le autorizzazioni ad altri Servizi AWS aggiungendo una policy inline IAM al ruolo. Per ulteriori informazioni, consulta [\(Facoltativo\) Aggiungi una policy in linea di Automation o una policy gestita dal cliente per richiamarne altre Servizi AWS](#).

## Argomenti

- [Proprietà condivise da tutte le operazioni](#)
- [aws:approve — Sospende un'automazione per l'approvazione manuale](#)
- [aws:assert — Assert AwsResourceProperty AWS stato della risorsa o stato dell'evento](#)
- [aws:branch — Esegue passaggi di automazione condizionali](#)
- [aws:change InstanceState — Cambia o afferma lo stato dell'istanza](#)
- [aws:copyImage: copia o crittografa un'Amazon Machine Image](#)
- [aws:createImage: creazione di un'Amazon Machine Image](#)
- [AWS:CreateStack — Crea un CloudFormation stack](#)
- [AWS:createTags — Crea tag per AWS risorse](#)
- [aws:deleteImage: eliminazione di un'Amazon Machine Image](#)
- [AWS>DeleteStack — Elimina un CloudFormation stack](#)
- [AWS:ExecuteAutomation — Esegui un'altra automazione](#)

- [aws:execute AwsApi — Chiama ed esegui AWS operazioni API](#)
- [aws:ExecuteScript — Esegue uno script](#)
- [aws:executeStateMachine— Esegui una macchina a AWS Step Functions stati](#)
- [aws:invokeWebhook: richiamo dell'integrazione di un webhook di Automation](#)
- [aws:invokeLambdaFunction— Invoca una funzione AWS Lambda](#)
- [aws:loop: intera sui passaggi di un'automazione](#)
- [aws:pause: sospensione di un'automazione](#)
- [aws:runCommand: esecuzione di un comando su un'istanza gestita](#)
- [aws:runInstances: avvio di un'istanza di Amazon EC2](#)
- [aws:sleep: ritardo di un'automazione](#)
- [aws:updateVariable: aggiorna un valore per una variabile di runbook](#)
- [aws:wait ForAwsResourceProperty — Attendi un AWS proprietà della risorsa](#)
- [Variabili di sistema del servizio di automazione](#)

Proprietà condivise da tutte le operazioni

Le proprietà comuni sono parametri o opzioni che si trovano in tutte le operazioni. Alcune opzioni definiscono il comportamento per una fase, ad esempio quanto tempo attendere il completamento di una fase e cosa fare se la fase non riesce. Le seguenti proprietà sono comuni a tutte le operazioni.

### [description](#)

Informazioni fornite per descrivere lo scopo di un runbook o di un passaggio.

─Tipo: stringa

Obbligatorio: no

### [name](#)

Identificatore che deve essere univoco per tutti i nomi di fase nel runbook.

Tipo: String

Modello consentito: [a-z A-Z0-9 \_] +\$

Obbligatorio: sì

## action

Nome dell'operazione che la fase deve eseguire. [aws:runCommand: esecuzione di un comando su un'istanza gestita](#) è un esempio di operazione che puoi specificare. Questo documento fornisce informazioni dettagliate su tutte le operazioni disponibili.

Tipo: stringa

Obbligatorio: sì

## maxAttempts

Numero di nuovi tentativi di esecuzione della fase in caso di errore. Se il valore è maggiore di 1, la fase non viene considerata non riuscita finché tutti i nuovi tentativi non hanno restituito esito negativo. Il valore predefinito è 1.

Tipo: Integer

Obbligatorio: no

## timeoutSeconds

Valore di timeout per la fase. Se il timeout viene raggiunto e il valore di `maxAttempts` è maggiore di 1, la fase non viene considerata scaduta finché non vengono eseguiti tutti i nuovi tentativi.

Tipo: Integer

Obbligatorio: no

## onFailure

Indica se, in caso di errore, l'automazione deve essere interrotta, deve continuare o deve passare a un'altra fase. Il valore predefinito di questa opzione è interrompi.

Tipo: String

Valori validi: Abort | Continue | step: *step\_name*

Obbligatorio: no

## onCancel

Indica a quale passaggio deve procedere l'automazione se un utente annulla l'automazione. L'automazione esegue il flusso di lavoro di annullamento per un massimo di due minuti.

Tipo: String

Valori validi: Abort | step: *step\_name*

Obbligatorio: no

La proprietà `onCancel` non supporta il passaggio alle seguenti operazioni:

- `aws:approve`
- `aws:copyImage`
- `aws:createImage`
- `aws:createStack`
- `aws:createTags`
- `aws:loop`
- `aws:pause`
- `aws:runInstances`
- `aws:sleep`

### [isEnd](#)

Questa opzione arresta l'automazione alla fine di una fase specifica. L'automazione viene arrestata se la fase ha esito positivo o negativo. Il valore predefinito è `false`.

Tipo: Booleano

Valori validi: `true` | `false`

Obbligatorio: no

### [nextStep](#)

Specifica la successiva fase di un'automazione da elaborare dopo il completamento di una fase.

─Tipo: stringa

Obbligatorio: no

### [isCritical](#)

Designa una fase come fase critica per il corretto completamento dell'automazione. Se una fase con questa definizione ha esito negativo, il servizio di automazione restituisce come stato finale dell'automazione il valore `Non riuscito`. Questa proprietà viene valutata solo se viene definita esplicitamente nella fase. Se la proprietà `onFailure` viene impostata su `Continue` in una fase, il valore predefinito è `false`. Altrimenti, il valore predefinito per questa opzione è `"true"`.

Tipo: Booleano

Valori validi: true | false

Obbligatorio: no

### inputs

Proprietà specifiche dell'azione.

Tipo: Map

Obbligatorio: sì

### Esempio

```

description: "Custom Automation Example"
schemaVersion: '0.3'
assumeRole: "{{ AutomationAssumeRole }}"
parameters:
 AutomationAssumeRole:
 type: String
 description: "(Required) The ARN of the role that allows Automation to perform
 the actions on your behalf. If no role is specified, Systems Manager Automation
 uses your IAM permissions to run this runbook."
 default: ''
 InstanceId:
 type: String
 description: "(Required) The Instance Id whose root EBS volume you want to
 restore the latest Snapshot."
 default: ''
mainSteps:
- name: getInstanceDetails
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: DescribeInstances
 InstanceIds:
 - "{{ InstanceId }}"
 outputs:
 - Name: availabilityZone
 Selector: "$.Reservations[0].Instances[0].Placement.AvailabilityZone"
```

```

 Type: String
 - Name: rootDeviceName
 Selector: "$.Reservations[0].Instances[0].RootDeviceName"
 Type: String
 nextStep: getRootVolumeId
- name: getRootVolumeId
 action: aws:executeAwsApi
 maxAttempts: 3
 onFailure: Abort
 inputs:
 Service: ec2
 Api: DescribeVolumes
 Filters:
 - Name: attachment.device
 Values: ["{{ getInstanceDetails.rootDeviceName }}"]
 - Name: attachment.instance-id
 Values: ["{{ InstanceId }}"]
 outputs:
 - Name: rootVolumeId
 Selector: "$.Volumes[0].VolumeId"
 Type: String
 nextStep: getSnapshotsByStartTime
- name: getSnapshotsByStartTime
 action: aws:executeScript
 timeoutSeconds: 45
 onFailure: Abort
 inputs:
 Runtime: python3.8
 Handler: getSnapshotsByStartTime
 InputPayload:
 rootVolumeId : "{{ getRootVolumeId.rootVolumeId }}"
 Script: |-
 def getSnapshotsByStartTime(events, context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 rootVolumeId = events['rootVolumeId']
 snapshotsQuery = ec2.describe_snapshots(
 Filters=[
 {
 "Name": "volume-id",
 "Values": [rootVolumeId]
 }
]

```

```

]
)
 if not snapshotsQuery['Snapshots']:
 noSnapshotFoundString = "NoSnapshotFound"
 return { 'noSnapshotFound' : noSnapshotFoundString }
 else:
 jsonSnapshots = snapshotsQuery['Snapshots']
 sortedSnapshots = sorted(jsonSnapshots, key=lambda k: k['StartTime'],
reverse=True)
 latestSortedSnapshotId = sortedSnapshots[0]['SnapshotId']
 return { 'latestSnapshotId' : latestSortedSnapshotId }
outputs:
- Name: Payload
 Selector: $.Payload
 Type: StringMap
- Name: latestSnapshotId
 Selector: $.Payload.latestSnapshotId
 Type: String
- Name: noSnapshotFound
 Selector: $.Payload.noSnapshotFound
 Type: String
nextStep: branchFromResults
- name: branchFromResults
 action: aws:branch
 onFailure: Abort
 onCancel: step:startInstance
 inputs:
 Choices:
 - NextStep: createNewRootVolumeFromSnapshot
 Not:
 Variable: "{{ getSnapshotsByStartTime.noSnapshotFound }}"
 StringEquals: "NoSnapshotFound"
 isEnd: true
- name: createNewRootVolumeFromSnapshot
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: CreateVolume
 AvailabilityZone: "{{ getInstanceDetails.availabilityZone }}"
 SnapshotId: "{{ getSnapshotsByStartTime.latestSnapshotId }}"
 outputs:
 - Name: newRootVolumeId
 Selector: ".$VolumeId"

```

```
 Type: String
 nextStep: stopInstance
- name: stopInstance
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: StopInstances
 InstanceIds:
 - "{{ InstanceId }}"
 nextStep: verifyVolumeAvailability
- name: verifyVolumeAvailability
 action: aws:waitForAwsResourceProperty
 timeoutSeconds: 120
 inputs:
 Service: ec2
 Api: DescribeVolumes
 VolumeIds:
 - "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
 PropertySelector: "$.Volumes[0].State"
 DesiredValues:
 - "available"
 nextStep: verifyInstanceStopped
- name: verifyInstanceStopped
 action: aws:waitForAwsResourceProperty
 timeoutSeconds: 120
 inputs:
 Service: ec2
 Api: DescribeInstances
 InstanceIds:
 - "{{ InstanceId }}"
 PropertySelector: "$.Reservations[0].Instances[0].State.Name"
 DesiredValues:
 - "stopped"
 nextStep: detachRootVolume
- name: detachRootVolume
 action: aws:executeAwsApi
 onFailure: Abort
 isCritical: true
 inputs:
 Service: ec2
 Api: DetachVolume
 VolumeId: "{{ getRootVolumeId.rootVolumeId }}"
 nextStep: verifyRootVolumeDetached
```



```
- name: verifyRootVolumeDetached
 action: aws:waitForAwsResourceProperty
 timeoutSeconds: 30
 inputs:
 Service: ec2
 Api: DescribeVolumes
 VolumeIds:
 - "{{ getRootVolumeId.rootVolumeId }}"
 PropertySelector: "$.Volumes[0].State"
 DesiredValues:
 - "available"
 nextStep: attachNewRootVolume
- name: attachNewRootVolume
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: AttachVolume
 Device: "{{ getInstanceDetails.rootDeviceName }}"
 InstanceId: "{{ InstanceId }}"
 VolumeId: "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
 nextStep: verifyNewRootVolumeAttached
- name: verifyNewRootVolumeAttached
 action: aws:waitForAwsResourceProperty
 timeoutSeconds: 30
 inputs:
 Service: ec2
 Api: DescribeVolumes
 VolumeIds:
 - "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
 PropertySelector: "$.Volumes[0].Attachments[0].State"
 DesiredValues:
 - "attached"
 nextStep: startInstance
- name: startInstance
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: StartInstances
 InstanceIds:
 - "{{ InstanceId }}"
```

## **aws:approve** — Sospende un'automazione per l'approvazione manuale

Sospende temporaneamente un'automazione finché i principali designati non approvano o rifiutano l'operazione. Una volta raggiunto il numero richiesto di approvazioni, viene ripresa l'automazione. Puoi inserire la fase di approvazione in qualsiasi punto della sezione `mainSteps` del runbook.

### Note

Questa operazione non supporta le automazioni per più account e regioni. Il timeout predefinito per questa azione è di 7 giorni (60.4800 secondi) e il valore massimo è di 30 giorni (259.2000 secondi). Puoi limitare o estendere il timeout specificando il parametro `timeoutSeconds` per una fase `aws:approve`.

Nell'esempio seguente l'operazione `aws:approve` sospende temporaneamente l'automazione finché un approvatore non accetta o rifiuta l'automazione. Dopo l'approvazione, l'automazione esegue un semplice comando PowerShell

### YAML

```

description: RunInstancesDemo1
schemaVersion: '0.3'
assumeRole: "{{ assumeRole }}"
parameters:
 assumeRole:
 type: String
 message:
 type: String
mainSteps:
- name: approve
 action: aws:approve
 timeoutSeconds: 1000
 onFailure: Abort
 inputs:
 NotificationArn: arn:aws:sns:us-east-2:12345678901:AutomationApproval
 Message: "{{ message }}"
 MinRequiredApprovals: 1
 Approvers:
 - arn:aws:iam::12345678901:user/AWS-User-1
- name: run
 action: aws:runCommand
```

```
inputs:
 InstanceIds:
 - i-1a2b3c4d5e6f7g
 DocumentName: AWS-RunPowerShellScript
 Parameters:
 commands:
 - date
```

## JSON

```
{
 "description": "RunInstancesDemo1",
 "schemaVersion": "0.3",
 "assumeRole": "{{ assumeRole }}",
 "parameters": {
 "assumeRole": {
 "type": "String"
 },
 "message": {
 "type": "String"
 }
 },
 "mainSteps": [
 {
 "name": "approve",
 "action": "aws:approve",
 "timeoutSeconds": 1000,
 "onFailure": "Abort",
 "inputs": {
 "NotificationArn": "arn:aws:sns:us-east-2:12345678901:AutomationApproval",
 "Message": "{{ message }}",
 "MinRequiredApprovals": 1,
 "Approvers": [
 "arn:aws:iam::12345678901:user/AWS-User-1"
]
 }
 },
 {
 "name": "run",
 "action": "aws:runCommand",
 "inputs": {
 "InstanceIds": [
```

```

 "i-1a2b3c4d5e6f7g"
],
 "DocumentName": "AWS-RunPowerShellScript",
 "Parameters": {
 "commands": [
 "date"
]
 }
}
}
]
}

```

È possibile approvare o rifiutare le automazioni in attesa di approvazione nella console.

Per approvare o rifiutare le automazioni in attesa

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Automazione.
3. Scegli l'opzione accanto un'automazione con stato In attesa.

| Automation executions                                                                                                    |                                    |                                                                                             |                               |                |
|--------------------------------------------------------------------------------------------------------------------------|------------------------------------|---------------------------------------------------------------------------------------------|-------------------------------|----------------|
| <div> <input type="text"/> </div>                                                                                        |                                    |                                                                                             |                               |                |
| <div> <span>↻</span> <span>View details</span> <span>Cancel execution</span> <span>Approve/Deny</span> </div>            |                                    |                                                                                             |                               |                |
| Execution ID                                                                                                             | Document name                      | Status                                                                                      | Start time (UTC)              | End time (UTC) |
|  7e4e1ea9-f186-11e7-9a57-e1a762426a2a | AWS-RestartEC2InstanceWithApproval |  Waiting | Thu, 04 Jan 2018 19:36:00 GMT | -              |

4. Scegli Approve/Deny.
5. Rivedere i dettagli dell'automazione.
6. Scegli Approva o Rifiuta, immetti un commento facoltativo, quindi scegli Invia.

Esempio di input

YAML

```

NotificationArn: arn:aws:sns:us-west-1:12345678901:Automation-ApprovalRequest
Message: Please approve this step of the Automation.

```

```
MinRequiredApprovals: 3
Approvers:
- IamUser1
- IamUser2
- arn:aws:iam::12345678901:user/IamUser3
- arn:aws:iam::12345678901:role/IamRole
```

## JSON

```
{
 "NotificationArn": "arn:aws:sns:us-west-1:12345678901:Automation-ApprovalRequest",
 "Message": "Please approve this step of the Automation.",
 "MinRequiredApprovals": 3,
 "Approvers": [
 "IamUser1",
 "IamUser2",
 "arn:aws:iam::12345678901:user/IamUser3",
 "arn:aws:iam::12345678901:role/IamRole"
]
}
```

## NotificationArn

L'Amazon Resource Name (ARN) di un argomento Amazon Simple Notification Service (Amazon SNS) per approvazioni del servizio di automazione. Quando si specifica una fase `aws:approve` in un runbook, il servizio di automazione invia un messaggio a questo argomento per informare i principali che devono approvare o rifiutare una fase di automazione. Il titolo dell'argomento Amazon SNS devono avere il prefisso "Automation".

─Tipo: stringa

Obbligatorio: no

## Messaggio

Informazioni da includere nell'argomento Amazon SNS quando viene inviata la richiesta di approvazione. La lunghezza massima del messaggio è 4096 caratteri;

─Tipo: stringa

Obbligatorio: no

## MinRequiredApprovals

Numero minimo di approvazioni richieste per riprendere l'automazione. Se non si specifica un valore, il valore predefinito è uno. Il valore di questo parametro deve essere un numero intero positivo. Il valore di questo parametro non può superare il numero di approvatori definiti dal parametro `Approvers`.

Tipo: Integer

Obbligatorio: no

## Approvers

Un elenco di committenti AWS autenticati che possono approvare o rifiutare l'azione. Il numero massimo di approvatori è 10. È possibile specificare i principali utilizzando uno dei seguenti formati:

- Un nome utente
- Un ARN utente
- Un ARN del ruolo IAM
- Un ARN del ruolo presunto IAM

Tipo: StringList

Obbligatorio: sì

## EnhancedApprovals

Questo input viene utilizzato solo per i modelli Change Manager. Un elenco di responsabili AWS autenticati che possono approvare o rifiutare l'azione, il tipo di responsabile IAM e il numero minimo di approvatori. Di seguito è riportato un esempio:

```
schemaVersion: "0.3"
emergencyChange: false
autoApprovable: false
mainSteps:
 - name: ApproveAction1
 action: aws:approve
 timeoutSeconds: 604800
 inputs:
 Message: Please approve this change request
 MinRequiredApprovals: 3
 EnhancedApprovals:
 Approvers:
```

```
- approver: John Stiles
type: IamUser
minRequiredApprovals: 0
- approver: Ana Carolina Silva
type: IamUser
minRequiredApprovals: 0
- approver: GroupOfThree
type: IamGroup
minRequiredApprovals: 0
- approver: RoleOfTen
type: IamRole
minRequiredApprovals: 0
```

Tipo: StringList

Obbligatorio: sì

## Output

### ApprovalStatus

Stato di approvazione della fase. Lo stato può avere uno dei seguenti valori: Approvato, Rifiutato o In attesa. "In attesa" indica che l'automazione è in attesa di input dagli approvatori.

Tipo: String

### ApproverDecisions

Mappa JSON che include la decisione di approvazione di ciascun approvatore.

Tipo: MapList

## **aws:assert – Assert AwsResourceProperty** AWS stato della risorsa o stato dell'evento

L'azione `aws:assertAwsResourceProperty` consente di affermare uno stato specifico della risorsa o dell'evento per una fase di automazione specifica.

### Note

L'azione `aws:assertAwsResourceProperty` supporta un nuovo tentativo di limitazione (della larghezza di banda della rete) automatico. Per ulteriori informazioni, consulta

Configurazione della ripetizione dei tentativi automatica per le operazioni di limitazione (della larghezza di banda della rete).

Per ulteriori esempi di utilizzo di questa operazione, consulta [Ulteriori esempi di runbook](#).

## Input

Gli input vengono definiti dall'operazione API selezionata.

## YAML

```
action: aws:assertAwsResourceProperty
inputs:
 Service: The official namespace of the service
 Api: The API operation or method name
 API operation inputs or parameters: A value
 PropertySelector: Response object
 DesiredValues:
 - Desired property values
```

## JSON

```
{
 "action": "aws:assertAwsResourceProperty",
 "inputs": {
 "Service": "The official namespace of the service",
 "Api": "The API operation or method name",
 "API operation inputs or parameters": "A value",
 "PropertySelector": "Response object",
 "DesiredValues": [
 "Desired property values"
]
 }
}
```

## Servizio

Lo spazio Servizio AWS dei nomi che contiene l'operazione API da eseguire. Ad esempio, il namespace per Systems Manager è ssm. Il namespace per Amazon EC2 è ec2. Puoi visualizzare



un elenco di namespace di Servizio AWS supportati nella sezione [Servizi disponibili](#) della Documentazione di riferimento al comando della AWS CLI .

Tipo: String

Obbligatorio: sì

## Api

Nome dell'operazione API da eseguire. Puoi visualizzare le operazioni API (definite anche metodi) scegliendo un servizio nel pannello di navigazione a sinistra nella pagina [Documentazione di riferimento ai servizi](#). Scegliere un metodo nella sezione Client del servizio che si desidera chiamare. Ad esempio, tutte le operazioni API (metodi) per Amazon Relational Database Service (Amazon RDS) sono elencate nella seguente pagina: [Amazon RDS methods](#) (Metodi Amazon RDS).

Tipo: stringa

Campo obbligatorio: sì

## Input dell'operazione API

Uno o più input dell'operazione API. Puoi visualizzare gli input disponibili (definiti anche parametri) scegliendo un servizio nel pannello di navigazione a sinistra nella pagina [Documentazione di riferimento ai servizi](#). Scegliere un metodo nella sezione Client del servizio che si desidera chiamare. Ad esempio, tutti i metodi per Amazon RDS sono elencati nella pagina: [metodi di Amazon RDS](#). Scegli il [metodo](#) `describe_db_instances` e scorri verso il basso per visualizzare i parametri disponibili, ad esempio Nome e Valori. `DBInstanceIdentifier` Usare il seguente formato per specificare più di un input.

## YAML

```
inputs:
 Service: The official namespace of the service
 Api: The API operation name
 API input 1: A value
 API Input 2: A value
 API Input 3: A value
```

## JSON

```
"inputs":{
```

```
"Service": "The official namespace of the service",
"Api": "The API operation name",
"API input 1": "A value",
"API Input 2": "A value",
"API Input 3": "A value"
}
```

Tipo: determinato dall'operazione API selezionata

Obbligatorio: sì

PropertySelector

Elemento JSONPath di un attributo specifico nell'oggetto di risposta. Puoi visualizzare gli oggetti di risposta scegliendo un servizio nel pannello di navigazione a sinistra nella pagina [Documentazione di riferimento ai servizi](#). Scegliere un metodo nella sezione Client del servizio che si desidera chiamare. Ad esempio, tutti i metodi per Amazon RDS sono elencati nella pagina: [metodi di Amazon RDS](#). Scegliere il metodo [describe\\_db\\_instances](#) e scorrere fino alla sezione Struttura risposta. DBInstances è presente nell'elenco come oggetto di risposta.

Tipo: String

Obbligatorio: sì

DesiredValues

Stato previsto o stato con il quale continuare l'automazione. Se specifichi un valore booleano, devi utilizzare una lettera maiuscola, ad esempio True o False.

Tipo: StringList

Obbligatorio: sì

**aws:branch** — Esegue passaggi di automazione condizionali

L'aws:branchazione consente di creare un'automazione dinamica che valuta diverse scelte in un unico passaggio e poi passa a una fase diversa del runbook in base ai risultati di tale valutazione.

Quando per una fase viene specificata l'operazione aws:branch, è necessario specificare l'elemento Choices l'automazione deve valutare. ChoicesPuò essere basato su un valore della Parameters sezione del runbook o su un valore dinamico generato come output dal passaggio

precedente. L'automazione valuta ogni scelta utilizzando un'espressione booleana. Se la prima scelta è "true", l'automazione passa alla fase definita per tale scelta. Se la prima scelta è "false", l'automazione valuta la scelta successiva. L'automazione continua la valutazione di ogni scelta finché non elabora una scelta "true". L'automazione passa quindi alla fase definita per la scelta di tipo "true".

Se nessuna delle scelte restituisce "true", l'automazione controlla se la fase contiene un valore di default. Un valore di default definisce una fase in cui l'automazione deve passare se nessuna delle scelte restituisce "true". Se non è stato specificato alcun valore di default per la fase, l'automazione elabora la fase successiva nel runbook.

L'operazione `aws:branch` supporta valutazioni di scelte complesse mediante l'uso di una combinazione di operatori `And`, `Not` e `Or`. Per ulteriori informazioni su come utilizzare `aws:branch`, con runbook di esempio ed esempi che utilizzano diversi operatori, consulta [Utilizzo di istruzioni condizionali nei runbook](#).

## Input

Specificare uno o più elementi `Choices` in una fase. L'elemento `Choices` può fare riferimento a un valore specificato nella sezione `Parameters` del runbook oppure a un valore dinamico generato come output di una fase precedente. Ecco un esempio di sintassi YAML che restituisce un parametro.

```
mainSteps:
- name: chooseOS
 action: aws:branch
 inputs:
 Choices:
 - NextStep: runWindowsCommand
 Variable: "{{Name of a parameter defined in the Parameters section. For example: OS_name}}"
 StringEquals: windows
 - NextStep: runLinuxCommand
 Variable: "{{Name of a parameter defined in the Parameters section. For example: OS_name}}"
 StringEquals: linux
 Default:
 sleep3
```

Ecco un esempio di sintassi YAML che valuta l'output di una fase precedente.

```
mainSteps:
```

```
- name: chooseOS
 action: aws:branch
 inputs:
 Choices:
 - NextStep: runPowerShellCommand
 Variable: "{{Name of a response object. For example: GetInstance.platform}}"
 StringEquals: Windows
 - NextStep: runShellCommand
 Variable: "{{Name of a response object. For example: GetInstance.platform}}"
 StringEquals: Linux
 Default:
 sleep3
```

## Choices

Una o più espressioni che il servizio di automazione deve valutare durante l'individuazione della fase successiva da elaborare. Le scelte vengono valutate utilizzando un'espressione booleana. Ogni scelta deve definire le seguenti opzioni:

- **NextStep:** La fase successiva del runbook da elaborare se la scelta designata è vera.
- **Variable:** specifica il nome di un parametro definito nella sezione `Parameters` del runbook. In alternativa, specifica un oggetto di output della fase precedente nel runbook. Per ulteriori informazioni sulla creazione di variabili per `aws:branch`, consulta [Informazioni sulla creazione della variabile di output](#).
- **Operation:** i criteri utilizzati per valutare la scelta. L'operazione `aws:branch` supporta le operazioni seguenti:

### Operazioni di stringa

- `StringEquals`
- `EqualsIgnoreCase`
- `StartsWith`
- `EndsWith`
- `Contiene`

### Operazioni numeriche

- `NumericEquals`
- `NumericGreater`
- `NumericLesser`

- NumericGreaterOrEquals
- NumericLesser
- NumericLesserOrEquals

#### Operazioni booleane

- BooleanEquals

#### Important

Quando si crea un runbook, il sistema convalida ogni operazione nel runbook. Se un'operazione non è supportata, il sistema restituisce un errore quando si tenta di creare il runbook.

#### Predefinito

Nome di una fase a cui l'automazione deve passare se nessuno degli elementi Choices restituisce "true".

─Tipo: stringa

Obbligatorio: no

#### Note

L'operazione `aws:branch` supporta gli operatori And, Or e Not. Per esempi di operazioni `aws:branch` che utilizzano gli operatori, consulta [Utilizzo di istruzioni condizionali nei runbook](#).

### **aws:change InstanceState** — Cambia o afferma lo stato dell'istanza

Modifica o rileva lo stato dell'istanza.

Questa operazione può essere utilizzata in modalità presuntiva (non esegue l'API per modificare lo stato, ma verifica se l'istanza è nello stato desiderato). Per utilizzare la modalità presuntiva, impostare il parametro `CheckStateOnly` su `true`. Questa modalità è utile, quando si esegue il comando Sysprep in Windows Server, in quanto si tratta di un comando asincrono, eseguibile in background

per lunghi periodi di tempo. Puoi assicurarti che l'istanza venga interrotta prima di creare una Amazon Machine Image (). AMI

#### Note

Il valore di timeout predefinito per questa operazione è 3600 secondi (un'ora). Puoi limitare o estendere il timeout specificando il parametro `timeoutSeconds` per una fase `aws:changeInstanceState`.

#### Note

L'azione `aws:changeInstanceState` supporta un nuovo tentativo di limitazione (della larghezza di banda della rete) automatico. Per ulteriori informazioni, consulta [Configurazione della ripetizione dei tentativi automatica per le operazioni di limitazione \(della larghezza di banda della rete\)](#).

## Input

## YAML

```
name: startMyInstance
action: aws:changeInstanceState
maxAttempts: 3
timeoutSeconds: 3600
onFailure: Abort
inputs:
 InstanceIds:
 - i-1234567890abcdef0
 CheckStateOnly: true
 DesiredState: running
 FailOnUnexpectedStopped: true
```

## JSON

```
{
 "name": "startMyInstance",
 "action": "aws:changeInstanceState",
 "maxAttempts": 3,
```

```
"timeoutSeconds": 3600,
"onFailure": "Abort",
"inputs": {
 "InstanceIds": ["i-1234567890abcdef0"],
 "CheckStateOnly": true,
 "DesiredState": "running",
 "FailOnUnexpectedStopped": true
}
}
```

## InstanceIds

ID delle istanze.

Tipo: StringList

Obbligatorio: sì

## CheckStateOnly

Se false, imposta lo stato dell'istanza sullo stato desiderato. Se true, presume lo stato desiderato utilizzando il polling.

Impostazione predefinita: false

Tipo: Booleano

Obbligatorio: no

## DesiredState

Stato desiderato. Se è impostata su `running`, questa operazione attende che lo stato di Amazon EC2 sia `Running`, lo stato dell'istanza sia `OK` e lo stato del sistema sia `OK` prima del completamento.

Tipo: stringa

Valori validi: `running` | `stopped` | `terminated`

Obbligatorio: sì

## Force

Se impostato, forza l'arresto delle istanze. Le istanze non hanno la possibilità di svuotare le cache o i metadati del file system. Se utilizzi questa opzione, devi eseguire le procedure di verifica e

riparazione del file system. Questa opzione non è consigliata per le istanze di EC2 di Windows Server.

Tipo: Booleano

Obbligatorio: no

#### FailOnUnexpectedStopped

Se impostato su true, la fase di automazione ha esito negativo quando un'istanza passa allo stato di arresto durante un'operazione di avvio. Ciò è utile per rilevare i casi in cui un'istanza non riesce ad avviarsi correttamente, ad esempio quando un'istanza ha un volume EBS crittografato ma non dispone delle autorizzazioni di chiave KMS richieste.

Tipo: Booleano

Obbligatorio: no

#### AdditionalInfo

Riservata.

─Tipo: stringa

Obbligatorio: no

#### Output

Nessuno

**aws:copyImage:** copia o crittografa un'Amazon Machine Image

Copia un Amazon Machine Image (AMI) da qualsiasi Regione AWS nella regione corrente. Questa operazione consente inoltre di crittografare la nuova AMI.

#### Note

L'azione `aws:copyImage` supporta un nuovo tentativo di limitazione (della larghezza di banda della rete) automatico. Per ulteriori informazioni, consulta [Configurazione della ripetizione dei tentativi automatica per le operazioni di limitazione \(della larghezza di banda della rete\)](#).



## Input

Questa operazione supporta la maggior parte dei parametri CopyImage. Per ulteriori informazioni, consulta [CopyImage](#).

L'esempio seguente crea una copia di un'AMI nella regione di Seoul (SourceImageID: ami-0fe10819. SourceRegion: ap-northeast-2). La nuova AMI viene copiata nella regione in cui è stata avviata l'operazione di automazione. L'AMI copiata verrà crittografata perché il flag Encrypted facoltativo è impostato su true.

## YAML

```
name: createEncryptedCopy
action: aws:copyImage
maxAttempts: 3
onFailure: Abort
inputs:
 SourceImageId: ami-0fe10819
 SourceRegion: ap-northeast-2
 ImageName: Encrypted Copy of LAMP base AMI in ap-northeast-2
 Encrypted: true
```

## JSON

```
{
 "name": "createEncryptedCopy",
 "action": "aws:copyImage",
 "maxAttempts": 3,
 "onFailure": "Abort",
 "inputs": {
 "SourceImageId": "ami-0fe10819",
 "SourceRegion": "ap-northeast-2",
 "ImageName": "Encrypted Copy of LAMP base AMI in ap-northeast-2",
 "Encrypted": true
 }
}
```

## SourceRegion

Regione in cui esiste l'AMI di origine.

Tipo: stringa

Obbligatorio: sì

SourceImageId

ID dell'AMI da copiare dalla regione di origine.

Tipo: stringa

Obbligatorio: sì

ImageName

Nome della nuova immagine.

Tipo: stringa

Obbligatorio: sì

ImageDescription

Descrizione dell'immagine di destinazione.

─Tipo: stringa

Obbligatorio: no

Crittografato

Crittografa l'AMI di destinazione.

Tipo: Booleano

Obbligatorio: no

KmsKeyId

L'Amazon Resource Name (ARN) completo AWS KMS key da utilizzare per crittografare le istantanee di un'immagine durante un'operazione di copia. Per ulteriori informazioni, consulta [CopyImage](#).

─Tipo: stringa

Obbligatorio: no

ClientToken

Identificatore univoco con distinzione tra maiuscole e minuscole che fornisci per assicurare l'idempotenza della richiesta. Per ulteriori informazioni, consulta [CopyImage](#).

▪Tipo: stringa

Obbligatorio: no

## Output

### ImageId

ID dell'immagine copiata.

### ImageState

Stato dell'immagine copiata.

Valori validi: available | pending | failed

**aws:createImage:** creazione di un'Amazon Machine Image

Crea un'Amazon Machine Image (AMI) da un'istanza in esecuzione, in arresto o già arrestata, e vota affinché ImageState sia available.

#### Note

L'azione `aws:createImage` supporta un nuovo tentativo di limitazione (della larghezza di banda della rete) automatico. Per ulteriori informazioni, consulta [Configurazione della ripetizione dei tentativi automatica per le operazioni di limitazione \(della larghezza di banda della rete\)](#).

## Input

Questa azione supporta i seguenti parametri `CreateImage`. Per ulteriori informazioni, consulta [CreateImage](#).

## YAML

```
name: createMyImage
action: aws:createImage
maxAttempts: 3
onFailure: Abort
```

```
inputs:
 InstanceId: i-1234567890abcdef0
 ImageName: AMI Created on{{global:DATE_TIME}}
 NoReboot: true
 ImageDescription: My newly created AMI
```

## JSON

```
{
 "name": "createMyImage",
 "action": "aws:createImage",
 "maxAttempts": 3,
 "onFailure": "Abort",
 "inputs": {
 "InstanceId": "i-1234567890abcdef0",
 "ImageName": "AMI Created on{{global:DATE_TIME}}",
 "NoReboot": true,
 "ImageDescription": "My newly created AMI"
 }
}
```

### InstanceId

ID dell'istanza.

Tipo: stringa

Obbligatorio: sì

### ImageName

Nome dell'immagine.

Tipo: stringa

Obbligatorio: sì

### ImageDescription

Descrizione dell'immagine.

─Tipo: stringa

Obbligatorio: no

## NoReboot

Valore letterale booleano.

Per impostazione predefinita, Amazon Elastic Compute Cloud (Amazon EC2) tenta di arrestare e riavviare l'istanza prima di creare l'immagine. Se l'opzione No Reboot (Non riavviare) è impostata su `true`, Amazon EC2 non arresta l'istanza prima di creare l'immagine. Quando viene utilizzata questa opzione, non è garantita l'integrità del file system per l'immagine creata.

Se non desideri che l'istanza venga eseguita dopo averne creata una AMI da essa, utilizza prima [l'aws:change InstanceState — Cambia o afferma lo stato dell'istanza](#) azione per arrestare l'istanza, quindi utilizza questa `aws:createImage` azione con l'`NoReboot` opzione impostata su `true`.

Tipo: Booleano

Obbligatorio: no

## BlockDeviceMappings

Dispositivi a blocchi per l'istanza.

Tipo: Map

Obbligatorio: no

## Output

### ImageId

ID della nuova immagine creata.

Tipo: String

### ImageState

Lo stato corrente dell'immagine. Se lo stato è disponibile, l'immagine viene registrata correttamente e può essere utilizzata per avviare un'istanza.

Tipo: String

## AWS:CreateStack – Crea un CloudFormation stack

Crea una AWS CloudFormation pila da un modello.

### Note

L'azione `aws:createStack` supporta un nuovo tentativo di limitazione (della larghezza di banda della rete) automatico. Per ulteriori informazioni, consulta [Configurazione della ripetizione dei tentativi automatica per le operazioni di limitazione \(della larghezza di banda della rete\)](#).

Per ulteriori informazioni sulla creazione di CloudFormation stack, consulta [CreateStack](#) l'AWS CloudFormation API Reference.

### Input

### YAML

```
name: makeStack
action: aws:createStack
maxAttempts: 1
onFailure: Abort
inputs:
 Capabilities:
 - CAPABILITY_IAM
 StackName: myStack
 TemplateURL: http://s3.amazonaws.com/amzn-s3-demo-bucket/myStackTemplate
 TimeoutInMinutes: 5
 Parameters:
 - ParameterKey: LambdaRoleArn
 ParameterValue: "{{LambdaAssumeRole}}"
 - ParameterKey: createdResource
 ParameterValue: createdResource-{{automation:EXECUTION_ID}}
```

### JSON

```
{
 "name": "makeStack",
 "action": "aws:createStack",
 "maxAttempts": 1,
```

```
"onFailure": "Abort",
"inputs": {
 "Capabilities": [
 "CAPABILITY_IAM"
],
 "StackName": "myStack",
 "TemplateURL": "http://s3.amazonaws.com/amzn-s3-demo-bucket/
myStackTemplate",
 "TimeoutInMinutes": 5,
 "Parameters": [
 {
 "ParameterKey": "LambdaRoleArn",
 "ParameterValue": "{{LambdaAssumeRole}}"
 },
 {
 "ParameterKey": "createdResource",
 "ParameterValue": "createdResource-{{automation:EXECUTION_ID}}"
 }
]
}
```

## Funzionalità

Un elenco di valori specificati in precedenza CloudFormation può creare determinati stack. Alcuni modelli di stack includono risorse che possono influire sulle autorizzazioni del tuo Account AWS. Per questi stack, è necessario confermare in modo esplicito le relative funzionalità specificando questo parametro.

I valori validi includono CAPABILITY\_IAM, CAPABILITY\_NAMED\_IAM e CAPABILITY\_AUTO\_EXPAND.

### CAPABILITY\_IAM e CAPABILITY\_NAMED\_IAM

Se sono presenti risorse IAM, è possibile specificare una delle funzionalità. In presenza di risorse IAM con nomi personalizzati, devi specificare CAPABILITY\_NAMED\_IAM. Se non specifichi questo parametro, questa operazione restituisce un errore `InsufficientCapabilities`. Le seguenti risorse richiedono di specificare CAPABILITY\_IAM o CAPABILITY\_NAMED\_IAM.

- [AWS::IAM::AccessKey](#)
- [AWS::IAM::Group](#)
- [AWS::IAM::InstanceProfile](#)

- [AWS::IAM::Policy](#)
- [AWS::IAM::Role](#)
- [AWS::IAM::User](#)
- [AWS::IAM::UserToGroupAddition](#)

Se il modello di stack contiene queste risorse, ti consigliamo di esaminare tutte le autorizzazioni a esse associate e modificarle, se necessario.

Per ulteriori informazioni, consulta [Riconoscere le risorse IAM nei CloudFormation modelli](#).

## CAPABILITY\_AUTO\_EXPAND

Alcuni modelli contengono macro. Le macro consentono di eseguire l'elaborazione personalizzata su modelli, da semplici operazioni quali ricerca e sostituzione ad ampie trasformazioni di interi modelli. Per questo motivo, gli utenti in genere creano un set di modifiche dal modello elaborato, in modo che possano rivedere le modifiche risultanti dalle macro prima di creare effettivamente lo stack. Se il modello di stack contiene una o più macro e si sceglie di creare uno stack direttamente dal modello elaborato, senza prima esaminare le modifiche risultanti in un set di modifiche, è necessario riconoscere questa funzionalità.

Per ulteriori informazioni, consulta [Utilizzo delle AWS CloudFormation macro per eseguire l'elaborazione personalizzata sui modelli](#) nella Guida per l'AWS CloudFormation utente.

Tipo: Array of Strings

Valori validi: CAPABILITY\_IAM | CAPABILITY\_NAMED\_IAM | CAPABILITY\_AUTO\_EXPAND

Campo obbligatorio: no

## ClientRequestToken

Un identificatore univoco per questa CreateStack richiesta. Specifica questo token se imposti maxAttempts in questa fase su un valore maggiore di 1. Specificando questo token, CloudFormation sa che non stai tentando di creare un nuovo stack con lo stesso nome.

─Tipo: stringa

Obbligatorio: no

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 128 caratteri.



Schema: [a-zA-Z0-9] [-a-z] \* A-Z0-9

## DisableRollback

Imposta su `true` per disattivare il rollback dello stack se la creazione dello stack ha esito negativo.

Condizionale: puoi specificare il parametro `DisableRollback` o il parametro `OnFailure`, ma non entrambi.

Impostazione predefinita: `false`

Tipo: Booleano

Obbligatorio: no

## NotificationARNs

Gli ARN dell'argomento Amazon Simple Notification Service (Amazon SNS) per pubblicare eventi correlati allo stack. Puoi trovare gli ARN degli argomenti SNS utilizzando la console Amazon SNS, <https://console.aws.amazon.com/sns/v3/home>

Tipo: Array of Strings

Membri della matrice: numero massimo di 5 elementi.

Obbligatorio: no

## OnFailure

Determina l'operazione da eseguire se la creazione dello stack ha esito negativo. È necessario specificare `DO_NOTHING`, `ROLLBACK` o `DELETE`.

Condizionale: puoi specificare il parametro `OnFailure` o il parametro `DisableRollback`, ma non entrambi.

Impostazione predefinita: `ROLLBACK`

Tipo: stringa

Valori validi: `DO_NOTHING` | `ROLLBACK` | `DELETE`

Obbligatorio: no

## Parameters

Elenco di strutture `Parameter` che specificano i parametri di input per lo stack. Per ulteriori informazioni, consulta il tipo di dati [Parameter](#).

Tipo: matrice di oggetti [Parametro](#)

Obbligatorio: no

## ResourceTypes

Tipi di risorse modello che si è autorizzati a utilizzare per questa operazione di creazione dello stack. Ad esempio: `AWS::EC2::Instance`, `AWS::EC2::*` o `Custom::MyCustomInstance`. Utilizza la seguente sintassi per descrivere i tipi di risorse modello.

- Per tutte le risorse: AWS

```
AWS::*
```

- Per tutte le risorse personalizzate:

```
Custom::*
```

- Per una risorsa personalizzata specifica:

```
Custom::logical_ID
```

- Per tutte le risorse di un particolare Servizio AWS:

```
AWS::service_name::*
```

- Per una AWS risorsa specifica:

```
AWS::service_name::resource_logical_ID
```

Se l'elenco dei tipi di risorse non include una risorsa in fase di creazione, la creazione dello stack ha esito negativo. Per impostazione predefinita, CloudFormation concede le autorizzazioni a tutti i tipi di risorse. IAM utilizza questo parametro per le chiavi di CloudFormation-specific condizione nelle policy IAM. Per ulteriori informazioni, consulta [Controlling Access with AWS Identity and Access Management](#).

Tipo: Array of Strings

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Obbligatorio: no

## RoleARN

L'Amazon Resource Name (ARN) di un ruolo IAM che CloudFormation presuppone la creazione dello stack. CloudFormation utilizza le credenziali del ruolo per effettuare chiamate per tuo conto. CloudFormation utilizza sempre questo ruolo per tutte le future operazioni sullo stack. Se gli utenti dispongono dell'autorizzazione per intervenire sullo stack, CloudFormation usa questo ruolo anche se gli utenti non sono autorizzati a passare tale parametro. Assicurati che il ruolo conceda il minor numero di privilegi.

Se non specifichi un valore, CloudFormation utilizza il ruolo precedentemente associato allo stack. Se non è disponibile alcun ruolo, CloudFormation utilizza una sessione temporanea generata dalle credenziali dell'utente.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Obbligatorio: no

## StackName

Nome associato allo stack. Il nome deve essere univoco nella regione in cui si sta creando lo stack.

### Note

Il nome di uno stack può contenere solo caratteri alfanumerici (con distinzione tra lettere maiuscole e minuscole) e trattini. Deve iniziare con un carattere alfabetico e non può avere una lunghezza superiore a 128 caratteri.

Tipo: stringa

Obbligatorio: sì

## StackPolicyBody

Struttura contenente il corpo della policy dello stack. Per ulteriori informazioni, consulta [Impedire gli aggiornamenti delle risorse stack](#).

Condizionale: puoi specificare il parametro `StackPolicyBody` o il parametro `StackPolicyURL`, ma non entrambi.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 16384 caratteri.

Obbligatorio: no

#### StackPolicyURL

Posizione di un file contenente la policy dello stack. L'URL deve puntare a una policy che si trova in un bucket S3 nella stessa regione dello stack. La dimensione massima consentita del file della policy dello stack è 16 KB.

Condizionale: puoi specificare il parametro `StackPolicyBody` o il parametro `StackPolicyURL`, ma non entrambi.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 1350 caratteri.

Obbligatorio: no

#### Tag

Key-value coppie da associare a questo stack. CloudFormation inoltre propaga questi tag alle risorse create nello stack. Puoi specificare un massimo di 10 tag.

Tipo: matrice di oggetti [Tag](#)

Obbligatorio: no

#### TemplateBody

Struttura contenente il corpo del modello con una lunghezza minima di 1 byte e una lunghezza massima di 51.200 byte. Per ulteriori informazioni, consulta [Anatomia dei modelli](#).

Condizionale: puoi specificare il parametro `TemplateBody` o il parametro `TemplateURL`, ma non entrambi.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1.

Obbligatorio: no

## TemplateURL

Posizione di un file contenente il corpo del modello. L'URL deve puntare a un modello che si trova in un bucket S3. La dimensione massima consentita per il modello è 460.800 byte. Per ulteriori informazioni, consulta [Anatomia dei modelli](#).

Condizionale: puoi specificare il parametro `TemplateBody` o il parametro `TemplateURL`, ma non entrambi.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 1024 caratteri.

Obbligatorio: no

## TimeoutInMinutes

Intervallo di tempo che può trascorrere prima che lo stato dello stack diventi `CREATE_FAILED`. Se `DisableRollback` non è impostato o è impostato su `false`, verrà eseguito il rollback dello stack.

Tipo: numero intero

Intervallo valido: valore minimo di 1.

Obbligatorio: no

## Output

### StackId

Identificatore univoco dello stack.

Tipo: stringa

### StackStatus

Stato corrente dello stack.

Tipo: stringa

Valori validi: `CREATE_IN_PROGRESS` | `CREATE_FAILED` | `CREATE_COMPLETE`  
| `ROLLBACK_IN_PROGRESS` | `ROLLBACK_FAILED` | `ROLLBACK_COMPLETE`

| DELETE\_IN\_PROGRESS | DELETE\_FAILED | DELETE\_COMPLETE |  
UPDATE\_IN\_PROGRESS | UPDATE\_COMPLETE\_CLEANUP\_IN\_PROGRESS |  
UPDATE\_COMPLETE | UPDATE\_ROLLBACK\_IN\_PROGRESS | UPDATE\_ROLLBACK\_FAILED |  
UPDATE\_ROLLBACK\_COMPLETE\_CLEANUP\_IN\_PROGRESS | UPDATE\_ROLLBACK\_COMPLETE  
| REVIEW\_IN\_PROGRESS

Obbligatorio: sì

## StackStatusReason

Messaggio di operazione riuscita o non riuscita associato allo stato dello stack.

─Tipo: stringa

Obbligatorio: no

Per ulteriori informazioni, consulta [CreateStack](#).

## Considerazioni relative alla sicurezza

Prima di utilizzare l'operazione `aws:createStack`, devi assegnare la seguente policy al ruolo presunto del servizio di automazione di IAM. Per ulteriori informazioni sul ruolo presunto, consulta [Processo 1: creazione di un ruolo di servizio per il servizio di automazione](#).

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "sqs:*",
 "cloudformation:CreateStack",
 "cloudformation:DescribeStacks"
],
 "Resource": "*"
 }
]
}
```

## AWS:createTags — Crea tag per AWS risorse

Crea nuovi tag per istanze Amazon Elastic Compute Cloud (Amazon EC2) o istanze gestite. AWS Systems Manager

### Note

L'azione `aws:createTags` supporta un nuovo tentativo di limitazione (della larghezza di banda della rete) automatico. Per ulteriori informazioni, consulta [Configurazione della ripetizione dei tentativi automatica per le operazioni di limitazione \(della larghezza di banda della rete\)](#).

### Input

Questa operazione supporta la maggior parte di parametri `CreateTags` di Amazon EC2 e di `AddTagsToResource` di Systems Manager. Per ulteriori informazioni, consulta [CreateTags](#) e [AddTagsToResource](#).

L'esempio seguente mostra come contrassegnare mediante tag un'Amazon Machine Image (AMI) e un'istanza come risorse di produzione per un determinato reparto.

### YAML

```
name: createTags
action: aws:createTags
maxAttempts: 3
onFailure: Abort
inputs:
 ResourceType: EC2
 ResourceIds:
 - ami-9a3768fa
 - i-02951acd5111a8169
 Tags:
 - Key: production
 Value: ''
 - Key: department
 Value: devops
```

### JSON

```
{
```

```
{
 "name": "createTags",
 "action": "aws:createTags",
 "maxAttempts": 3,
 "onFailure": "Abort",
 "inputs": {
 "ResourceType": "EC2",
 "ResourceIds": [
 "ami-9a3768fa",
 "i-02951acd5111a8169"
],
 "Tags": [
 {
 "Key": "production",
 "Value": ""
 },
 {
 "Key": "department",
 "Value": "devops"
 }
]
 }
}
```

## ResourceIds

ID della risorsa o delle risorse da contrassegnare mediante tag. Se il tipo di risorsa non è «EC2», questo campo può contenere un solo elemento.

Tipo: StringList

Obbligatorio: sì

## Tag

Tag da associare alla risorsa o alle risorse.

Tipo: elenco di mappe

Obbligatorio: sì

## ResourceType

Tipo della risorsa o delle risorse da contrassegnare mediante tag. Se non viene fornito, viene utilizzato il valore predefinito «EC2».



■Tipo: stringa

Obbligatorio: no

Valori validi: EC2 | ManagedInstance | MaintenanceWindow | Parameter

## Output

Nessuno

**aws:deleteImage:** eliminazione di un'Amazon Machine Image

Elimina l'Amazon Machine Image (AMI) specificata e tutti gli snapshot correlati.

### Note

L'azione `aws:deleteImage` supporta un nuovo tentativo di limitazione (della larghezza di banda della rete) automatico. Per ulteriori informazioni, consulta [Configurazione della ripetizione dei tentativi automatica per le operazioni di limitazione \(della larghezza di banda della rete\)](#).

## Input

Questa operazione supporta un solo parametro. Per ulteriori informazioni, consulta la documentazione relativa a [DeregisterImage](#) e [DeleteSnapshot](#).

## YAML

```
name: deleteMyImage
action: aws:deleteImage
maxAttempts: 3
timeoutSeconds: 180
onFailure: Abort
inputs:
 ImageId: ami-12345678
```

## JSON

```
{
```

```
"name": "deleteMyImage",
"action": "aws:deleteImage",
"maxAttempts": 3,
"timeoutSeconds": 180,
"onFailure": "Abort",
"inputs": {
 "ImageId": "ami-12345678"
}
}
```

## ImageId

ID dell'immagine da eliminare.

Tipo: stringa

Obbligatorio: sì

## Output

Nessuno

## AWS:DeleteStack – Elimina un CloudFormation stack

Elimina una AWS CloudFormation pila.

### Note

L'azione `aws:deleteStack` supporta un nuovo tentativo di limitazione (della larghezza di banda della rete) automatico. Per ulteriori informazioni, consulta [Configurazione della ripetizione dei tentativi automatica per le operazioni di limitazione \(della larghezza di banda della rete\)](#).

## Input

## YAML

```
name: deleteStack
action: aws:deleteStack
```

```
maxAttempts: 1
onFailure: Abort
inputs:
 StackName: "{{stackName}}"
```

## JSON

```
{
 "name": "deleteStack",
 "action": "aws:deleteStack",
 "maxAttempts": 1,
 "onFailure": "Abort",
 "inputs": {
 "StackName": "{{stackName}}"
 }
}
```

## ClientRequestToken

Identificatore univoco per la richiesta DeleteStack. Specifica questo token se intendi riprovare le richieste in modo che CloudFormation sappia che non stai tentando di eliminare uno stack con lo stesso nome. Puoi riprovare l'esecuzione delle richieste DeleteStack per verificare che CloudFormation le abbia ricevute.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 128 caratteri.

Schema: [a-zA-Z] [-a-z] \* A-Z0-9

Obbligatorio: no

## RetainResources.member.N

Questo input è valido solo per gli stack il cui stato è DELETE\_FAILED. Elenco di ID di risorse logiche per le risorse da conservare. Durante l'eliminazione, CloudFormation elimina lo stack, ma non elimina le risorse conservate.

La conservazione delle risorse è utile quando non è possibile eliminare una risorsa, ad esempio un bucket S3 non vuoto, ma si desidera eliminare lo stack.

Tipo: Array of Strings

Obbligatorio: no

## RoleARN

L'Amazon Resource Name (ARN) di un ruolo AWS Identity and Access Management (IAM) che CloudFormation presuppone la creazione dello stack. CloudFormation utilizza le credenziali del ruolo per effettuare chiamate per tuo conto. CloudFormation utilizza sempre questo ruolo per tutte le future operazioni sullo stack. Se gli utenti dispongono dell'autorizzazione per operare sullo stack, CloudFormation utilizza questo ruolo anche se gli utenti non sono autorizzati a passarlo. Assicurati che il ruolo conceda il minor numero di privilegi.

Se non specifichi un valore, CloudFormation utilizza il ruolo precedentemente associato allo stack. Se non è disponibile alcun ruolo, CloudFormation utilizza una sessione temporanea generata dalle credenziali dell'utente.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Obbligatorio: no

## StackName

Nome o ID stack univoco associato allo stack.

Tipo: stringa

Obbligatorio: sì

## Considerazioni relative alla sicurezza

Prima di utilizzare l'operazione `aws:deleteStack`, devi assegnare la seguente policy al ruolo presunto del servizio di automazione di IAM. Per ulteriori informazioni sul ruolo presunto, consulta [Processo 1: creazione di un ruolo di servizio per il servizio di automazione](#).

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
```

```
 "Effect": "Allow",
 "Action": [
 "sqs:*",
 "cloudformation:DeleteStack",
 "cloudformation:DescribeStacks"
],
 "Resource": "*"
 }
]
```

## AWS:ExecuteAutomation – Esegui un'altra automazione

Esegui un'automazione secondaria mediante una chiamata a un runbook secondario. Questa operazione consente di creare runbook per le operazioni più comuni e fare riferimento a tali runbook durante l'automazione. Questa operazione permette di semplificare i runbook in quanto elimina la necessità di duplicare le fasi tra runbook simili.

L'automazione secondaria viene eseguita nel contesto dell'utente che ha avviato l'automazione principale. Ciò significa che l'automazione secondaria utilizza lo stesso ruolo o utente AWS Identity and Access Management (IAM) dell'utente che ha avviato la prima automazione.

### Important

Se è necessario specificare i parametri in un'automazione secondaria che utilizza un ruolo presunto (un ruolo che usa la policy `iam:passRole`), l'utente o il ruolo che ha avviato l'automazione principale deve disporre dell'autorizzazione necessaria per passare il ruolo presunto specificato nell'automazione secondaria. Per ulteriori informazioni sulla configurazione di un ruolo presunto per l'automazione, consulta [Crea ruoli di servizio per l'automazione tramite la console](#).

## Input

### YAML

```
name: Secondary_Automation
action: aws:executeAutomation
maxAttempts: 3
timeoutSeconds: 3600
```

```
onFailure: Abort
inputs:
 DocumentName: secondaryAutomation
 RuntimeParameters:
 instanceIds:
 - i-1234567890abcdef0
```

## JSON

```
{
 "name": "Secondary_Automation",
 "action": "aws:executeAutomation",
 "maxAttempts": 3,
 "timeoutSeconds": 3600,
 "onFailure": "Abort",
 "inputs": {
 "DocumentName": "secondaryAutomation",
 "RuntimeParameters": {
 "instanceIds": [
 "i-1234567890abcdef0"
]
 }
 }
}
```

## DocumentName

Nome del runbook secondario da eseguire durante la fase. Per i runbook che utilizzano la stessa funzionalità Account AWS, specifica il nome del runbook. Per i runbook condivisi da un altro utente Account AWS, specifica l'Amazon Resource Name (ARN) del runbook. Per informazioni sull'uso di runbook condivisi, consulta [Utilizzo di documenti SSM condivisi](#).

Tipo: stringa

Obbligatorio: sì

## DocumentVersion

Versione del runbook secondario da eseguire. Se non è specificato, il servizio di automazione esegue la versione predefinita del runbook.

─Tipo: stringa

Obbligatorio: no

## MaxConcurrency

Il numero massimo di destinazioni consentito per eseguire questa operazione in parallelo. È possibile specificare un numero, ad esempio 10, o una percentuale, ad esempio 10%.

─Tipo: stringa

Obbligatorio: no

## MaxErrors

Numero di errori consentiti prima che il sistema interrompa l'esecuzione dell'automazione su destinazioni aggiuntive. Puoi specificare un numero assoluto di errori, ad esempio 10, oppure una percentuale della serie di destinazioni, ad esempio 10%. Se ad esempio specifichi 3, il sistema interrompe l'esecuzione dell'automazione quando riceve il quarto errore. Se specifichi 0, il sistema interrompe l'esecuzione dell'automazione su destinazioni aggiuntive dopo che viene restituito il risultato del primo errore. Se si esegue un'automazione su 50 risorse e si imposta `MaxErrors` sul 10%, il sistema interrompe l'esecuzione dell'automazione su destinazioni aggiuntive quando riceve il sesto errore.

Alle automazioni già in esecuzione al raggiungimento della soglia di `MaxErrors`, è permesso di arrivare al termine; tuttavia, queste automazioni potrebbero anche avere esito negativo. Se devi assicurarti che non ci siano più automazioni fallite di quelle specificate `MaxErrors`, imposta su 1 in modo che le automazioni procedano una `MaxConcurrency` alla volta.

─Tipo: stringa

Obbligatorio: no

## RuntimeParameters

Parametri obbligatori per il runbook secondario. La mappatura usa il seguente formato:  
`{"parameter1" : "value1", "parameter2" : "value2" }`

Tipo: Map

Obbligatorio: no

## Tag

I metadati facoltativi assegnati a una risorsa. È possibile specificare un massimo di cinque tag per un'automazione.

Tipo: MapList

Obbligatorio: no

## TargetLocations

Una posizione è una combinazione di Regioni AWS and/or Account AWS dove vuoi eseguire l'automazione. È necessario specificare un numero minimo di 1 elemento ed è possibile specificare un numero massimo di 100 elementi. Quando si specifica un valore per questo parametro, gli output non vengono restituiti all'automazione padre. Se necessario, bisogna effettuare chiamate successive alle operazioni API per recuperare l'output dalle automazioni figlio.

Tipo: MapList

Obbligatorio: no

## TargetMaps

Un elenco di mappature chiave-valore dei parametri del documento alle risorse di destinazione. Sia Targets che TargetMaps non possono essere specificati insieme.

Tipo: MapList

Obbligatorio: no

## TargetParameterName

Nome del parametro utilizzato come risorsa di destinazione per l'automazione controllata dalla velocità. Necessario solo se si specificano Targets.

─Tipo: stringa

Obbligatorio: no

## Target

Un elenco di mapping chiave-valore alle risorse di destinazione. Necessario solo se si specifica TargetParameterName.

Tipo: MapList

Obbligatorio: no



## Output

### Output

Output generato dall'automazione secondaria. È possibile fare riferimento all'output utilizzando il seguente formato: *Secondary\_Automation\_Step\_Name*.Output

Tipo: StringList

Ecco un esempio:

```
- name: launchNewWindowsInstance
 action: 'aws:executeAutomation'
 onFailure: Abort
 inputs:
 DocumentName: launchWindowsInstance
 nextStep: getNewInstanceRootVolume
- name: getNewInstanceRootVolume
 action: 'aws:executeAwsApi'
 onFailure: Abort
 inputs:
 Service: ec2
 Api: DescribeVolumes
 Filters:
 - Name: attachment.device
 Values:
 - /dev/sda1
 - Name: attachment.instance-id
 Values:
 - '{{launchNewWindowsInstance.Output}}'
 outputs:
 - Name: rootVolumeId
 Selector: '$.Volumes[0].VolumeId'
 Type: String
 nextStep: snapshotRootVolume
- name: snapshotRootVolume
 action: 'aws:executeAutomation'
 onFailure: Abort
 inputs:
 DocumentName: AWS-CreateSnapshot
 RuntimeParameters:
 VolumeId:
 - '{{getNewInstanceRootVolume.rootVolumeId}}'
 Description:
```

```
- 'Initial root snapshot for {{launchNewWindowsInstance.Output}}'
```

## ExecutionId

ID dell'automazione secondaria.

Tipo: stringa

## Stato

Stato dell'automazione secondaria.

Tipo: stringa

## **aws:execute AwsApi** — Chiama ed esegui AWS operazioni API

Chiama ed esegue operazioni AWS API. È supportata la maggior parte delle operazioni API, sebbene non tutte le operazioni API siano state sottoposte a test. Le operazioni API di streaming, come l'[GetObject](#) operazione, non sono supportate. Se non hai la certezza che un'operazione API che desideri utilizzare sia un'operazione di streaming, consulta la documentazione [Boto3](#) del servizio per stabilire se un'API richiede input o output di streaming. Aggiorniamo regolarmente la versione Boto3 utilizzata da questa operazione. Tuttavia, dopo il rilascio di una nuova versione di Boto3, possono essere necessarie alcune settimane prima che le modifiche vengano applicate in questa operazione. Ogni operazione `aws:executeAwsApi` può durare al massimo 25 secondi. Per ulteriori esempi di utilizzo di questa operazione, consulta [Ulteriori esempi di runbook](#).

### Note

L'azione `aws:executeAwsApi` supporta un nuovo tentativo di limitazione (della larghezza di banda della rete) automatico. Per ulteriori informazioni, consulta [Configurazione della ripetizione dei tentativi automatica per le operazioni di limitazione \(della larghezza di banda della rete\)](#).

## Input

Gli input vengono definiti dall'operazione API selezionata.

## YAML

```
action: aws:executeAwsApi
```

```
inputs:
 Service: The official namespace of the service
 Api: The API operation or method name
 API operation inputs or parameters: A value
outputs: # These are user-specified outputs
- Name: The name for a user-specified output key
 Selector: A response object specified by using jsonpath format
 Type: The data type
```

## JSON

```
{
 "action": "aws:executeAwsApi",
 "inputs": {
 "Service": "The official namespace of the service",
 "Api": "The API operation or method name",
 "API operation inputs or parameters": "A value"
 },
 "outputs": [These are user-specified outputs
 {
 "Name": "The name for a user-specified output key",
 "Selector": "A response object specified by using JSONPath format",
 "Type": "The data type"
 }
]
}
```

## Servizio

Lo spazio dei Servizio AWS nomi che contiene l'operazione API che desideri eseguire. [È possibile visualizzare un elenco di Servizio AWS namespace supportati in Servizi disponibili di.](#) AWS SDK per Python (Boto3) Il namespace è disponibile nella sezione Client. Ad esempio, il namespace per Systems Manager è ssm. Il namespace per Amazon Elastic Compute Cloud (Amazon EC2) è ec2.

Tipo: stringa

Obbligatorio: sì

## Api

Nome dell'operazione API da eseguire. Puoi visualizzare le operazioni API (definite anche metodi) scegliendo un servizio nel pannello di navigazione a sinistra nella pagina [Documentazione di riferimento ai servizi](#). Scegliere un metodo nella sezione Client del servizio che si desidera chiamare. Ad esempio, tutte le operazioni API (metodi) per Amazon Relational Database Service (Amazon RDS) sono elencate nella seguente pagina: [Amazon RDS methods](#) (Metodi Amazon RDS).

Tipo: stringa

Campo obbligatorio: sì

### Input dell'operazione API

Uno o più input dell'operazione API. Puoi visualizzare gli input disponibili (definiti anche parametri) scegliendo un servizio nel pannello di navigazione a sinistra nella pagina [Documentazione di riferimento ai servizi](#). Scegliere un metodo nella sezione Client del servizio che si desidera chiamare. Ad esempio, tutti i metodi per Amazon RDS sono elencati nella pagina: [metodi di Amazon RDS](#). Scegliete il metodo [describe\\_db\\_instances](#) e scorrete verso il basso per visualizzare i parametri disponibili, ad esempio Nome e Valori. DBInstanceIdentifier

### YAML

```
inputs:
 Service: The official namespace of the service
 Api: The API operation name
 API input 1: A value
 API Input 2: A value
 API Input 3: A value
```

### JSON

```
"inputs":{
 "Service":"The official namespace of the service",
 "Api":"The API operation name",
 "API input 1":"A value",
 "API Input 2":"A value",
 "API Input 3":"A value"
}
```

Tipo: determinato dall'operazione API selezionata

Obbligatorio: sì

## Output

Gli output sono specificati dall'utente in base alla risposta dell'operazione API scelta.

### Nome

Nome dell'output.

Tipo: stringa

Obbligatorio: sì

### Selector

Elemento JSONPath di un attributo specifico nell'oggetto di risposta. Puoi visualizzare gli oggetti di risposta scegliendo un servizio nel pannello di navigazione a sinistra nella pagina [Documentazione di riferimento ai servizi](#). Scegliere un metodo nella sezione Client del servizio che si desidera chiamare. Ad esempio, tutti i metodi per Amazon RDS sono elencati nella pagina: [metodi di Amazon RDS](#). Scegliere il metodo [describe\\_db\\_instances](#) e scorrere fino alla sezione Struttura risposta. DBInstances è presente nell'elenco come oggetto di risposta.

Digitate: Integer, Boolean, String,, o StringList StringMap MapList

Obbligatorio: sì

### Tipo

Tipo di dati dell'elemento di risposta.

Tipo: vario

Obbligatorio: sì

## **aws:ExecuteScript – Esegue uno script**

Esegue il Python o PowerShell lo script fornito utilizzando il runtime e il gestore specificati. Ogni operazione `aws:executeScript` può durare al massimo 600 secondi (10 minuti). Puoi limitare il timeout specificando il parametro `timeoutSeconds` per una fase `aws:executeScript`.

Usa le istruzioni `return` nella funzione per aggiungere output al payload di output. Per esempi di definizione degli output per l'operazione `aws:executeScript`, consulta [Esempio 2: Runbook con](#)

[script](#). Puoi anche inviare l'output delle `aws:executeScript` azioni nei tuoi runbook al gruppo di CloudWatch log di Amazon Logs specificato. Per ulteriori informazioni, consulta [Uscita dell'azione Logging Automation con Logs CloudWatch](#).

Se desideri inviare l'output `aws:executeScript` delle azioni a CloudWatch Logs o se gli script specificati per `aws:executeScript` le azioni chiamano operazioni AWS API, per eseguire il runbook è sempre necessario un ruolo di servizio AWS Identity and Access Management (IAM) (o assume un ruolo).

#### Note

L'azione `aws:executeScript` non supporta il nuovo tentativo di limitazione (della larghezza di banda della rete) automatico. Se lo script effettua chiamate AWS API che potrebbero essere limitate, devi implementare la tua logica di ripetizione nel codice dello script.

L'`aws:executeScript` azione contiene i seguenti moduli Core PowerShell preinstallati:

- `Microsoft.PowerShell.Host`
- `Microsoft.PowerShell.Management`
- `Microsoft.PowerShell.Security`
- `Microsoft.PowerShell.Utility`
- `PackageManagement`
- `PowerShellGet`

Per utilizzare i moduli PowerShell Core che non sono preinstallati, lo script deve installare il modulo con il `-Force` flag, come mostrato nel comando seguente. Il modulo `AWSPowerShell.NetCore` non è supportato. Sostituiscilo *ModuleName* con il modulo che desideri installare.

```
Install-Module ModuleName -Force
```

Per utilizzare i cmdlet PowerShell Core nello script, si consiglia di utilizzare i `AWS.Tools` moduli, come illustrato nei comandi seguenti. Sostituisci ogni *example resource placeholder* con le tue informazioni.

- Cmdlet Amazon S3

```
Install-Module AWS.Tools.S3 -Force
Get-S3Bucket -BucketName amzn-s3-demo-bucket
```

- Cmdlet Amazon EC2

```
Install-Module AWS.Tools.EC2 -Force
Get-EC2InstanceStatus -InstanceId instance-id
```

- Cmdlet comuni o indipendenti dal AWS Tools for Windows PowerShell servizio.

```
Install-Module AWS.Tools.Common -Force
Get-AWSRegion
```

Se lo script inizializza nuovi oggetti oltre a utilizzare i cmdlet PowerShell Core, è inoltre necessario importare il modulo come illustrato nel comando seguente.

```
Install-Module AWS.Tools.EC2 -Force
Import-Module AWS.Tools.EC2

$tag = New-Object Amazon.EC2.Model.Tag
$tag.Key = "Tag"
$tag.Value = "TagValue"

New-EC2Tag -Resource i-02573cafcfEXAMPLE -Tag $tag
```

Per esempi di installazione e importazione di AWS.Tools moduli e utilizzo dei cmdlet PowerShell Core nei runbook, vedere. [Esperienza di progettazione visiva per i runbook Automation](#)

## Input

Fornisci le informazioni necessarie per eseguire lo script. Sostituisci ogni *example resource placeholder* con le tue informazioni.

### Note

L'allegato per uno script Python può essere un file .py o un file .zip che contiene lo script. PowerShell gli script devono essere archiviati in file .zip.

## YAML

```
action: "aws:executeScript"
inputs:
 Runtime: runtime
 Handler: "functionName"
 InputPayload:
 scriptInput: '{{parameterValue}}'
 Script: |-
 def functionName(events, context):
 ...
 Attachment: "scriptAttachment.zip"
```

## JSON

```
{
 "action": "aws:executeScript",
 "inputs": {
 "Runtime": "runtime",
 "Handler": "functionName",
 "InputPayload": {
 "scriptInput": "{{parameterValue}}"
 },
 "Attachment": "scriptAttachment.zip"
 }
}
```

## Runtime

Il linguaggio di runtime da utilizzare per l'esecuzione dello script fornito.  
aws:executeScript supporta i tempi di esecuzione nella tabella seguente.

| Nome runtime              | Valore di runtime per l'input <i>runtime</i> |
|---------------------------|----------------------------------------------|
| Python 3.12               | <b>python3.12</b>                            |
| Python 3.11               | <b>python3.11</b>                            |
| Python 3.10               | <b>python3.10</b>                            |
| PowerShell 7.4 () dotnet8 | <b>PowerShell 7.4</b>                        |



Tipo: stringa

Obbligatorio: sì

 Note

Per i runtime di Python, l'ambiente fornisce 512 MB di memoria e 512 MB di spazio su disco. Per i PowerShell runtime, l'ambiente fornisce 1024 MB di memoria e 512 MB di spazio su disco.

## Gestore

Il nome della funzione. È necessario assicurarsi che la funzione definita nel gestore abbia due parametri e. events context Il PowerShell runtime non supporta questo parametro.

Tipo: stringa

Obbligatorio: Sì (Python) | Non supportato (PowerShell)

## InputPayload

Un oggetto JSON o YAML che verrà passato al primo parametro del gestore. Questo può essere usato per passare i dati di input allo script.

─Tipo: stringa

Obbligatorio: no

Python

```
description: Tag an instance
schemaVersion: '0.3'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
 AutomationAssumeRole:
 type: String
 description: '(Required) The Amazon Resource Name (ARN) of the IAM role
that allows Automation to perform the actions on your behalf. If no role is
specified, Systems Manager Automation uses your IAM permissions to operate this
runbook.'
 InstanceId:
 type: String
```

```

 description: (Required) The ID of the EC2 instance you want to tag.
mainSteps:
 - name: tagInstance
 action: 'aws:executeScript'
 inputs:
 Runtime: "python3.11"
 Handler: tagInstance
 InputPayload:
 instanceId: '{{InstanceId}}'
 Script: |-
 def tagInstance(events,context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 instanceId = events['instanceId']
 tag = {
 "Key": "Env",
 "Value": "ExamplePython"
 }
 print(f"Adding tag {tag} to instance id {instanceId}")
 ec2.create_tags(
 Resources=[instanceId],
 Tags=[tag]
)
 return tag
 outputs:
 - Type: String
 Name: TagKey
 Selector: $.Payload.Key
outputs:
 - tagInstance.TagKey

```

## PowerShell

```

description: Tag an instance
schemaVersion: '0.3'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
 AutomationAssumeRole:
 type: String
 description: (Required) The Amazon Resource Name (ARN) of the IAM role
 that allows Automation to perform the actions on your behalf. If no role is

```

specified, Systems Manager Automation uses your IAM permissions to operate this runbook.

InstanceId:

type: String

description: (Required) The ID of the EC2 instance you want to tag.

mainSteps:

- name: tagInstance

action: aws:executeScript

isEnd: true

inputs:

Runtime: PowerShell 7.4

InputPayload:

instanceId: '{{InstanceId}}'

Script: |-

Install-Module AWS.Tools.EC2 -Force

Import-Module AWS.Tools.EC2

\$input = \$env:InputPayload | ConvertFrom-Json

\$tag = New-Object Amazon.EC2.Model.Tag

\$tag.Key = "Env"

\$tag.Value = "ExamplePowerShell"

Write-Information "Adding tag key: \$(\$tag.Key) and value: \$(\$tag.Value)  
to instance id \$(\$input.instanceId)"

New-EC2Tag -Resource \$input.instanceId -Tag \$tag

return \$tag

outputs:

- Type: String

Name: TagKey

Selector: \$.Payload.Key

outputs:

- tagInstance.TagKey

## Script

Uno script incorporato che si desidera eseguire durante l'automazione.

Tipo: stringa

Richiesto: No (Python) | Sì ( ) PowerShell

## Allegato

Il nome di un file di script standalone o di un file .zip che può essere richiamato dall'operazione. Specifica lo stesso valore del Name del file allegato del documento che specifichi nel parametro della richiesta `Attachments`. Per ulteriori informazioni, consulta la sezione [Allegati](#) nella Documentazione di riferimento API di AWS Systems Manager . Se stai fornendo uno script utilizzando un allegato, devi anche definire una sezione `files` negli elementi di primo livello del runbook. Per ulteriori informazioni, consulta [Versione dello schema 0.3](#).

Per richiamare un file per python, utilizzare il formato `filename.method_name` in `Handler`.

### Note

L'allegato per uno script Python può essere un file .py o un file .zip che contiene lo script. PowerShell gli script devono essere archiviati in file .zip.

Quando si includono librerie Python nell'allegato, si consiglia di aggiungere un file `__init__.py` vuoto in ogni directory del modulo. Ciò consente di importare i moduli dalla libreria contenuti negli allegati all'interno del contenuto dello script. Ad esempio, `from library import module`

─Tipo: stringa

Obbligatorio: no

## Output

## Payload

Rappresentazione JSON dell'oggetto restituito dalla funzione. Vengono restituiti fino a 100 KB. Se si genera un elenco, viene restituito un massimo di 100 elementi.

## Utilizzo degli allegati con `aws:executeScript`

Gli allegati forniscono un modo efficace per impacchettare e riutilizzare script complessi, moduli multipli e dipendenze esterne nelle tue azioni `aws:executeScript`. Utilizza gli allegati quando devi:

- Confeziona più moduli o PowerShell script Python insieme.
- Riutilizzare la stessa logica di script su più runbook.

- Includi librerie o dipendenze esterne nei tuoi script.
- Mantieni pulita la definizione del runbook separando la logica degli script complessi.
- Condividi pacchetti di script tra team o flussi di lavoro di automazione.

## Struttura degli allegati e creazione del pacchetto

È possibile allegare file singoli o pacchetti zip contenenti più file. La struttura varia a seconda del caso d'uso:

### Singoli file allegati

Per gli script semplici, puoi allegare un singolo .py file (Python) o un .zip file contenente un singolo script. PowerShell

### Multi-module pacchetti

Per un'automazione complessa che richiede numerosi moduli, crea un pacchetto zip con la seguente struttura consigliata:

```
my-automation-package.zip
main.py # Entry point script
utils/
__init__.py # Required for Python module imports
helper_functions.py # Utility functions
aws_operations.py # AWS-specific operations
config/
__init__.py
settings.py # Configuration settings
requirements.txt # Optional: document dependencies
```

### Important

Per i pacchetti Python, è necessario includere un file `__init__.py` vuoto in ogni directory che contiene i moduli Python. Ciò consente di importare moduli utilizzando una sintassi di importazione standard di Python come `from utils import helper_functions`

## PowerShell struttura del pacchetto

PowerShell gli allegati devono essere impacchettati in file zip con la seguente struttura:

```
my-powershell-package.zip
Main.ps1 # Entry point script
Modules/
HelperFunctions.ps1 # Utility functions
AWSOperations.ps1 # AWS-specific operations
Config/
Settings.ps1 # Configuration settings
```

## Creazione di runbook con allegati

Segui questi passaggi per creare runbook che utilizzano allegati:

### 1. Carica il tuo allegato su Amazon S3

Carica il file di script o il pacchetto zip in un bucket S3, a cui può accedere il tuo ruolo di automazione. Annota l'URI S3 per l'utilizzo nel passaggio successivo.

```
aws s3 cp my-automation-package.zip s3://my-automation-bucket/scripts/
```

### 2. Calcola il checksum degli allegati

Calcola il SHA-256 checksum del tuo file allegato per la verifica di sicurezza:

```
Linux/macOS
shasum -a 256 my-automation-package.zip

Windows PowerShell
Get-FileHash -Algorithm SHA256 my-automation-package.zip
```

### 3. Definisci la sezione dei file nel tuo runbook

Aggiungi una sezione `files` al livello superiore del runbook, per fare riferimento all'allegato:

```
files:
 my-automation-package.zip:
 checksums:
 sha256: "your-calculated-checksum-here"
```

### 4. Fai riferimento all'allegato nel passaggio `executeScript`

Utilizza il parametro `Attachment`, per fare riferimento al file caricato:

```
- name: runMyScript
 action: aws:executeScript
 inputs:
 Runtime: python3.11
 Handler: main.process_data
 Attachment: my-automation-package.zip
 InputPayload:
 inputData: "{{InputParameter}}"
```

## aws:executeScript (esempi di allegati)

Gli esempi seguenti mostrano diversi modi di utilizzare gli allegati con l'azione `aws:executeScript`.

### Esempio 1: singolo file allegato

Questo esempio mostra come utilizzare un singolo file Python come allegato, per elaborare i dati delle istanze EC2.

File allegato: `process_instance.py`

Crea un file Python con i seguenti contenuti:

```
import boto3
import json

def process_instance_data(events, context):
 """Process EC2 instance data and return formatted results."""
 try:
 instance_id = events.get('instanceId')
 if not instance_id:
 raise ValueError("instanceId is required")

 ec2 = boto3.client('ec2')

 # Get instance details
 response = ec2.describe_instances(InstanceIds=[instance_id])
 instance = response['Reservations'][0]['Instances'][0]

 # Format the response
 result = {
```

```
 'instanceId': instance_id,
 'instanceType': instance['InstanceType'],
 'state': instance['State']['Name'],
 'availabilityZone': instance['Placement']['AvailabilityZone'],
 'tags': {tag['Key']: tag['Value'] for tag in instance.get('Tags', [])}
 }

 print(f"Successfully processed instance {instance_id}")
 return result

except Exception as e:
 print(f"Error processing instance: {str(e)}")
 raise
```

## Runbook completo

Ecco il runbook completo che utilizza il singolo file allegato:

```
description: Process EC2 instance data using single file attachment
schemaVersion: '0.3'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
 AutomationAssumeRole:
 type: String
 description: (Required) IAM role for automation execution
 InstanceId:
 type: String
 description: (Required) EC2 instance ID to process

files:
 process_instance.py:
 checksums:
 sha256: "abc123def456..."

mainSteps:
 - name: processInstance
 action: aws:executeScript
 inputs:
 Runtime: python3.11
 Handler: process_instance.process_instance_data
 Attachment: process_instance.py
 InputPayload:
 instanceId: '{{InstanceId}}'
 outputs:
```



```
- Type: StringMap
 Name: InstanceData
 Selector: $.Payload
```

outputs:

```
- processInstance.InstanceData
```

## Esempio 2: pacchetto Multi-module

Questo esempio dimostra l'utilizzo di un pacchetto zip contenente numerosi moduli Python per operazioni complesse con bucket S3.

### Struttura del pacchetto

Crea un pacchetto zip con la seguente struttura:

```
s3-operations.zip
main.py
utils/
__init__.py
s3_helper.py
validation.py
config/
__init__.py
settings.py
```

main.py (punto di ingresso)

Lo script principale che orchestra le operazioni:

```
from utils.s3_helper import S3Operations
from utils.validation import validate_bucket_name
from config.settings import get_default_settings

def cleanup_s3_bucket(events, context):
 """Clean up S3 bucket based on specified criteria."""
 try:
 bucket_name = events.get('bucketName')
 max_age_days = events.get('maxAgeDays', 30)

 # Validate inputs
 if not validate_bucket_name(bucket_name):
 raise ValueError(f"Invalid bucket name: {bucket_name}")
```

```
Initialize S3 operations
s3_ops = S3Operations()
settings = get_default_settings()

Perform cleanup
deleted_objects = s3_ops.delete_old_objects(
 bucket_name,
 max_age_days,
 settings['dry_run']
)

result = {
 'bucketName': bucket_name,
 'deletedCount': len(deleted_objects),
 'deletedObjects': deleted_objects[:10], # Return first 10 for brevity
 'dryRun': settings['dry_run']
}

print(f"Cleanup completed for bucket {bucket_name}")
return result

except Exception as e:
 print(f"Error during S3 cleanup: {str(e)}")
 raise
```

## Risoluzione dei problemi relativi agli allegati aws:executeScript

Utilizza le seguenti linee guida per risolvere i problemi più comuni relativi agli allegati aws:executeScript:

### Errori di importazione del modulo

Se ricevi errori di importazione, quando usi pacchetti multimodulo:

- Assicurati di aver incluso un `__init__.py` file vuoto in ogni directory contenente i moduli Python.
- Verifica che le istruzioni di importazione corrispondano all'effettiva struttura di file e directory nel pacchetto zip.
- Utilizza le importazioni relative (ad esempio `from .utils import helper`) o le importazioni assolute (ad esempio `from utils import helper`) in modo coerente.

### Errori per allegati non trovati

Se l'automazione non riesce a trovare l'allegato:

- Verifica che il valore del `Attachment` parametro corrisponda esattamente alla chiave nella tua sezione `files`.
- Controlla che il percorso del bucket S3 e il nome del file siano corretti nella sezione `files`.
- Assicurati che il tuo ruolo di automazione disponga `s3:GetObject` dell'autorizzazione per la posizione S3 dell'allegato.
- Verifica che il checksum nel runbook corrisponda al checksum effettivo del file.

Errori della funzione del gestore

Se ricevi errori relativi al gestore:

- Per Python: utilizza il formato `filename.function_name` nel parametro `Handler` (ad esempio `main.process_data`).
- Assicurati che la tua funzione di gestione accetti esattamente due parametri: `events` e `context`.
- Per PowerShell: non specificate un `Handler` parametro; lo script viene eseguito direttamente.

Errori di esecuzione dello script

Se lo script fallisce durante l'esecuzione:

- Controlla la cronologia di esecuzione dell'automazione per messaggi di errore dettagliati e tracce dello stack.
- Usa `print()` le istruzioni (Python) o `Write-Information` (PowerShell) per aggiungere l'output di debug.
- Verifica che tutte le AWS autorizzazioni richieste siano concesse al tuo ruolo di automazione.
- Testa la logica dello script localmente prima di assemblarlo come allegato.

Codici di uscita e gestione degli errori

Per gestire correttamente gli errori e restituire i codici di uscita:

- In Python: usa `raise Exception("error message")` per indicare l'errore dello script.
- In PowerShell: usa `throw "error message"` o `Write-Error` per indicare un errore.
- Restituisci i dati strutturati dalle tue funzioni per fornire success/failure informazioni dettagliate.

- Usa i blocchi try-catch per gestire le eccezioni agilmente e fornire messaggi di errore significativi.

**aws:executeStateMachine**— Esegui una macchina a AWS Step Functions stati

Esegue una macchina a AWS Step Functions stati.

 Note

L'azione `aws:executeStateMachine` supporta un nuovo tentativo di limitazione (della larghezza di banda della rete) automatico. Per ulteriori informazioni, consulta [Configurazione della ripetizione dei tentativi automatica per le operazioni di limitazione \(della larghezza di banda della rete\)](#).

## Input

Questa azione supporta la maggior parte dei parametri per il funzionamento dell'[StartExecution](#) API Step Functions.

Autorizzazioni richieste AWS Identity and Access Management (IAM)

- `states:DescribeExecution`
- `states:StartExecution`
- `states:StopExecution`

## YAML

```
name: executeTheStateMachine
action: aws:executeStateMachine
inputs:
 stateMachineArn: StateMachine_ARN
 input: '{"parameters":"values"}'
 name: name
```

## JSON

```
{
 "name": "executeTheStateMachine",
 "action": "aws:executeStateMachine",
```

```
"inputs": {
 "stateMachineArn": "StateMachine_Arn",
 "input": "{\\"parameters\\":\\"values\\"}",
 "name": "name"
}
}
```

## state MachineArn

Il nome della risorsa Amazon (ARN) della macchina dello stato Step Functions.

Tipo: stringa

Obbligatorio: sì

## nome

Nome dell'esecuzione.

─Tipo: stringa

Obbligatorio: no

## input

Stringa contenente i dati di input JSON per l'esecuzione.

─Tipo: stringa

Obbligatorio: no

## Output

I seguenti output sono predefiniti per questa operazione.

## executionArn

L'ARN dell'esecuzione.

Tipo: String

## input

Stringa contenente i dati di input JSON dell'esecuzione. I vincoli di lunghezza si applicano alla dimensione del payload e sono espressi in byte nella codifica.. UTF-8

Tipo: String

nome

Nome dell'esecuzione.

Tipo: String

output

Dati di output JSON dell'esecuzione. I vincoli di lunghezza si applicano alla dimensione del payload e sono espressi in byte nella codifica. UTF-8

Tipo: String

startDate

Data di inizio dell'esecuzione.

Tipo: String

stato MachineArn

L'ARN della macchina a stati in esecuzione.

Tipo: String

status

Stato attuale dell'esecuzione.

Tipo: String

stopDate

Se l'esecuzione è già terminata, la data in cui l'esecuzione è stata interrotta.

Tipo: String

**aws:invokeWebhook:** richiamo dell'integrazione di un webhook di Automation

Questa azione richiama l'integrazione del webhook di Automation specificato. Per informazioni sulla creazione di integrazioni di automazione, consulta [Creazione di integrazioni webhook per Automazione](#).

**Note**

L'azione `aws:invokeWebhook` supporta un nuovo tentativo di limitazione (della larghezza di banda della rete) automatico. Per ulteriori informazioni, consulta [Configurazione della ripetizione dei tentativi automatica per le operazioni di limitazione \(della larghezza di banda della rete\)](#).

**Note**

Per utilizzare l'operazione `aws:invokeWebhook`, l'utente o il ruolo di servizio deve consentire le seguenti operazioni:

- `sms:GetParameter`
- `kms:Decrypt`

L'autorizzazione per l'Decryptoperazione AWS Key Management Service (AWS KMS) è richiesta solo se si utilizza una chiave gestita dal cliente per crittografare il parametro per l'integrazione.

**Input**

Fornisci le informazioni per l'integrazione di Automation che desideri richiamare.

**YAML**

```
action: "aws:invokeWebhook"
inputs:
 IntegrationName: "exampleIntegration"
 Body: "Request body"
```

**JSON**

```
{
 "action": "aws:invokeWebhook",
 "inputs": {
 "IntegrationName": "exampleIntegration",
 "Body": "Request body"
 }
}
```

```
}
}
```

## IntegrationName

Il nome dell'integrazione di Automazione. Ad esempio, `exampleIntegration`. L'integrazione specificata deve esistere già.

Tipo: stringa

Obbligatorio: sì

## Body

Il payload che desideri inviare quando viene richiamata l'integrazione del webhook.

─Tipo: stringa

Obbligatorio: no

## Output

### Risposta

Il testo ricevuto dalla risposta del provider di webhook.

### ResponseCode

Il codice di stato HTTP ricevuto dalla risposta del provider di webhook.

**aws:invokeLambdaFunction**— Invoca una funzione AWS Lambda

Richiama la funzione specificata. AWS Lambda

### Note

Ogni operazione `aws:invokeLambdaFunction` può durare al massimo 300 secondi (5 minuti). Puoi limitare il timeout specificando il parametro `timeoutSeconds` per una fase `aws:invokeLambdaFunction`.



 Note

L'azione `aws:invokeLambdaFunction` supporta un nuovo tentativo di limitazione (della larghezza di banda della rete) automatico. Per ulteriori informazioni, consulta [Configurazione della ripetizione dei tentativi automatica per le operazioni di limitazione \(della larghezza di banda della rete\)](#).

## Input

Questa operazione supporta la maggior parte dei parametri richiamati per il servizio Lambda. Per ulteriori informazioni, consulta [Invoke \(Chiamata\)](#).

## YAML

```
name: invokeMyLambdaFunction
action: aws:invokeLambdaFunction
maxAttempts: 3
timeoutSeconds: 120
onFailure: Abort
inputs:
 FunctionName: MyLambdaFunction
```

## JSON

```
{
 "name": "invokeMyLambdaFunction",
 "action": "aws:invokeLambdaFunction",
 "maxAttempts": 3,
 "timeoutSeconds": 120,
 "onFailure": "Abort",
 "inputs": {
 "FunctionName": "MyLambdaFunction"
 }
}
```

## FunctionName

Il nome della funzione Lambda. Questa funzione deve esistere.

Tipo: stringa

Obbligatorio: sì

## Qualificatore

Versione o nome alias della funzione.

■Tipo: stringa

Obbligatorio: no

## InvocationType

Tipi di chiamata. Il valore predefinito è `RequestResponse`.

Tipo: String

Valori validi: `Event` | `RequestResponse` | `DryRun`

Obbligatorio: no

## LogType

Se il valore predefinito è `Tail`, il tipo di chiamata deve essere `RequestResponse`. Lambda restituisce gli ultimi 4 KB di dati di log prodotti dalla funzione Lambda, con codifica base64

Tipo: String

Valori validi: `None` | `Tail`

Obbligatorio: no

## ClientContext

Informazioni specifiche del client.

Obbligatorio: no

## InputPayload

Un oggetto YAML o JSON che viene passato al primo parametro del gestore. Questo input può essere utilizzato per passare i dati alla funzione. Questo input offre maggiore flessibilità e supporto rispetto all'input `Payload legacy`. Se vengono definiti sia `InputPayload` che `Payload` per l'operazione, `InputPayload` ha la precedenza e il valore `Payload` non viene utilizzato.

Tipo: StringMap

Obbligatorio: no

## Carico utile

Una stringa JSON che viene passata al primo parametro del gestore. Questo può essere utilizzato per passare i dati di input alla funzione. Consigliamo di utilizzare l'input `InputPayload` per funzionalità aggiuntive.

─Tipo: stringa

Obbligatorio: no

## Output

### StatusCode

Codice di stato HTTP .

### FunctionError

Se presente, indica che si è verificato un errore durante l'esecuzione della funzione. I dettagli sull'errore sono inclusi nel payload di risposta.

### LogResult

I log di codifica base64 per la chiamata della funzione Lambda. I log sono presenti solo se il tipo di chiamata è `RequestResponse` e sono stati richiesti i log.

## Carico utile

Rappresentazione JSON dell'oggetto restituito dalla funzione Lambda. Il payload è presente solo se il tipo di chiamata è `RequestResponse`.

Di seguito è riportata una parte del runbook `AWS-PatchInstanceWithRollback` che dimostra come fare riferimento agli output dall'operazione `aws:invokeLambdaFunction`.

## YAML

```
- name: IdentifyRootVolume
 action: aws:invokeLambdaFunction
 inputs:
 FunctionName: "IdentifyRootVolumeLambda-{{automation:EXECUTION_ID}}"
 Payload: '{"InstanceId": "{{InstanceId}}"}'
- name: PrePatchSnapshot
```

```

action: aws:executeAutomation
inputs:
 DocumentName: "AWS-CreateSnapshot"
 RuntimeParameters:
 VolumeId: "{{IdentifyRootVolume.Payload}}"
 Description: "ApplyPatchBaseline restoration case contingency"

```

## JSON

```

{
 "name": "IdentifyRootVolume",
 "action": "aws:invokeLambdaFunction",
 "inputs": {
 "FunctionName": "IdentifyRootVolumeLambda-{{automation:EXECUTION_ID}}",
 "Payload": "{\"InstanceId\": \"{{InstanceId}}\"}"
 }
},
{
 "name": "PrePatchSnapshot",
 "action": "aws:executeAutomation",
 "inputs": {
 "DocumentName": "AWS-CreateSnapshot",
 "RuntimeParameters": {
 "VolumeId": "{{IdentifyRootVolume.Payload}}",
 "Description": "ApplyPatchBaseline restoration case contingency"
 }
 }
}

```

**aws:loop:** intera sui passaggi di un'automazione

Questa operazione esegue un'iterazione su un sottoinsieme di passaggi in un runbook Automation. È possibile scegliere un ciclo di stile `do while` o `for each`. Per costruire un ciclo `do while`, utilizza il parametro di input `LoopCondition`. Per costruire un ciclo `for each`, utilizza i parametri di input `Iterators` e `IteratorDataType`. Quando utilizzi un'azione `aws:loop`, specifica solo il parametro di input `Iterators` o `LoopCondition`. Il numero massimo di iterazioni è 100.

La proprietà `onCancel` può essere utilizzata solo per i passaggi definiti all'interno di un ciclo. La proprietà `onCancel` non è supportata per l'azione `aws:loop`. La proprietà `onFailure` può essere utilizzata per un'operazione `aws:loop`, ma solo se si verifica un errore imprevisto che impedisce la corretta esecuzione del passaggio. Se si definiscono le proprietà `onFailure` per i passaggi

all'interno di un ciclo, l'operazione `aws:loop` eredita tali proprietà e reagisce di conseguenza quando si verifica un errore.

## Esempi

Di seguito sono riportati alcuni esempi di come costruire i diversi tipi di operazioni di un ciclo.

### do while

```
name: RepeatMyLambdaFunctionUntilOutputIsReturned
action: aws:loop
inputs:
 Steps:
 - name: invokeMyLambda
 action: aws:invokeLambdaFunction
 inputs:
 FunctionName: LambdaFunctionName
 outputs:
 - Name: ShouldRetry
 Selector: $.Retry
 Type: Boolean
 LoopCondition:
 Variable: "{{ invokeMyLambda.ShouldRetry }}"
 BooleanEquals: true
 MaxIterations: 3
```

### for each

```
name: stopAllInstancesWithWaitTime
action: aws:loop
inputs:
 Iterators: "{{ DescribeInstancesStep.InstanceIds }}"
 IteratorDataType: "String"
 Steps:
 - name: stopOneInstance
 action: aws:changeInstanceState
 inputs:
 InstanceIds:
 - "{{stopAllInstancesWithWaitTime.CurrentIteratorValue}}"
 CheckStateOnly: false
 DesiredState: stopped
 - name: wait10Seconds
 action: aws:sleep
```

```
inputs:
Duration: PT10S
```

## Input

Di seguito è riportato l'input.

## Iterators

L'elenco degli elementi per i passaggi su cui eseguire l'iterazione. Il numero massimo di iteratori è 100.

Tipo: `StringList`

Obbligatorio: no

## IteratorDataType

Un parametro facoltativo per specificare il tipo di dati di `Iterators`. Un valore per questo parametro può essere fornito insieme al parametro di input `Iterators`. Se non si specifica un valore per questo parametro e `Iterators`, sarà necessario specificare un valore per il parametro `LoopCondition`.

Tipo: `String`

Valori validi: `Boolean` | `Integer` | `String` | `StringMap`

Predefinito: `String`

Obbligatorio: no

## LoopCondition

Costituito da una `Variable` e una condizione dell'operatore da valutare. Se non si specifica un valore per questo parametro, allora sarà necessario specificare i valori per i parametri `Iterators` e `IteratorDataType`. È possibile utilizzare valutazioni complesse degli operatori utilizzando una combinazione degli operatori `And`, `Not` e `Or`. La condizione viene valutata dopo il completamento dei passaggi del ciclo. Se la condizione è `true` e il valore `MaxIterations` non è stato raggiunto, i passaggi del ciclo saranno eseguiti nuovamente. Le condizioni dell'operatore sono le seguenti:

Operazioni di stringa

- `StringEquals`

- EqualsIgnoreCase
- StartsWith
- EndsWith
- Contiene

#### Operazioni numeriche

- NumericEquals
- NumericGreater
- NumericLesser
- NumericGreaterOrEquals
- NumericLesser
- NumericLesserOrEquals

#### Operazioni booleane

- BooleanEquals

Tipo: StringMap

Obbligatorio: no

#### MaxIterations

Il numero massimo di volte che vengono eseguiti i passaggi del ciclo. Una volta raggiunto il valore specificato per questo input, il ciclo smette di funzionare anche se `LoopCondition` è ancora `true` o se ci sono oggetti rimanenti nel parametro `Iterators`.

Tipo: numero intero

Valori validi: 1-100

Obbligatorio: no

#### Fasi

L'elenco di passaggi da eseguire nel ciclo. Funzionano come un runbook nidificato. In questi passaggi è possibile accedere al valore corrente dell'iteratore per un ciclo `for each` utilizzando la sintassi `{{loopStepName.CurrentIteratorValue}}`. È inoltre possibile accedere a un valore intero dell'iterazione corrente per entrambi i tipi di ciclo utilizzando la sintassi `{{loopStepName.CurrentIteration}}`.

Tipo: elenco di passaggi

Obbligatorio: sì

## Output

### CurrentIteration

L'iterazione del ciclo corrente come numero intero. I valori di iterazione iniziano da 1.

Tipo: numero intero

### CurrentIteratorValue

Il valore dell'iteratore corrente come stringa. Questo output è presente solo nei cicli `for each`.

Tipo: String

**aws:pause:** sospensione di un'automazione

Questa operazione sospende l'esecuzione dell'automazione. Una volta sospesa, lo stato dell'automazione è `Waiting` (In attesa). Per continuare l'automazione, utilizza l'operazione [SendAutomationSignal](#) API con il tipo di `Resume` segnale. Ti consigliamo di usare l'operazione `aws:sleep` o `aws:approve` per un controllo più granulare dei flussi di lavoro.

#### Note

Il timeout predefinito per questa azione è di 7 giorni (60.4800 secondi) e il valore massimo è di 30 giorni (259.2000 secondi). Puoi limitare o estendere il timeout specificando il parametro `timeoutSeconds` per una fase `aws:pause`.

## Input

Di seguito è riportato l'input.

## YAML

```
name: pauseThis
action: aws:pause
```



```
timeoutSeconds: 1209600
inputs: {}
```

## JSON

```
{
 "name": "pauseThis",
 "action": "aws:pause",
 "timeoutSeconds": "1209600",
 "inputs": {}
}
```

## Output

Nessuno

**aws:runCommand:** esecuzione di un comando su un'istanza gestita

Esegue i comandi specificati.

### Note

L'automazione supporta solo l'output di un'operazione AWS Systems Manager Run Command. Un runbook può includere più operazioni Run Command, ma l'output è supportato solo per un'operazione alla volta.

## Input

Questa operazione supporta la maggior parte dei parametri dell'operazione SendCommand. Per ulteriori informazioni, consulta [SendCommand](#).

## YAML

```
- name: checkMembership
 action: 'aws:runCommand'
 inputs:
 DocumentName: AWS-RunPowerShellScript
 InstanceIds:
```

```
- '{{InstanceIds}}'
Parameters:
 commands:
 - (Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain
```

## JSON

```
{
 "name": "checkMembership",
 "action": "aws:runCommand",
 "inputs": {
 "DocumentName": "AWS-RunPowerShellScript",
 "InstanceIds": [
 "{{InstanceIds}}"
],
 "Parameters": {
 "commands": [
 "(Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain"
]
 }
 }
}
```

### DocumentName

Se il documento di tipo Comando è di tua proprietà o AWS, specifica il nome del documento. Se stai usando un documento condiviso con te da un Account AWS differente, specifica il nome della risorsa Amazon (ARN) del documento. Per ulteriori informazioni sull'utilizzo di documenti condivisi, consulta [Utilizzo di documenti SSM condivisi](#).

Tipo: stringa

Obbligatorio: sì

### InstanceIds

ID delle istanze in cui eseguire il comando. Puoi specificare un massimo di 50 ID.

È inoltre possibile utilizzare lo pseudo parametro `{{RESOURCE_ID}}` al posto degli ID di istanza per eseguire il comando su tutte le istanze del gruppo di destinazione. Per ulteriori informazioni sugli pseudoparametri, consulta [Utilizzo degli pseudo parametri durante la registrazione delle attività della finestra di manutenzione](#).

Un'altra alternativa consiste nell'inviare comandi a un parco istanze utilizzando il parametro `Targets`. Il parametro `Targets` accetta i tag di Amazon Elastic Compute Cloud (Amazon EC2). Per ulteriori informazioni su come utilizzare il parametro `Targets`, consulta [Esecuzione di comandi su vasta scala](#).

Tipo: `StringList`

Obbligatorio: No (se non si specifica `InstanceIds` o non si utilizza lo `{{RESOURCE_ID}}` pseudo parametro, è necessario specificare il `Targets` parametro).

## Targets

Una matrice di criteri di ricerca che definisce le istanze come destinazioni utilizzando una combinazione di chiave-valore specificata dall'utente. `Targets` è obbligatorio se non vengono forniti uno o più ID di istanza nella chiamata. Per ulteriori informazioni su come utilizzare il parametro `Targets`, consulta [Esecuzione di comandi su vasta scala](#).

Tipo: `MapList` (Lo schema della mappa nell'elenco deve corrispondere all'oggetto.) Per ulteriori informazioni, consulta [Target](#) (Destinazione) nella Documentazione di riferimento dell'API di AWS Systems Manager .

Obbligatorio: No (se non si specifica `Targets`, è necessario specificare `InstanceIds` o utilizzare lo `{{RESOURCE_ID}}` pseudo parametro.)

Di seguito è riportato un esempio.

## YAML

```
- name: checkMembership
 action: aws:runCommand
 inputs:
 DocumentName: AWS-RunPowerShellScript
 Targets:
 - Key: tag:Stage
 Values:
 - Gamma
 - Beta
 - Key: tag-key
 Values:
 - Suite
 Parameters:
 commands:
```

```
- (Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain
```

## JSON

```
{
 "name": "checkMembership",
 "action": "aws:runCommand",
 "inputs": {
 "DocumentName": "AWS-RunPowerShellScript",
 "Targets": [
 {
 "Key": "tag:Stage",
 "Values": [
 "Gamma", "Beta"
]
 },
 {
 "Key": "tag:Application",
 "Values": [
 "Suite"
]
 }
],
 "Parameters": {
 "commands": [
 "(Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain"
]
 }
 }
}
```

## Parameters

Parametri obbligatori e facoltativi specificati nel documento.

Tipo: Map

Obbligatorio: no

## CloudWatchOutputConfig

Opzioni di configurazione per l'invio dell'output dei comandi ad Amazon CloudWatch Logs. Per ulteriori informazioni sull'invio dell'output del comando a CloudWatch Logs, consulta.

[Configurazione di Amazon CloudWatch Logs per Run Command](#)

Tipo: StringMap (Lo schema della mappa deve corrispondere all'oggetto. Per ulteriori informazioni, [CloudWatchOutputConfig](#) consulta l'AWS Systems Manager API Reference).

Obbligatorio: no

Di seguito è riportato un esempio.

YAML

```
- name: checkMembership
 action: aws:runCommand
 inputs:
 DocumentName: AWS-RunPowerShellScript
 InstanceIds:
 - "{{InstanceIds}}"
 Parameters:
 commands:
 - "(Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain"
 CloudWatchOutputConfig:
 CloudWatchLogGroupName: CloudWatchGroupForSSMAutomationService
 CloudWatchOutputEnabled: true
```

JSON

```
{
 "name": "checkMembership",
 "action": "aws:runCommand",
 "inputs": {
 "DocumentName": "AWS-RunPowerShellScript",
 "InstanceIds": [
 "{{InstanceIds}}"
],
 "Parameters": {
 "commands": [
 "(Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain"
]
 }
 },
 "CloudWatchOutputConfig" : {
 "CloudWatchLogGroupName":
"CloudWatchGroupForSSMAutomationService",
 "CloudWatchOutputEnabled": true
 }
}
```

```
}
```

## Comment

User-defined informazioni sul comando.

─Tipo: stringa

Obbligatorio: no

## DocumentHash

Hash del documento.

─Tipo: stringa

Obbligatorio: no

## DocumentHashType

Tipo di hash.

Tipo: String

Valori validi: Sha256 | Sha1

Obbligatorio: no

## NotificationConfig

Configurazioni per l'invio delle notifiche.

Obbligatorio: no

## OutputS3BucketName

Nome del bucket S3 per le risposte dell'output del comando. Il nodo gestito deve disporre delle autorizzazioni, affinché il bucket S3 registri correttamente l'output.

─Tipo: stringa

Obbligatorio: no

## OutputS3KeyPrefix

Prefisso.

■Tipo: stringa

Obbligatorio: no

#### ServiceRoleArn

L'ARN del ruolo AWS Identity and Access Management (IAM).

■Tipo: stringa

Obbligatorio: no

#### TimeoutSeconds

La quantità di tempo, in secondi, di attesa per l'invio di un comando AWS Systems Manager SSM Agent su un'istanza. Se il comando non viene ricevuto da SSM Agent sull'istanza prima che venga raggiunto il valore specificato, lo stato del comando cambia in `Delivery Timed Out`.

Tipo: Integer

Obbligatorio: no

Valori validi: 30-2592000

#### Output

##### CommandId

ID del comando.

##### Status

Stato del comando.

##### ResponseCode

Codice di risposta del comando. Se il documento eseguito presenta più di un passaggio, non viene restituito un valore per questo output.

#### Output

Output del comando. Se il comando è rivolto a un tag o a più istanze, non viene restituito alcun valore di output. È possibile utilizzare le operazioni API `GetCommandInvocation` e `ListCommandInvocations` per recuperare l'output di singole istanze.

**aws:runInstances:** avvio di un'istanza di Amazon EC2

Avvia una nuova istanza di Amazon Elastic Compute Cloud (Amazon EC2).

 **Note**

L'azione `aws:runInstances` supporta un nuovo tentativo di limitazione (della larghezza di banda della rete) automatico. Per ulteriori informazioni, consulta [Configurazione della ripetizione dei tentativi automatica per le operazioni di limitazione \(della larghezza di banda della rete\)](#).

**Input**

L'operazione supporta la maggior parte dei parametri API. Per ulteriori informazioni, consulta la documentazione dell'[RunInstances](#) API.

**YAML**

```
name: launchInstance
action: aws:runInstances
maxAttempts: 3
timeoutSeconds: 1200
onFailure: Abort
inputs:
 ImageId: ami-12345678
 InstanceType: t2.micro
 MinInstanceCount: 1
 MaxInstanceCount: 1
 IamInstanceProfileName: myRunCmdRole
 TagSpecifications:
 - ResourceType: instance
 Tags:
 - Key: LaunchedBy
 Value: SSMAutomation
 - Key: Category
 Value: HighAvailabilityFleetHost
```

**JSON**

```
{
```



```
"name": "launchInstance",
"action": "aws:runInstances",
"maxAttempts": 3,
"timeoutSeconds": 1200,
"onFailure": "Abort",
"inputs": {
 "ImageId": "ami-12345678",
 "InstanceType": "t2.micro",
 "MinInstanceCount": 1,
 "MaxInstanceCount": 1,
 "IamInstanceProfileName": "myRunCmdRole",
 "TagSpecifications": [
 {
 "ResourceType": "instance",
 "Tags": [
 {
 "Key": "LaunchedBy",
 "Value": "SSMAutomation"
 },
 {
 "Key": "Category",
 "Value": "HighAvailabilityFleetHost"
 }
]
 }
]
}
```

## AdditionalInfo

Riservata.

─Tipo: stringa

Obbligatorio: no

## BlockDeviceMappings

Dispositivi a blocchi per l'istanza.

Tipo: MapList

Obbligatorio: no

## ClientToken

Identificatore univoco per assicurare l'idempotenza della richiesta.

─Tipo: stringa

Obbligatorio: no

## DisableApiTermination

Attiva o disattiva la terminazione dell'API dell'istanza.

Tipo: Booleano

Obbligatorio: no

## EbsOptimized

Attiva o disattiva l'ottimizzazione di Amazon Elastic Block Store (Amazon EBS).

Tipo: Booleano

Obbligatorio: no

## IamInstanceProfileArn

L'Amazon Resource Name (ARN) del profilo dell'istanza AWS Identity and Access Management (IAM) per l'istanza.

─Tipo: stringa

Obbligatorio: no

## IamInstanceProfileName

Nome del profilo dell'istanza IAM per l'istanza.

─Tipo: stringa

Obbligatorio: no

## ImageId

L'ID del Amazon Machine Image (AMI).

Tipo: stringa

Obbligatorio: sì

## InstanceInitiatedShutdownBehavior

Indica se l'istanza viene arrestata o terminata in caso di arresto del sistema.

─Tipo: stringa

Obbligatorio: no

## InstanceType

Il tipo di istanza.

### Note

Se non viene fornito un valore di un tipo di istanza, viene utilizzato il tipo di istanza m1.small.

─Tipo: stringa

Obbligatorio: no

## KernelId

ID del kernel.

─Tipo: stringa

Obbligatorio: no

## KeyName

Nome della coppia di chiavi.

─Tipo: stringa

Obbligatorio: no

## MaxInstanceCount

Numero massimo di istanze da avviare.

─Tipo: stringa

Obbligatorio: no

## MetadataOptions

Le opzioni dei metadati per l'istanza. Per ulteriori informazioni, consulta [InstanceMetadataOptionsRequest](#).

Tipo: StringMap

Obbligatorio: no

## MinInstanceCount

Numero minimo di istanze da avviare.

─Tipo: stringa

Obbligatorio: no

## Monitoraggio

Attiva o disattiva il monitoraggio dettagliato.

Tipo: Booleano

Obbligatorio: no

## NetworkInterfaces

Interfacce di rete.

Tipo: MapList

Obbligatorio: no

## Placement

Posizionamento dell'istanza.

Tipo: StringMap

Obbligatorio: no

## PrivateIpAddress

Indirizzo IPv4 primario.

─Tipo: stringa

Obbligatorio: no

## RamdiskId

L'ID del disco RAM.

▪Tipo: stringa

Obbligatorio: no

## SecurityGroupIds

ID dei gruppi di sicurezza per l'istanza.

Tipo: StringList

Obbligatorio: no

## SecurityGroups

Nomi dei gruppi di sicurezza per l'istanza.

Tipo: StringList

Obbligatorio: no

## SubnetId

L'ID sottorete.

▪Tipo: stringa

Obbligatorio: no

## TagSpecifications

I tag da applicare alle risorse durante il lancio. È possibile contrassegnare mediante tag solo le istanze e i volumi all'avvio. I tag specificati vengono applicati a tutti i volumi o le istanze che vengono creati durante il lancio. Per contrassegnare mediante tag un'istanza dopo che è stata avviata, utilizza l'operazione [AWS:createTags — Crea tag per AWS risorse](#).

Tipo: MapList (per ulteriori informazioni, consulta [TagSpecification](#).)

Obbligatorio: no

## UserData

Script fornito sotto forma di valore letterale di stringa. Se viene immesso un valore letterale, deve Base64-encoded esserlo.

■Tipo: stringa

Obbligatorio: no

## Output

### InstanceIds

ID delle istanze.

### InstanceStates

Lo stato attuale dell'istanza.

## **aws:sleep**: ritardo di un'automazione

Ritarda l'automazione per un periodo di tempo specificato. Questa operazione usa valori di data/ora in formato ISO (International Organization for Standardization) 8601. Per ulteriori informazioni su questo formato di data e ora, consulta [ISO 8601](#).

## Input

È possibile ritardare un'automazione per una durata specificata.

## YAML

```
name: sleep
action: aws:sleep
inputs:
 Duration: PT10M
```

## JSON

```
{
 "name": "sleep",
 "action": "aws:sleep",
 "inputs": {
 "Duration": "PT10M"
 }
}
```

È anche possibile ritardare un'automazione fino alla data e all'ora specificate. Se la data e l'ora specificate sono trascorse, l'operazione viene eseguita immediatamente.

## YAML

```
name: sleep
action: aws:sleep
inputs:
 Timestamp: '2020-01-01T01:00:00Z'
```

## JSON

```
{
 "name": "sleep",
 "action": "aws:sleep",
 "inputs": {
 "Timestamp": "2020-01-01T01:00:00Z"
 }
}
```

### Note

L'automazione supporta un ritardo massimo di 604.799 secondi (7 giorni).

## Durata

Durata in formato ISO 8601. Non è possibile specificare una durata negativa.

─Tipo: stringa

Obbligatorio: no

## Time stamp

Timestamp in formato ISO 8601. Se non si specifica un valore per questo parametro, è necessario specificare un valore per il parametro `Duration`.

─Tipo: stringa

Obbligatorio: no

## Output

Nessuno

**aws:updateVariable:** aggiorna un valore per una variabile di runbook

Questa azione aggiorna un valore per una variabile di runbook. Il tipo di dati per il valore deve corrispondere al tipo di dati della variabile da aggiornare. Le conversioni dei tipi di dati non sono supportate. La proprietà `onCancel` non è supportata per l'azione `aws:updateVariable`.

## Input

Di seguito è riportato l'input.

## YAML

```
name: updateStringList
action: aws:updateVariable
inputs:
 Name: variable:variable name
 Value:
 - "1"
 - "2"
```

## JSON

```
{
 "name": "updateStringList",
 "action": "aws:updateVariable",
 "inputs": {
 "Name": "variable:variable name",
 "Value": ["1","2"]
 }
}
```

## Nome

Il nome della variabile di cui vuoi aggiornare il valore. È necessario utilizzare il formato `variable:variable name`

Tipo: stringa



Obbligatorio: sì

Valore

Il nuovo valore da assegnare alla variabile. Il valore deve corrispondere al tipo di dati della variabile. Le conversioni dei tipi di dati non sono supportate.

Tipo: Boolean | Intero | | Stringa | MapList | StringList StringMap

Obbligatorio: sì

Vincoli:

- MapList può contenere un numero massimo di 200 articoli.
- La lunghezza delle chiavi può essere minimo 1 e massimo 50.
- StringList può essere un numero minimo di 0 elementi e un numero massimo di 50 elementi.
- La lunghezza delle stringhe può essere minimo 1 e massimo 512.

Output

Nessuno

### **aws:wait ForAwsResourceProperty – Attendi** un AWS proprietà della risorsa

L'operazione `aws:waitForAwsResourceProperty` consente all'automazione di attendere lo stato di una risorsa specifica o lo stato di un evento prima di continuare l'automazione. Per ulteriori esempi di utilizzo di questa operazione, consulta [Ulteriori esempi di runbook](#).

#### Note

Il valore di timeout predefinito per questa operazione è 3600 secondi (un'ora). Puoi limitare o estendere il timeout specificando il parametro `timeoutSeconds` per una fase `aws:waitForAwsResourceProperty`. Per ulteriori informazioni ed esempi su come utilizzare questa operazione, consulta [Gestione dei timeout nei runbook](#).

#### Note

L'azione `aws:waitForAwsResourceProperty` supporta un nuovo tentativo di limitazione (della larghezza di banda della rete) automatico. Per ulteriori informazioni, consulta

Configurazione della ripetizione dei tentativi automatica per le operazioni di limitazione (della larghezza di banda della rete).

## Input

Gli input vengono definiti dall'operazione API selezionata.

## YAML

```
action: aws:waitForAwsResourceProperty
inputs:
 Service: The official namespace of the service
 Api: The API operation or method name
 API operation inputs or parameters: A value
 PropertySelector: Response object
 DesiredValues:
 - Desired property value
```

## JSON

```
{
 "action": "aws:waitForAwsResourceProperty",
 "inputs": {
 "Service": "The official namespace of the service",
 "Api": "The API operation or method name",
 "API operation inputs or parameters": "A value",
 "PropertySelector": "Response object",
 "DesiredValues": [
 "Desired property value"
]
 }
}
```

## Servizio

Lo spazio dei Servizio AWS nomi che contiene l'operazione API che desideri eseguire. Ad esempio, lo spazio dei nomi per è. AWS Systems Manager ssm Il namespace per Amazon Elastic Compute Cloud (Amazon EC2) è ec2. È possibile visualizzare un elenco dei Servizio AWS namespace supportati nella sezione [Servizi disponibili del Command Reference](#).AWS CLI

Tipo: stringa

Obbligatorio: sì

## Api

Nome dell'operazione API da eseguire. Puoi visualizzare le operazioni API (definite anche metodi) scegliendo un servizio nel pannello di navigazione a sinistra nella pagina [Documentazione di riferimento ai servizi](#). Scegliere un metodo nella sezione Client del servizio che si desidera chiamare. Ad esempio, tutte le operazioni API (metodi) per Amazon Relational Database Service (Amazon RDS) sono elencate nella seguente pagina: [Amazon RDS methods](#) (Metodi Amazon RDS).

Tipo: stringa

Campo obbligatorio: sì

## Input dell'operazione API

Uno o più input dell'operazione API. Puoi visualizzare gli input disponibili (definiti anche parametri) scegliendo un servizio nel pannello di navigazione a sinistra nella pagina [Documentazione di riferimento ai servizi](#). Scegliere un metodo nella sezione Client del servizio che si desidera chiamare. Ad esempio, tutti i metodi per Amazon RDS sono elencati nella pagina: [metodi di Amazon RDS](#). Scegliete il metodo [describe\\_db\\_instances](#) e scorrete verso il basso per visualizzare i parametri disponibili, ad esempio Nome e Valori. DBInstanceIdentifier

## YAML

```
inputs:
 Service: The official namespace of the service
 Api: The API operation name
 API input 1: A value
 API Input 2: A value
 API Input 3: A value
```

## JSON

```
"inputs":{
 "Service":"The official namespace of the service",
 "Api":"The API operation name",
 "API input 1":"A value",
 "API Input 2":"A value",
 "API Input 3":"A value"
}
```

```
}
```

Tipo: determinato dall'operazione API selezionata

Obbligatorio: sì

PropertySelector

Elemento JSONPath di un attributo specifico nell'oggetto di risposta. Puoi visualizzare gli oggetti di risposta scegliendo un servizio nel pannello di navigazione a sinistra nella pagina [Documentazione di riferimento ai servizi](#). Scegliere un metodo nella sezione Client del servizio che si desidera chiamare. Ad esempio, tutti i metodi per Amazon RDS sono elencati nella pagina: [metodi di Amazon RDS](#). Scegliere il metodo [describe\\_db\\_instances](#) e scorrere fino alla sezione Struttura risposta. DBInstances è presente nell'elenco come oggetto di risposta.

Tipo: String

Obbligatorio: sì

DesiredValues

Stato previsto o stato con il quale continuare l'automazione.

MapListDigita:, StringList

Obbligatorio: sì

Variabili di sistema del servizio di automazione

AWS Systems Manager I runbook di automazione utilizzano le seguenti variabili. Per un esempio di come vengono utilizzate queste variabili, visualizza il testo JSON di origine del runbook AWS-UpdateWindowsAmi.

Per visualizzare l'origine JSON del runbook di **AWS-UpdateWindowsAmi**

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Documenti.
3. Nell'elenco di documenti utilizzare la barra di ricerca o i numeri alla sua destra per scegliere il runbook **AWS-UpdateWindowsAmi**.
4. Scegli la scheda Contenuti.

## Variabili di sistema

I runbook del servizio di automazione supportano le seguenti variabili di sistema.

| Variabile                         | Informazioni                                                                                                                                                                                                                                                                |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>global:ACCOUNT_ID</code>    | L' Account AWS ID dell'utente o del ruolo in cui viene eseguita Automation.                                                                                                                                                                                                 |
| <code>global:DATE</code>          | La data (in fase di esecuzione) nel formato yyyy-. MM-dd                                                                                                                                                                                                                    |
| <code>global:DATE_TIME</code>     | La data e l'ora (in fase di esecuzione) nel formato yyyy- _ . MM-dd HH.mm.ss                                                                                                                                                                                                |
| <code>global:AWS_PARTITION</code> | Partizione in cui si trova la risorsa. Per impostazione standard Regioni AWS, la partizione è. aws Per risorse in altre partizioni, la partizione è aws- <i>partitionname</i> . Ad esempio, la partizione per le risorse nella regione AWS GovCloud (US-West) è. aws-us-gov |
| <code>global:REGION</code>        | La regione in cui viene eseguito il runbook. Ad esempio, us-east-2.                                                                                                                                                                                                         |

## Variabili del servizio di automazione

I runbook del servizio di automazione supportano le seguenti variabili di automazione.

| Variabile                            | Informazioni                                                                                                       |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <code>automation:EXECUTION_ID</code> | L'identificatore univoco assegnato all'automazione corrente. Ad esempio, 1a2b3c-1a2b3c-1a2b3c-1a2b3c1a2b3c1a2b3c . |

## Argomenti

- [Terminologia](#)
- [Scenari supportati](#)
- [Scenari non supportati](#)

## Terminologia

I seguenti termini descrivono come vengono risolte le variabili e i parametri.

| Termine              | Definizione                                                                                                                                                                                                   | Esempio                                                                                                                                                                                                                                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ARN costante         | Un Amazon Resource Name (ARN) valido senza variabili.                                                                                                                                                         | arn:aws:iam::123456789012:role/roleName                                                                                                                                                                                                                                                         |
| Parametro Runbook    | Parametro definito a livello di runbook (ad esempio, <code>instanceId</code> ). Il parametro viene utilizzato in una sostituzione di stringa di base. Il relativo valore è fornito all'avvio dell'esecuzione. | <pre>{   "description":     "Create Image Demo",   "version": "0.3",   "assumeRole":     "<i>Your_Automation_Assume_Role_ARN</i> ",   "parameters":{     "instanceId": {       "type":         "String",       "description":         "Instance to create         image from"     }   } }</pre> |
| Variabile di sistema | Variabile generica sostituita nel runbook quando una qualsiasi parte del runbook viene valutata.                                                                                                              | <pre>"activities": [   {     "id": "copyImage",     "activityType":       "AWS-CopyImage",     "maxAttempts": 1,     "onFailure":       "Continue",</pre>                                                                                                                                       |

| Termine | Definizione | Esempio                                                                                                                                                                                                                                                         |
|---------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |             | <pre>"inputs": {   "ImageName":     "{{imageName}}",   "SourceImageId": "{{sourceImageId}}",   "SourceRegion": "{{sourceRegion}}",   "Encrypted":     true,   "ImageDescription": "Test     CopyImage Description     created on {{global: DATE}} "   } }</pre> |

| Termine                               | Definizione                                                                                                       | Esempio                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Variabile del servizio di automazione | Variabile relativa all'automazione, sostituita nel runbook quando una qualsiasi parte del runbook viene valutata. | <pre>{   "name": "runFixed Cmds",   "action": "aws:runC ommand",   "maxAttempts": 1,   "onFailure": "Continue",   "inputs": {     "DocumentName": "AWS-RunPowerShell Script",     "InstanceIds": [       "{{Launch Instance.InstanceI ds}}"     ],     "Parameters": {       "commands": [         "dir",         "date",         ""{{outpu tFormat}}"         -f "left","r ight","{{global:DA TE}}"," {{automat ion:EXECUTION_ID}}  "       ]     }   } }</pre> |



| Termine                      | Definizione                                                                                                                                                                                                          | Esempio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parametro di Systems Manager | Una variabile definita all'interno AWS Systems Manager Parameter Store. Non è possibile farvi riferimento direttamente nell'input della fase. Potrebbero essere necessarie autorizzazioni per accedere al parametro. | <pre>description: Launch new Windows test instance schemaVersion: '0.3' assumeRole: '{{AutomationAssumeRole}}' parameters:   AutomationAssumeRole:     type: String     default: ''     description: &gt;-       (Required) The       ARN of the role that       allows Automation to       perform the       actions on your       behalf. If no role is       specified, Systems       Manager       Automation uses       your IAM permissions       to run this runbook.   LatestAmi:     type: String     default: &gt;-       {{ssm:/aws/ service/ami-wind ows-latest/Windows _Server-2016-English- Full-Base}}     description: The     latest Windows Server     2016 AMI queried from     the public parameter. mainSteps:   - name: launchIns tance     action: 'aws:runI nstances'     maxAttempts: 3</pre> |

| Termine | Definizione | Esempio                                                                                                                                      |
|---------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------|
|         |             | <pre>         timeoutSeconds:         1200         onFailure: Abort         inputs:             ImageId: '{{Latest Ami}}'         ... </pre> |

## Scenari supportati

| Scenario                                                                         | Commenti                                                                                                                                   | Esempio                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ARN costante assumeRole al momento della creazione.                              | Viene eseguito un controllo delle autorizzazioni per verificare che l'utente che esegue la chiamata sia autorizzato a passare assumeRole . | <pre> {   "description":     "Test all Automation resolvable parameter s",   "schemaVersion":     "0.3",   "assumeRo le":  "<b>arn:aws:iam::123456789012:role/roleName"</b> ,   "parameters": {     ... </pre> |
| Parametro del runbook fornito per AssumeRole quando viene avviata l'automazione. | Deve essere definito nell'elenco di parametri del runbook.                                                                                 | <pre> {   "description":     "Test all Automation resolvable parameter s",   "schemaVersion":     "0.3",   "assumeRo le":  "<b>{{dynamicARN}}</b>" ,   "parameters": {     ... </pre>                          |

| Scenario                                               | Commenti                                                                                                                                                             | Esempio                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Valore fornito per il parametro del runbook all'avvio. | Il cliente fornisce il valore da utilizzare per un parametro. Gli input di esecuzione forniti all'avvio devono essere definiti nell'elenco di parametri del runbook. | <pre>... "parameters": {   "amiId": {     "type": "String",     "default":       "<i>ami-12345678</i> ",     "description":       "list of commands to       run as part of first       step"   },   ... }</pre> <p>Gli input per l'avvio dell'esecuzione dell'automazione includono: {"amiId" : ["<i>ami-12345678</i> " ] }</p> |

| Scenario                                                                                | Commenti                                                                                                                                                                                                                                                                                                                                                                  | Esempio                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Parametro di Systems Manager referenziato all'interno del contenuto del runbook.</p> | <p>La variabile esiste nell'account del cliente, o è un parametro pubblicamente accessibile, e <code>AssumeRole</code> per il runbook ha accesso alla variabile. Viene eseguito un controllo in fase di creazione per verificare che <code>AssumeRole</code> disponga dell'accesso. Non è possibile fare riferimento al parametro direttamente nell'input della fase.</p> | <pre>... parameters:   LatestAmi:     type: String     default: &gt;-       {{ssm:/aws/ service/ami-wind ows-latest/Windows _Server-2016-English- Full-Base}}     description: The latest Windows Server 2016 AMI queried from the public parameter. mainSteps:   - name: launchIns tance     action: 'aws:runI nstances'     maxAttempts: 3     timeoutSeconds: 1200     onFailure: Abort     inputs:       ImageId: '{{Latest Ami}}' ...</pre> |

| Scenario                                                                               | Commenti                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Esempio                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Variabile di sistema a cui viene fatto riferimento nella definizione della fase</p> | <p>Una variabile di sistema viene sostituita nel runbook all'avvio dell'automazione. Il valore inserito nel runbook fa riferimento al momento in cui viene eseguita la sostituzione. Ad esempio, il valore di una variabile temporale inserita nella fase 1 sarà diverso da quello inserito nella fase 3 a causa del tempo intercorso tra le esecuzioni delle due fasi. Non è necessario che le variabili di sistema siano impostate nell'elenco di parametri del runbook.</p> | <pre>...   "mainSteps": [     {       "name": "RunSomeC ommands",       "action":         "aws:runCommand",       "maxAttempts": 1,       "onFailure":         "Continue",       "inputs": {         "DocumentName":           "AWS:RunPowerShell",         "InstanceIds":           ["{{LaunchInstance .InstanceIds}}"],         "Parameters": {           "commands " : [             "echo {The time is now {{global:DATE_TIME }}}"           ]         }       }     }, ...</pre> |

| Scenario                                                                                          | Commenti                                                                                                                                                                                        | Esempio                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Variabile del servizio di automazione a cui viene fatto riferimento nella definizione della fase. | Non è necessario impostare le variabili del servizio di automazione nell'elenco di parametri del runbook. L'unica variabile del servizio di automazione è supportata è automation:EXECUTION_ID. | <pre>... "mainSteps": [   {     "name": "invokeLambdaFunction",     "action":       "aws:invokeLambdaFunction",     "maxAttempts": 1,     "onFailure":       "Continue",     "inputs": {       "FunctionName":         "Hello-World-LambdaFunction",        "Payload" :         "{ \"executionId\" :           \"{{automation:EXECUTION_ID}}\" }"         }     }   } ] ...</pre> |

| Scenario                                                                                    | Commenti                                                                                                                                                                                                                                                                                                                                                                   | Esempio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Riferimento all'output della fase precedente nella definizione della fase successiva</p> | <p>Si tratta del reindirizzamento di un parametro. L'output di una fase precedente viene indicato con la sintassi <code>{{stepName.OutputName}}</code>. Questa sintassi non può essere utilizzata dal cliente per i parametri del runbook. Questo viene risolto quando viene eseguita la fase di riferimento. Il parametro non è elencato tra i parametri del runbook.</p> | <pre>... "mainSteps": [   {     "name": "LaunchInstance",     "action":       "aws:runInstances",     "maxAttempts": 1,     "onFailure":       "Continue",     "inputs": {       "ImageId":         "{{amiId}}",       "MinInstanceCount": 1,       "MaxInstanceCount": 2     }   },   {     "name": "changeState",     "action":       "aws:changeInstanceState",     "maxAttempts": 1,     "onFailure":       "Continue",     "inputs": {       "InstanceIds":         ["{{LaunchInstance.InstanceIds}}"],       "DesiredState":         "terminated"     }   } ] ...</pre> |

## Scenari non supportati

| Scenario                                                                        | Comment                                                                                  | Esempio                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parametro di Systems Manager fornito per <code>assumeRole</code> alla creazione | Non supportato.                                                                          | <pre> ...  {   "description":     "Test all Automation     resolvable parameter s",   "schemaVersion":     "0.3",   "assumeRole":     "{{ssm:administrato rRoleARN}}" ,   "parameters": {     ... </pre>                                                                                        |
| Parametro di Systems Manager a cui si fa riferimento nell'input della fase.     | Restituisce un'eccezione <code>InvalidDocumentContent</code> al momento della creazione. | <pre> ... mainSteps:   - name: launchIns     tance       action: 'aws:runI nstances'       maxAttempts: 3       timeoutSeconds: 1200       onFailure: Abort       inputs:         ImageId: '{{ssm:/ aws/service/ami-win dows-latest/Window s_Server-2016-Engl ish-Full-Base}}'       ... </pre> |
| Definizione della fase mediante variabili                                       | La definizione di una fase nel runbook si basa su variabili.                             | <pre> ... </pre>                                                                                                                                                                                                                                                                                |



| Scenario | Comment | Esempio                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          |         | <pre>"mainSteps": [<br/>  {<br/>    "name": "LaunchIn<br/>stance",<br/>    "action":<br/>      "aws:runInstances",<br/>    "{{attempt<br/>Model}} ": 1,<br/>    "onFailure":<br/>      "Continue",<br/>    "inputs": {<br/>      "ImageId":<br/>        "ami-12345678 ",<br/>      "MinInsta<br/>nceCount": 1,<br/>      "MaxInsta<br/>nceCount": 2<br/>    }<br/><br/>    ...<br/><br/>    User supplies input :<br/>    { "attemptModel" :<br/>      "minAttempts " }</pre> |

| Scenario                                       | Comment                                                                                                              | Esempio                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Riferimento incrociato a parametri del runbook | L'utente fornisce un parametro di input all'avvio, che rappresenta un riferimen to a un altro parametro nel runbook. | <pre>... "parameters": {   "amiId": {     "type": "String",     "default":       "ami-7f2e6015 ",     "description":       "list of commands to       run as part of first       step"   },   "alternateAmiId": {     "type": "String",     "description":       "The alternate AMI       to try if this first       fails".  "default" : "{{amiId} }"   }, ... </pre> |

| Scenario               | Comment                                                                                                                                                                                                                                          | Esempio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Multi-level espansione | Il runbook definisce una variabile che restituisce il nome di una variabile. Si trova all'interno dei delimitatori delle variabili (ovvero <code>{{}}</code> ) e viene espanso fino al valore di tale variabile. <code>variable/parameter</code> | <pre> ... "parameters": {   "<i>firstParameter</i> ": {     "type": "String",     "default": "param2",     "description": "The parameter to reference"   },   "<i>secondParameter</i> ": {   "type": "String",   "default" : "echo {Hello world}",   "description": "What to run" } }, "mainSteps": [{   "name": "runFixed Cmds",   "action": "aws:runCommand",   "maxAttempts": 1,   "onFailure": "Continue",   "inputs": {     "DocumentName": "AWS-RunPowerShell Script",  "InstanceIds" : "{{LaunchInstance. InstanceIds}}",     "Parameters": {       "commands ": [ "<i>firstPa rameter</i>"}  ]"} } </pre> |

| Scenario | Comment | Esempio                                                                                                                 |
|----------|---------|-------------------------------------------------------------------------------------------------------------------------|
|          |         | <div><div>...</div><div>Note: The customer intention here would be to run a command of "echo {Hello world}"</div></div> |

| Scenario                                                                             | Comment                                                                                                                                                                                                                 | Esempio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Riferimento all'output da una fase del runbook con un altro tipo di variabile</p> | <p>L'utente fa riferimento all'output da una fase di un runbook precedente all'interno di una fase successiva. L'output ha un tipo di variabile che non soddisfa i requisiti dell'operazione nella fase successiva.</p> | <pre> ... mainSteps: - name: getImageId   action: aws:executeAwsApi   inputs:     Service: ec2     Api: DescribeImages     Filters:       - Name: "name"       Values:         - "{{ImageName}}"   outputs:     - Name: ImageIdList       Selector: "\$.Images"     Type: "StringList" - name: copyMyImages   action: aws:copyImage   maxAttempts: 3   onFailure: Abort   inputs:     SourceImageId:       {{getImageId.ImageIdList}}     SourceRegion: ap-northeast-2     ImageName:       Encrypted Copies of LAMP base AMI in ap-northeast-2     Encrypted: true ... Note: You must provide the type required by the Automation action. In this case, aws:copyImage requires a "String" type variable but the preceding step </pre> |

| Scenario | Comment | Esempio                               |
|----------|---------|---------------------------------------|
|          |         | outputs a "StringList" type variable. |

## Creazione di runbook personalizzati

Un runbook di automazione definisce le azioni che Systems Manager esegue sulle istanze gestite e su altre AWS risorse quando viene eseguita un'automazione. L'automazione è uno strumento di AWS Systems Manager. Un runbook contiene una o più fasi che si eseguono in ordine sequenziale. Ogni fase è riferita a una singola operazione. L'output di una fase può essere utilizzato come input in una fase successiva.

Il processo di esecuzione di queste operazioni e delle relative fasi è chiamato automazione.

I tipi di azione supportati dai runbook consentono di automatizzare un'ampia varietà di operazioni nel proprio ambiente. AWS Ad esempio, utilizzando il tipo di `executeScript` azione, puoi incorporare un python o uno PowerShell script direttamente nel tuo runbook. (Quando si crea un runbook personalizzato, è possibile aggiungere lo script in linea o collegarlo da un bucket S3 o dal computer locale). Puoi automatizzare la gestione delle tue AWS CloudFormation risorse utilizzando i tipi di azione e `createStack` `deleteStack` Inoltre, utilizzando il tipo di `executeAwsApi` azione, un passaggio può eseguire qualsiasi operazione API in qualsiasi momento Servizio AWS, inclusa la creazione o l'eliminazione di AWS risorse, l'avvio di altri processi, l'avvio di notifiche e molto altro.

Per un elenco di tutti i 20 tipi di operazione supportati per le fasi di automazione, consulta [Riferimento alle operazioni del servizio di automazione di Systems Manager](#).

AWS Systems Manager L'automazione fornisce diversi runbook con passaggi predefiniti che puoi utilizzare per eseguire attività comuni come il riavvio di una o più istanze di Amazon Elastic Compute Cloud (Amazon EC2) o la creazione di una (). Amazon Machine Image AMI Puoi anche creare i tuoi runbook e condividerli con altri o renderli pubblici per tutti gli utenti di Account AWS Automation.

I runbook sono redatti in formato YAML o JSON. Tuttavia, utilizzando lo strumento Document Builder (Generatore documenti) nella console del servizio di automazione di Systems Manager, è possibile creare un runbook senza doverlo creare in formato JSON o YAML nativo.

 Important

Se si esegue un flusso di lavoro di automazione che chiama altri servizi utilizzando un ruolo di servizio (IAM) di AWS Identity and Access Management , tenere presente che tale ruolo di servizio deve essere configurato con l'autorizzazione per la chiamata di tali servizi. Questo requisito si applica a tutti i runbook (AWS - \*runbook) di AWS Automation come, e i AWS-RestartEC2Instance runbook AWS-ConfigureS3BucketLoggingAWS-CreateDynamoDBBackup, solo per citarne alcuni. Questo requisito si applica anche a tutti i runbook di Automation personalizzati creati che richiamano altri utenti Servizi AWS utilizzando azioni che richiamano altri servizi. Ad esempio, se utilizzi le operazioni `aws:executeAwsApi`, `aws:createStack` o `aws:copyImage`, devi configurare il ruolo di servizio con l'autorizzazione per richiamare tali servizi. Puoi concedere le autorizzazioni ad altri Servizi AWS aggiungendo una policy inline IAM al ruolo. Per ulteriori informazioni, consulta [\(Facoltativo\) Aggiungi una policy in linea di Automation o una policy gestita dal cliente per richiamarne altre Servizi AWS](#).

Per visualizzare informazioni su operazioni che è possibile specificare in runbook, consulta [Riferimento alle operazioni del servizio di automazione di Systems Manager](#).

Per informazioni sull'utilizzo di To Create AWS Toolkit for Visual Studio Code Runbook, consultate i documenti [Working with Systems Manager Automation](#) nella Guida per l'AWS Toolkit for Visual Studio Code utente.

Per informazioni sull'utilizzo del visual designer per creare un runbook personalizzato, consulta [Esperienza di progettazione visiva per i runbook Automation](#).

Esperienza di progettazione visiva per i runbook Automation

AWS Systems Manager L'automazione offre un'esperienza di progettazione visiva low-code che consente di creare runbook di automazione. Offre un'interfaccia drag-and-drop con la possibilità di aggiungere il proprio codice. Con l'esperienza di progettazione visiva puoi completare le seguenti operazioni:

Questa sezione contiene gli argomenti seguenti.

- [Gestione degli errori con l'esperienza di progettazione visiva](#)
- [Configurazione di input e output per le tue operazioni](#)

- [Tutorial: Creazione di un runbook utilizzando l'esperienza di progettazione visiva](#)
  - [Panoramica dell'interfaccia dell'esperienza di progettazione visiva](#)
  - [Utilizzo dell'esperienza di progettazione visiva](#)
- 
- Controlla le istruzioni condizionali.
  - Controllare come l'input e l'output vengono filtrati o trasformati per ogni azione.
  - Configura la gestione degli errori.
  - Creare prototipi di nuovi runbook.
  - Usare i tuoi runbook prototipati come punto di partenza per lo sviluppo locale con il AWS Toolkit for Visual Studio Code.

Quando crei o modifichi un runbook, puoi accedere all'esperienza di progettazione visiva dalla [console di Automation](#). Man mano che crei un runbook, l'esperienza di progettazione visiva convalida le operazioni e genera automaticamente il codice. Puoi rivedere il codice generato o esportarlo per lo sviluppo locale. Al termine, sarà possibile salvare il runbook, eseguirlo ed esaminare i risultati nella console di Systems Manager Automation.

## Argomenti

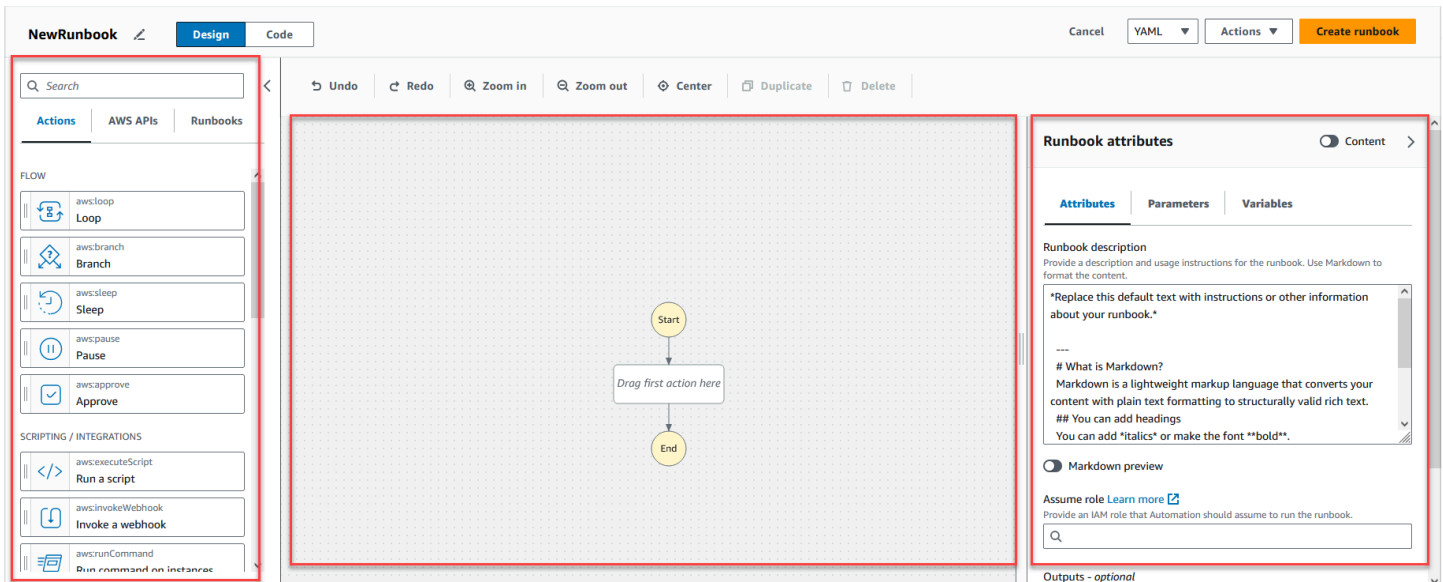
- [Panoramica dell'interfaccia dell'esperienza di progettazione visiva](#)
- [Utilizzo dell'esperienza di progettazione visiva](#)
- [Configurazione di input e output per le tue operazioni](#)
- [Gestione degli errori con l'esperienza di progettazione visiva](#)
- [Tutorial: Creazione di un runbook utilizzando l'esperienza di progettazione visiva](#)

## Panoramica dell'interfaccia dell'esperienza di progettazione visiva

L'esperienza di progettazione visiva per Systems Manager Automation è una progettazione di flussi di lavoro visivi con low code che consente di creare runbook Automation.

Scopri l'esperienza di progettazione visiva con una panoramica dei componenti dell'interfaccia:





- Il browser Operazioni contiene le schede Operazioni, API AWS e Runbook.
- La tela è il punto in cui sposti le azioni nel grafico del flusso di lavoro. Puoi anche modificare l'ordine delle azioni e selezionarle da configurare.
- Il pannello Modulo consente di visualizzare e modificare le proprietà di qualsiasi operazione selezionata nell'area di disegno. Seleziona l'interruttore Contenuto per visualizzare YAML o JSON per il runbook, con l'operazione correntemente selezionata evidenziata.

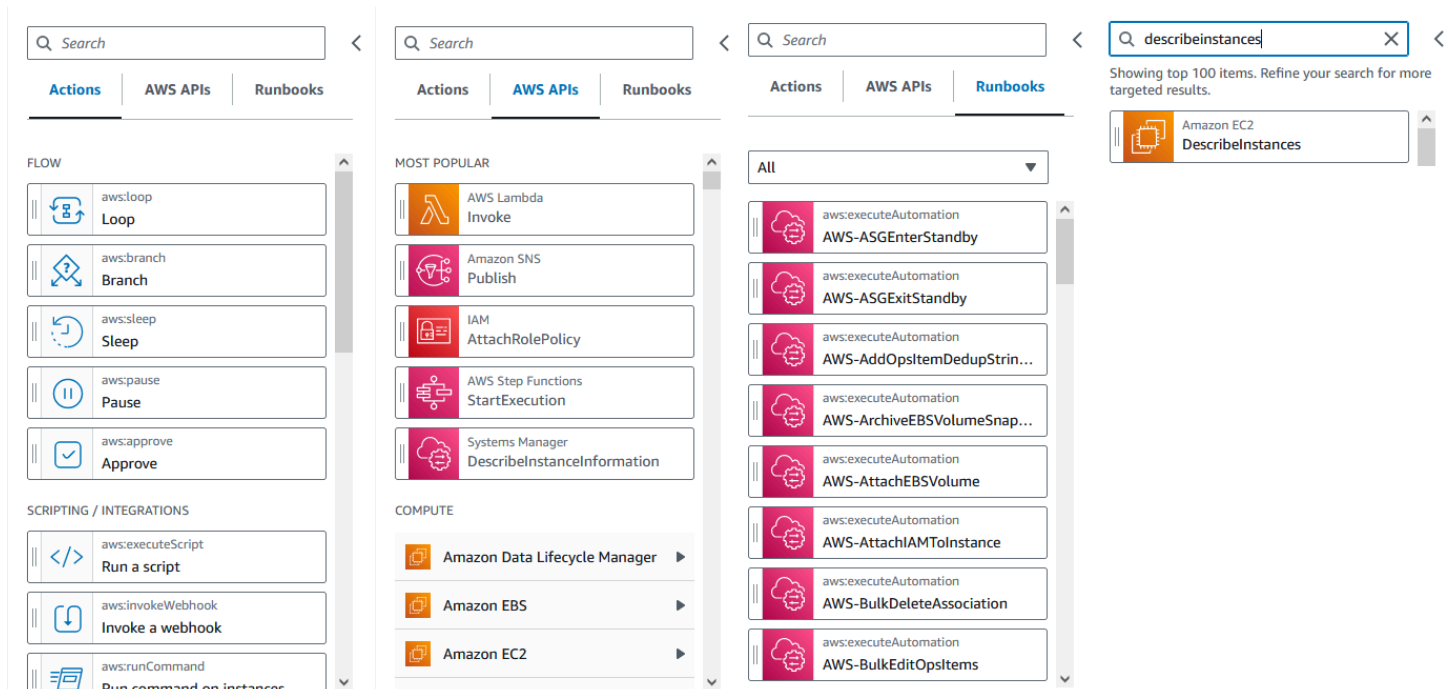
I link informativi aprono un pannello con informazioni contestuali quando hai bisogno di aiuto. Questi pannelli includono anche collegamenti ad argomenti correlati nella documentazione di Systems Manager Automation.

## Browser delle operazioni

Dal browser Azioni, puoi selezionare le azioni da spostare nel grafico del flusso di lavoro. Puoi cercare tutte le operazioni utilizzando il campo di ricerca nella parte superiore del browser Operazioni. Il browser Operazioni contiene le seguenti schede:

- La scheda Azioni fornisce un elenco di azioni di automazione che puoi spostare nel grafico del flusso di lavoro del runbook nell'area di disegno.
- La scheda AWS API elenca le AWS API che puoi spostare nel grafico del flusso di lavoro del runbook.

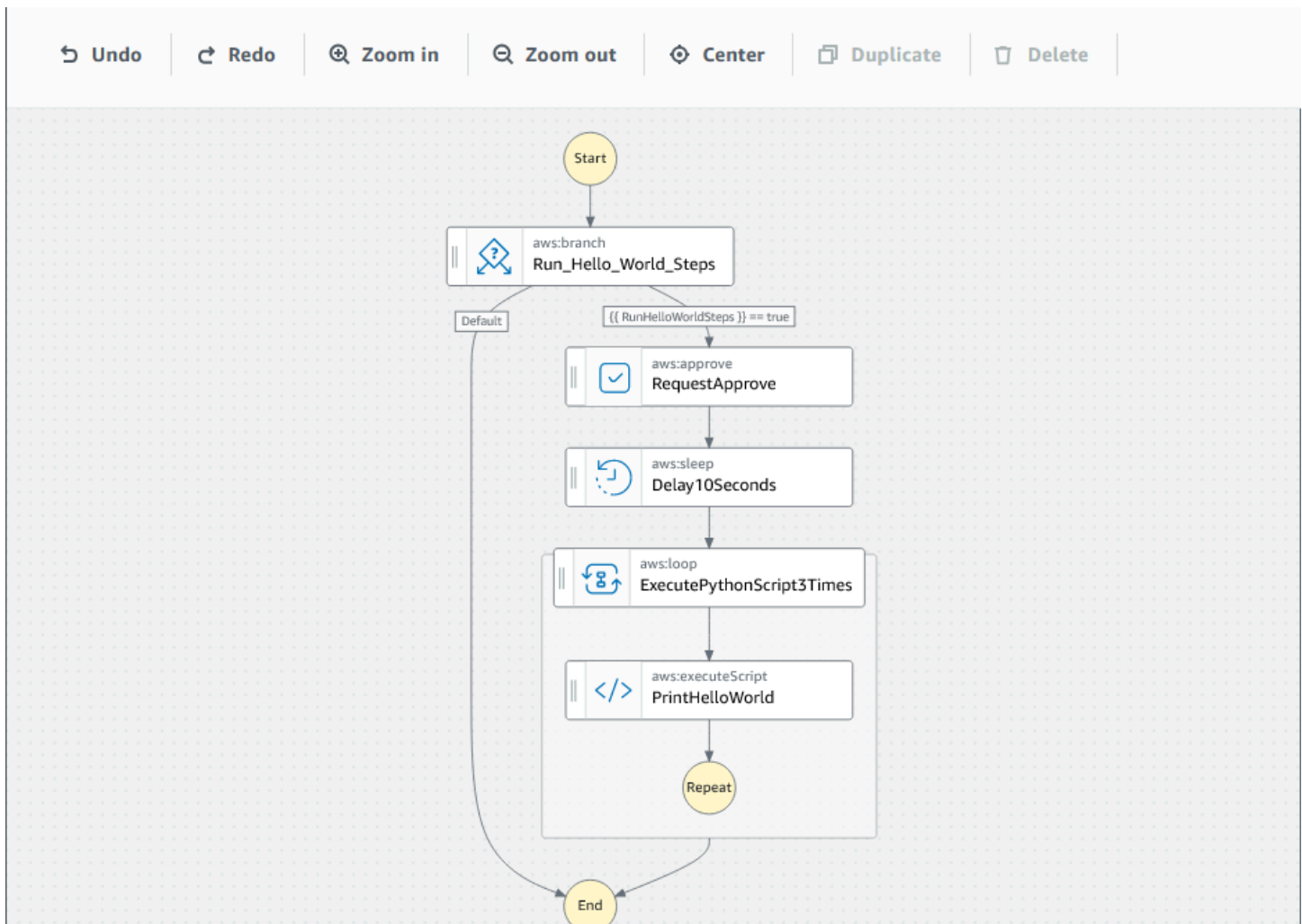
- La scheda Runbooks fornisce runbook pronti all'uso come elementi costitutivi. Ad esempio, puoi utilizzarli per eseguire attività di riparazione comuni sulle istanze Amazon EC2 senza ricreare le stesse azioni.



## Canvas

Dopo aver scelto un'azione, trascinala nell'area di disegno e inseriscila nel grafico del flusso di lavoro. Puoi anche spostare le azioni per riordinarle. Se il flusso di lavoro è complesso, potresti non visualizzarlo tutto in una volta. Usa i controlli in alto per ingrandire o rimpicciolire. Per visualizzare altre parti, sposta il grafico del flusso di lavoro nell'area di disegno.

Sposta un'azione dal browser Azioni nel grafico del flusso di lavoro del tuo runbook. Una riga mostra dove verrà posizionato nel flusso di lavoro. Per modificare l'ordine di un'azione, puoi spostarla in un punto diverso del flusso di lavoro. La nuova azione è stata aggiunta al flusso di lavoro e il relativo codice viene generato automaticamente.



## Modulo

Dopo aver aggiunto un'operazione al flusso di lavoro del runbook, puoi configurarla in base al tuo caso d'uso. Scegli l'azione che desideri configurare e ne vedrai i parametri e le opzioni nel pannello Modulo. Puoi vedere il codice YAML o JSON anche selezionando l'interruttore Contenuto. Il codice associato all'operazione selezionata viene evidenziato.

```
graph TD; Start((Start)) --> Branch[aws:branch
Run_Hello_World_Steps]; Branch -- Default --> End((End)); Branch -- "[[RunHelloWorldSteps]] == true" --> Approve[aws:approve
RequestApprove]; Approve --> Sleep[aws:sleep
Delay10Seconds]; Sleep --> Loop[aws:loop
ExecutePythonScript3Times]; Loop --> Script[aws:executeScript
PrintHelloWorld]; Script -- Repeat --> Loop; Loop -- Repeat --> End;
```

← Back to Runbook attributes

ExecutePythonScript3Times

Content

GeneralInputsOutputsConfiguration

Configure one or more inputs for the action type you selected. The input fields provided for you depend on the action type you selected for the step.

Loop type

The type of loop: Do while or For each loop

Do while

Loop condition

The condition that Automation will evaluate before starting another loop iteration.

Condition definition

[[ RunHelloWorldSteps ]] == true

Maximum iterations

The maximum number of times the steps in the loop run. Once the value specified for this input is reached, the loop stops running even if the LoopCondition is still true or if there are objects remaining in the Iterators parameter. The maximum value is 100.

3

```
graph TD; Start((Start)) --> Branch[aws:branch
Run_Hello_World_Steps]; Branch -- Default --> End((End)); Branch -- "[[RunHelloWorldSteps]] == true" --> Approve[aws:approve
RequestApprove]; Approve --> Sleep[aws:sleep
Delay10Seconds]; Sleep --> Loop[aws:loop
ExecutePythonScript3Times]; Loop --> Script[aws:executeScript
PrintHelloWorld]; Script -- Repeat --> Loop; Loop -- Repeat --> End;
```

Content (read-only)

Copy

Content

```
1 schemaVersion: '0.3'
2 parameters:
3 AutomationAssumeRole:
4 type: AWS::IAM::Role::Arn
5 default: ''
6 description: (Optional) The ARN of the role that allows
7 Automation to perform the actions on your behalf.
8 RunHelloWorldSteps:
9 type: Boolean
10 description: Determines which branch of actions to run.
11 Approvers:
12 type: StringList
13 description: (Required) IAM user or user arn of approvers
14 for the automation action
15 assumeRole: '{{ AutomationAssumeRole }}'
16 description: |-
17 This sample runbook demonstrates the usage of the following
18 Automation actions:
19 * aws:branch
20 * aws:approve
21 * aws:sleep
22 * aws:loop
23 * aws:executeScript
24 mainSteps:
25 - name: Run_Hello_World_Steps
26 action: aws:branch
27 isEnd: true
28 inputs:
29 Choices:
30 - NextStep: RequestApprove
31 Variable: '{{ RunHelloWorldSteps }}'
32 BooleanEquals: true
```

Tasti di scelta rapida

L'esperienza di progettazione visiva supporta le scelte rapide da tastiera mostrate nella tabella seguente.

Servizio di automazione

1408

|                                                                             |  |
|-----------------------------------------------------------------------------|--|
| <b>Fastione</b><br>di<br>scelta<br>rapida                                   |  |
| <b>Attiva</b><br>l'ultima<br>operazione<br>e.                               |  |
| <b>Attiva</b><br>l'ultima<br>operazione<br>eZ                               |  |
| <b>Centra</b><br>il<br>flusso<br>di<br>lavoro<br>nell'area<br>di<br>lavoro. |  |
| <b>Backspace</b><br>tutti<br>gli<br>stati<br>seleziona<br>ti.               |  |
| <b>Elimina</b><br>tutti<br>gli<br>stati<br>seleziona<br>ti.                 |  |

**Fastione**

di  
scelta  
rapida

**OTRica**

**to**  
stato  
seleziona  
to.

Utilizzo dell'esperienza di progettazione visiva

Impara a creare, modificare ed eseguire flussi di lavoro runbook utilizzando l'esperienza di progettazione visiva. Quando il flusso di lavoro è pronto, salvalo o esportalo. Puoi anche usarlo per la prototipazione rapida.

Creazione di un flusso di lavoro del runbook

1. Accedi alla [console di Systems Manager Automation](#).
2. Scegli Crea runbook.
3. Nella casella Nome, immetti un nome per il runbook, ad esempio *MyNewRunbook*.
4. Accanto agli interruttori Progettazione e Codice, seleziona l'icona a forma di matita e inserisci un nome per il runbook.

Ora puoi progettare un flusso di lavoro per il tuo nuovo runbook.

Progettazione di un runbook

Per progettare un flusso di lavoro in runbook, sposta un'azione di automazione dal browser Azioni nella tela. Posizionala dove vuoi nel tuo flusso di lavoro. Puoi riordinare le azioni spostandole in una posizione diversa. Quando sposti un'azione sull'area di disegno, una riga mostra dove puoi rilasciarla. Dopo aver rilasciato un'azione, il relativo codice viene generato automaticamente e aggiunto al contenuto del runbook.

Usa la casella di ricerca nella parte superiore del browser Azioni per trovare un'azione in base al nome.

Dopo aver trascinato un'operazione nell'area di lavoro, configurala utilizzando il pannello Modulo sulla destra. Questo pannello contiene le schede Generale, Ingressi, Uscite e Configurazione per ogni azione sull'area di disegno. La scheda Generale contiene le seguenti sezioni:

- Nome fase identifica la fase. Specifica un valore univoco per il nome della fase.
- Descrizione ti aiuta a descrivere cosa sta facendo l'operazione nel flusso di lavoro del runbook.

La scheda Input contiene campi che variano in base all'operazione. Ad esempio, l'operazione di automazione `aws:executeScript` contiene le sezioni seguenti:

- In Runtime, scegliere il linguaggio da utilizzare per eseguire lo script fornito.
- Il gestore è il nome della funzione. È necessario assicurarsi che la funzione definita nel gestore abbia due parametri: `events` e `context`. Il runtime di PowerShell non supporta questo parametro.
- Script è uno script incorporato che si desidera eseguire durante il flusso di lavoro.
- (Facoltativo) Allegato è destinato agli script autonomi o ai file .zip che possono essere richiamati dall'operazione. Questo parametro è obbligatorio per i runbook JSON.

La scheda Output consente di specificare i valori che si desidera generare da un'operazione. È possibile fare riferimento ai valori di output nelle operazioni successive del flusso di lavoro o generare output da operazioni a scopo di registrazione. Non tutte le operazioni avranno una scheda Output perché non tutte le operazioni supportano gli output. Ad esempio, l'operazione `aws:pause` non supporta gli output. Per le operazioni che supportano gli output, la scheda Output è composta dalle seguenti sezioni:

- Nome è il nome da utilizzare per il valore di output. È possibile fare riferimento agli output nelle operazioni successive del flusso di lavoro.
- Il selettore è una stringa di espressione JSONPath che inizia con "\$." e che viene utilizzata per selezionare uno o più componenti all'interno di un elemento JSON.
- Tipo è il tipo di dati per il valore di output. Ad esempio, un tipo di dati `String` o `Integer`.

La scheda Configurazione contiene proprietà e opzioni utilizzabili da tutte le operazioni di automazione. L'operazione è costituita dalle seguenti sezioni:

- La proprietà Numero massimo di tentativi indica il numero di tentativi di ripetizione di un'operazione in caso di esito negativo.

- La proprietà `Seconds of timeout` specifica il valore di timeout per un'operazione.
- La proprietà `Is critical` determina se l'errore dell'operazione interrompe l'intera automazione.
- La proprietà `Next phase` determina l'operazione successiva dell'automazione nel runbook.
- La proprietà `On error` determina l'operazione successiva dell'automazione nel runbook se l'operazione non riesce.
- La proprietà `On cancel` determina l'operazione successiva dell'automazione nel runbook se l'operazione viene annullata da un utente.

Per eliminare un'azione, puoi usare `backspace`, la barra degli strumenti sopra l'area di disegno, oppure aprire il menu contestuale e scegliere `Elimina azione`.

Man mano che il flusso di lavoro cresce, potrebbe non rientrare nell'area di lavoro. Per adattare il flusso di lavoro all'area di lavoro, prova una delle seguenti opzioni:

- Utilizza i controlli nei pannelli laterali per ridimensionare o chiudere i pannelli.
- Usa la barra degli strumenti nella parte superiore dell'area di lavoro per ingrandire o ridurre il grafico del flusso di lavoro.

## Aggiornamento del runbook

Puoi aggiornare un flusso di lavoro del runbook esistente creando una nuova versione del runbook. Gli aggiornamenti ai runbook possono essere effettuati utilizzando l'esperienza di progettazione visiva o modificando direttamente il codice. Per aggiornare un runbook esistente, completa la procedura descritta di seguito.

1. Accedi alla [console di Systems Manager Automation](#).
2. Scegli il runbook da aggiornare.
3. Scegliere `Create new version` (Crea nuova versione).
4. L'esperienza di progettazione visiva ha due riquadri: un riquadro del codice e un riquadro del flusso di lavoro dell'elemento visivo. Scegli `Progettazione` nel riquadro del flusso di lavoro dell'elemento visivo per modificare il flusso di lavoro con l'esperienza di progettazione visiva. Al termine, scegli `Creazione di una nuova versione` per salvare le modifiche e uscire.
5. (Facoltativo) Usa il riquadro del codice per modificare il contenuto del runbook in YAML o JSON.



## Esportazione del runbook

Per esportare il codice YAML o JSON del flusso di lavoro del runbook e anche un grafico del flusso di lavoro, utilizza la seguente procedura:

1. Scegli il tuo runbook nella console Documenti.
2. Scegliere Create new version (Crea nuova versione).
3. Nel menu a discesa Operazioni, scegli se esportare il grafico o il runbook e quale formato preferisci.

## Configurazione di input e output per le tue operazioni

Ogni operazione di automazione risponde in base all'input che riceve. Di solito, si passa quindi l'output alle azioni successive. Nell'esperienza di progettazione visiva, puoi configurare i dati di input e output di un'azione nelle schede Input e Output del riquadro Modulo.

Per informazioni dettagliate su come definire e usare l'output per le operazioni di automazione, consulta [Utilizzo degli output delle operazioni come input](#).

### Specifica dei dati di input per un'operazione

Ogni operazione di automazione ha uno o più input per i quali è necessario fornire un valore. Il valore fornito per l'input di un'azione è determinato dal tipo e dal formato di dati accettati dall'azione. Ad esempio, le operazioni `aws:sleep` richiedono un valore di stringa in formato ISO 8601 per l'input `Duration`.

In genere, si utilizzano operazioni nel flusso di lavoro del runbook che restituiscono l'output che si desidera utilizzare nelle operazioni successive. È importante assicurarsi che i valori di input siano corretti per evitare errori nel flusso di lavoro del runbook. I valori di input sono importanti anche perché determinano se l'azione restituisce l'output previsto. Ad esempio, quando usi l'`aws:executeAwsApi` azione, vuoi assicurarti di fornire il valore giusto per l'operazione API.

### Definizione dei dati di output per un'azione

Alcune operazioni di automazione restituiscono l'output dopo aver eseguito le operazioni definite. Le operazioni che restituiscono un output hanno output predefiniti o consentono di definire gli output autonomamente. Ad esempio, l'operazione `aws:createImage` ha output predefiniti che restituiscono un `ImageId` e `ImageState`. Comparativamente, con l'operazione `aws:executeAwsApi` è possibile definire gli output desiderati dall'operazione API specificata. Di

conseguenza, è possibile restituire uno o più valori da una singola operazione API da utilizzare nelle azioni successive.

Per definire i propri output per un'operazione di automazione è necessario specificare un nome dell'output, il tipo di dati e il valore dell'output. Per continuare a utilizzare l'operazione `aws:executeAwsApi` come esempio, supponiamo che tu stia chiamando l'operazione API `DescribeInstances` da Amazon EC2. In questo esempio, vuoi restituire, o emettere, lo `State` di un'istanza Amazon EC2 e ramificare il flusso di lavoro del runbook in base all'output. Scegli di assegnare un nome all'output **InstanceState** e utilizza il tipo di dati **String**.

Il modo in cui definisci il valore di output dipende dall'azione. Ad esempio, con `aws:executeScript`, utilizza `return` le istruzioni nelle tue funzioni per fornire dati agli output. Con azioni come `aws:executeAwsApi` o `aws:waitForAwsResourceProperty`, `aws:assertAwsResourceProperty`, a `Selector` è richiesto. La `Selector` (chiamata anche `PropertySelector`) è una `JSONPath` stringa che elabora la risposta JSON di un'operazione API. È necessario comprendere come è strutturata la risposta JSON in modo da poter selezionare il valore corretto. Utilizzando l'operazione `DescribeInstances` API, vedi il seguente esempio di risposta:

```
{
 "reservationSet": {
 "item": {
 "reservationId": "r-1234567890abcdef0",
 "ownerId": 123456789012,
 "groupSet": "",
 "instancesSet": {
 "item": {
 "instanceId": "i-1234567890abcdef0",
 "imageId": "ami-bff32ccc",
 "instanceState": {
 "code": 16,
 "name": "running"
 },
 "privateDnsName": "ip-192-168-1-88.eu-west-1.compute.internal",
 "dnsName": "ec2-54-194-252-215.eu-west-1.compute.amazonaws.com",
 "reason": "",
 "keyName": "my_keypair",
 "amiLaunchIndex": 0,
 "productCodes": "",
 "instanceType": "t2.micro",
 "launchTime": "2018-05-08T16:46:19.000Z",
```

```
"placement": {
 "availabilityZone": "eu-west-1c",
 "groupName": "",
 "tenancy": "default"
},
"monitoring": {
 "state": "disabled"
},
"subnetId": "subnet-56f5f000",
"vpcId": "vpc-11112222",
"privateIpAddress": "192.168.1.88",
"ipAddress": "54.194.252.215",
"sourceDestCheck": true,
"groupSet": {
 "item": {
 "groupId": "sg-e4076000",
 "groupName": "SecurityGroup1"
 }
},
"architecture": "x86_64",
"rootDeviceType": "ebs",
"rootDeviceName": "/dev/xvda",
"blockDeviceMapping": {
 "item": {
 "deviceName": "/dev/xvda",
 "ebs": {
 "volumeId": "vol-1234567890abcdef0",
 "status": "attached",
 "attachTime": "2015-12-22T10:44:09.000Z",
 "deleteOnTermination": true
 }
 }
},
"virtualizationType": "hvm",
"clientToken": "xMcwG14507example",
>tagSet": {
 "item": {
 "key": "Name",
 "value": "Server_1"
 }
},
"hypervisor": "xen",
"networkInterfaceSet": {
 "item": {
```

```
"networkInterfaceId": "eni-551ba000",
"subnetId": "subnet-56f5f000",
"vpcId": "vpc-11112222",
"description": "Primary network interface",
"ownerId": 123456789012,
"status": "in-use",
"macAddress": "02:dd:2c:5e:01:69",
"privateIpAddress": "192.168.1.88",
"privateDnsName": "ip-192-168-1-88.eu-west-1.compute.internal",
"sourceDestCheck": true,
"groupSet": {
 "item": {
 "groupId": "sg-e4076000",
 "groupName": "SecurityGroup1"
 }
},
"attachment": {
 "attachmentId": "eni-attach-39697adc",
 "deviceIndex": 0,
 "status": "attached",
 "attachTime": "2018-05-08T16:46:19.000Z",
 "deleteOnTermination": true
},
"association": {
 "publicIp": "54.194.252.215",
 "publicDnsName": "ec2-54-194-252-215.eu-west-1.compute.amazonaws.com",
 "ipOwnerId": "amazon"
},
"privateIpAddressesSet": {
 "item": {
 "privateIpAddress": "192.168.1.88",
 "privateDnsName": "ip-192-168-1-88.eu-west-1.compute.internal",
 "primary": true,
 "association": {
 "publicIp": "54.194.252.215",
 "publicDnsName": "ec2-54-194-252-215.eu-
west-1.compute.amazonaws.com",
 "ipOwnerId": "amazon"
 }
 }
},
"ipv6AddressesSet": {
 "item": {
 "ipv6Address": "2001:db8:1234:1a2b::123"
```

```
 }
 }
}

},
"iamInstanceProfile": {
 "arn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
 "id": "ABCAJEDNCAA64SSD123AB"
},
"ebsOptimized": false,
"cpuOptions": {
 "coreCount": 1,
 "threadsPerCore": 1
}
}
}
}
}
```

Nell'oggetto di risposta JSON, l'istanza State è nidificata in un oggetto Instances, che è nidificato nell'oggetto Reservations. Per restituire il valore dell'istanza State, usa la seguente stringa per il Selector in modo che il valore possa essere utilizzato nel nostro output:

```
$.Reservations[0].Instances[0].State.Name.
```

Per fare riferimento a un valore di output nelle operazioni successive del flusso di lavoro del runbook, viene utilizzato il seguente formato: `{{ StepName.NameOfOutput }}`. Ad esempio, `{{ GetInstanceState.InstanceState }}`. Nell'esperienza di progettazione visiva, puoi scegliere i valori di output da utilizzare nelle operazioni successive utilizzando il menu a discesa per l'input. Quando si utilizzano gli output in operazioni successive, il tipo di dati dell'output deve corrispondere al tipo di dati per l'input. In questo esempio, l'output InstanceState è una String. Pertanto, per utilizzare il valore nell'input di un'azione successiva, l'input deve accettare un String.

## Gestione degli errori con l'esperienza di progettazione visiva

Per impostazione predefinita, quando un'azione segnala un errore, Automation interrompe completamente il flusso di lavoro del runbook. Questo perché il valore predefinito per la proprietà `onFailure` su tutte le operazioni è `Abort`. Puoi configurare il modo in cui Automation gestisce gli errori nel flusso di lavoro del runbook. Anche se hai configurato la gestione degli errori, alcuni errori potrebbero comunque causare il fallimento di un'automazione. Per ulteriori informazioni, consulta [Risoluzione dei problemi di servizio di automazione di Systems Manager](#). Nell'esperienza di progettazione visiva, la gestione degli errori viene configurata nel pannello Configurazione.

**getInstanceState** Content >

**General** | **Inputs** | **Outputs** | **Configuration**

The following properties define execution behavior for a step. For example, how long to wait for a step to complete and what to do if it fails. [Learn more](#)

**Max attempts**

  
Valid characters include integers only

**Timeout seconds**

  
Valid characters include integers only

**Is critical**

**Next step**

**On failure**

**On cancel**

## Nuovo tentativo dell'azione in caso di errore

Per ripetere un'azione in caso di errore, specifica un valore per la proprietà Numero massimo di tentativi. Il valore predefinito è 1. Se si specifica un valore maggiore di 1, l'azione non viene considerata non riuscita finché tutti i nuovi tentativi non hanno restituito un esito negativo.

## Timeout

È possibile configurare un timeout per le operazioni per impostare il numero massimo di secondi in cui l'azione può essere eseguita prima che abbia esito negativo. Immettete il valore nella proprietà Timeout seconds. Se il timeout viene raggiunto ed Max attempts è maggiore di 1, il passaggio viene considerato scaduto solo dopo il completamento di tutti i tentativi.

## Operazioni non riuscite

Per impostazione predefinita, quando un'azione segnala un errore, Automation interrompe completamente il flusso di lavoro del runbook. È possibile modificare questo comportamento specificando un valore alternativo per la proprietà `In caso di errore delle operazioni nel runbook`. Se desideri che il flusso di lavoro continui con la fase successiva del runbook, scegli `Continua`. Se desideri che il flusso di lavoro passi a una fase successiva diversa nel runbook, scegli `Fase` e inserisci il nome della fase.

## Operazioni annullate

Per impostazione predefinita, quando un'operazione viene annullata da un utente, Automation interrompe completamente il flusso di lavoro del runbook. È possibile modificare questo comportamento specificando un valore alternativo per la proprietà `In caso di annullamento delle operazioni nel runbook`. Se desideri che il flusso di lavoro passi a una fase successiva diversa nel runbook, scegli `Fase` e inserisci il nome della fase.

## Operazioni critiche

È possibile designare un'operazione come critica, vale a dire che determina lo stato generale dei report dell'automazione. Se una fase con questa definizione ha esito negativo, Automation riporta lo stato finale come `Failed`, indipendentemente dalla riuscita di altre operazioni. Per configurare un'azione come critica, lascia il valore predefinito su `True` per la proprietà `Is critical`.

## Termine delle azioni

La proprietà `Is end` arresta l'automazione alla fine dell'operazione specificata. Il valore predefinito per questa proprietà è `false`. Se si configura questa proprietà per un'operazione, l'automazione si interrompe indipendentemente dal fatto che l'operazione riesca o meno. Questa proprietà viene spesso utilizzata con operazioni `aws:branch` per gestire valori di input imprevisti o non definiti. L'esempio seguente mostra un runbook che prevede uno stato dell'istanza di `running`, `stopping` o `stopped`. Se un'istanza si trova in uno stato diverso, l'automazione termina.

branchOnInstanceState

Content >

General

Inputs

Outputs

Configuration

Configure one or more inputs for the action type you selected. The input fields provided for you depend on the action type you selected for the step.

**Choices**

Branch rules let you create if-then-else logic to determine which step the runbook should transition to next.

Rule #1

{{getInstanceState.instanceState}} == "stopped"

Rule #2

{{getInstanceState.instanceState}} == "stopping"

Rule #3

{{getInstanceState.instanceState}} == "running"

Default - optional

Close

Default step

Default step if none of the choices are true

Go to end

```

- name: branchOnInstanceState
 action: aws:branch
 isEnd: true
 inputs:
 Choices:
 - NextStep: startInstance
 Variable: '{{getInstanceState.instanceState}}'
 StringEquals: stopped
 - NextStep: verifyInstanceStopped
 Variable: '{{getInstanceState.instanceState}}'
 StringEquals: stopping
 - NextStep: patchInstance
 Variable: '{{getInstanceState.instanceState}}'
 StringEquals: running

```

## Tutorial: Creazione di un runbook utilizzando l'esperienza di progettazione visiva

In questo tutorial, imparerai le basi per lavorare con l'esperienza di progettazione visiva fornita da Systems Manager Automation. Nell'esperienza di progettazione visiva, è possibile creare un runbook che utilizza più operazioni. È possibile utilizzare la funzione di spostamento per disporre le azioni sull'area di disegno. È possibile anche cercare, selezionare e configurare queste operazioni. Quindi, è possibile visualizzare il codice YAML generato automaticamente per il flusso di lavoro del runbook, uscire dall'esperienza di progettazione visiva, eseguire il runbook ed esaminare i dettagli di esecuzione.

Questo tutorial mostra anche come aggiornare il runbook e visualizzare la nuova versione. Alla fine del tutorial, eseguirai una fase di pulizia ed eliminerai il runbook.

Dopo aver completato questo tutorial, saprai come usare l'esperienza di progettazione visiva per creare un runbook. Saprai anche come aggiornare, eseguire ed eliminare il runbook.



**Note**

Prima di iniziare questo tutorial, assicurati di completare [Configurazione del servizio di automazione](#).

**Argomenti**

- [Fase 1: Passaggio all'esperienza di progettazione visiva](#)
- [Fase 2: Creazione di un flusso di lavoro](#)
- [Fase 3: Revisione del codice generato automaticamente](#)
- [Fase 4: Esecuzione del nuovo runbook](#)
- [Fase 5: rimozione](#)

**Fase 1: Passaggio all'esperienza di progettazione visiva**

1. Accedi alla [console di Systems Manager Automation](#).
2. Scegli Crea un runbook automazione.

**Fase 2: Creazione di un flusso di lavoro**

Nell'esperienza di progettazione visiva, un flusso di lavoro è una rappresentazione grafica del runbook nell'area di lavoro. È possibile usare l'esperienza di progettazione visiva per definire, configurare ed esaminare le singole operazioni del tuo runbook.

**Creazione di un flusso di lavoro**

1. Accanto agli interruttori Progettazione e Codice, seleziona l'icona a forma di matita e inserisci un nome per il runbook. Per questo tutorial, digita **VisualDesignExperienceTutorial**.

**VisualDesignExperienceTutorial**



Design



Code

2. Nella sezione Attributi del documento del pannello Modulo, espandi il menu a discesa Parametri di input e seleziona Aggiungi un parametro.
  - a. Nel campo Nome del parametro, immetti **InstanceId**.
  - b. Nel menu a discesa Tipo, scegli AWS::EC2::Instance.

- c. Seleziona l'interruttore Richiesto.

**Runbook attributes**

☐ Content >

Attributes 2

Parameters 1

Variables

✕ Close

Parameter name

Enter a unique name.

Instanceld

Type

Specify a data type.

AWS::EC2::Instance::Id ▼

☒ Required

Specify if the parameter is required.

3. Nel browser API AWS , immetti **DescribeInstances** nella barra di ricerca.
4. Sposta un' DescribeInstancesazione di Amazon EC2 nella tela vuota.
5. In Nome fase, immetti un valore. Per questo tutorial, è possibile utilizzare il nome **GetInstanceState**.

The screenshot shows the AWS Systems Manager console. On the left, a search bar contains 'DescribeInstances'. Below it, a list of search results is shown, with 'Amazon EC2 DescribeInstances' highlighted. The main area displays a workflow diagram with a 'Start' node, a 'GetInstanceState' action, and an 'End' node. The right sidebar shows the configuration for the 'GetInstanceState' action, with tabs for 'General', 'Inputs', 'Outputs', and 'Configuration'. The 'General' tab is active, showing the step name 'GetInstanceState', the action type 'aws:executeAwsApi', and a description field.

- Espandi il menu a discesa Input aggiuntivi e, nel campo Nome input, inserisci **InstanceIds**.
  - Scegli la scheda Input.
  - Nel campo Valore di input, scegli l'input del documento **InstanceId**. Fa riferimento al valore del parametro di input creato all'inizio della procedura. Poiché l'InstanceIdsinput per l'DescribeInstancesazione accetta StringList valori, è necessario racchiudere l'InstanceIdsinput tra parentesi quadre. È necessario che il codice YAML per il valore di input corrisponda al seguente: `[ '{{ InstanceId }} ' ]`.
  - Nella scheda Output, seleziona Aggiungi un output e inserisci **InstanceState** nel campo Nome.
  - Nel campo Selettore, inserisci `$.Reservations[0].Instances[0].State.Name`.
  - Dal menu a discesa Tipo, scegli Stringa.
- Sposta un'azione Branch dal browser Azioni nella posizione sotto il **GetInstanceState** passaggio.
  - In Nome fase, immetti un valore. Per questo tutorial, utilizza il nome **BranchOnInstanceState**.

Per definire la logica di ramificazione, completa le operazioni seguenti:

- Scegli lo stato **Branch** nell'area di lavoro. Quindi, in Input e Scelte, seleziona l'icona a forma di matita per modificare la Regola # 1.
- Scegli Aggiungi condizione.
- Nella finestra di dialogo Condizioni per la regola # 1, scegli l'output della fase **GetInstanceState.InstanceState** dal menu a discesa Variabile.

- d. Per Operatore, scegli è uguale a.
- e. Per Valore, scegli Stringa dall'elenco a discesa. Specificare **stopped**.

Conditions for choice #1

Choice rules are conditional statements that the Automation evaluates when determining the next step to process. [Learn more](#)

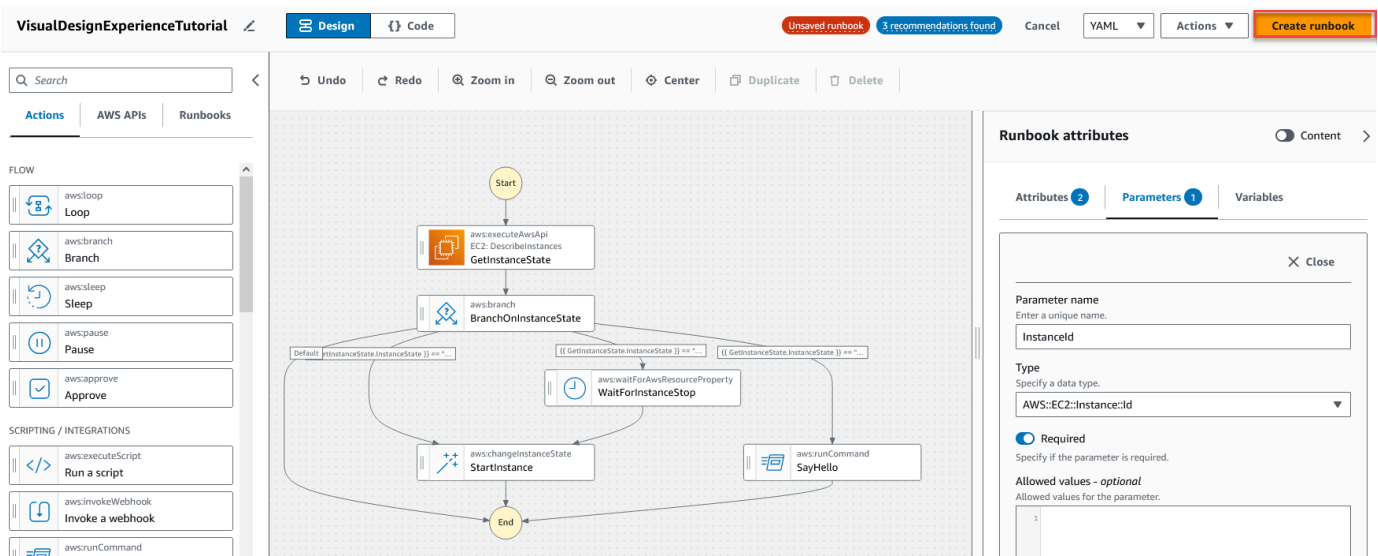
Simple  
Evaluates a single conditional statement.

| Not                      | Variable                             | Operator    | Value             |
|--------------------------|--------------------------------------|-------------|-------------------|
| <input type="checkbox"/> | {{ GetInstanceState.InstanceState }} | is equal to | String<br>stopped |

Cancel Save conditions

- f. Seleziona Salva condizioni.
  - g. Scegli Aggiungi una nuova regola di scelta.
  - h. Scegli Aggiungi condizioni per la Regola # 2.
  - i. Nella finestra di dialogo Condizioni per la regola # 2, scegli l'output della fase **GetInstanceState.InstanceState** dal menu a discesa Variabile.
  - j. Per Operatore, scegli è uguale a.
  - k. Per Valore, scegli Stringa dall'elenco a discesa. Specificare **stopping**.
  - l. Seleziona Salva condizioni.
  - m. Scegli Aggiungi una nuova regola di scelta.
  - n. Scegli Aggiungi condizioni per Regola # 3.
  - o. Nella finestra di dialogo Condizioni per la regola # 3, scegli l'output della fase **GetInstanceState.InstanceState** dal menu a discesa Variabile.
  - p. Per Operatore, scegli è uguale a.
  - q. Per Valore, scegli Stringa dall'elenco a discesa. Specificare **running**.
  - r. Seleziona Salva condizioni.
  - s. In Regola predefinita, scegli Vai alla fine per Fase predefinita.
8. Sposta un'azione Modifica lo stato di un'istanza nella casella vuota Trascina azione qui nella condizione {{ GetInstanceState.InstanceState }} == «fermato».
- a. Per Nome fase, immetti **StartInstance**.
  - b. Nella scheda Input, in Instance IDs, scegli il valore di input del InstanceId documento dal menu a discesa.
  - c. Per Stato desiderato, specificare **running**.

9. Sposta un'azione Attendi una AWS risorsa nella casella vuota Trascina azione qui nella condizione `{{ GetInstanceState.InstanceState }} == «arresto»`.
10. In Nome fase, immetti un valore. Per questo tutorial, utilizza il nome **WaitForInstanceStop**.
  - a. Per il campo Servizio, scegli Amazon EC2.
  - b. Per il campo API, scegli DescribeInstances.
  - c. Per il campo Selettore di proprietà, immetti **`$.Reservations[0].Instances[0].State.Name`**.
  - d. Per il parametro Valori desiderati, immetti **`["stopped"]`**.
  - e. Nella scheda WaitForInstanceStop Configurazione dell'azione, scegli StartInstance dal menu a discesa Passaggio successivo.
11. Sposta l'azione Esegui comando sulle istanze nella casella vuota Trascina azione qui nella condizione `{{ GetInstanceState.InstanceState }} == «in esecuzione»`.
12. Per Nome fase, immetti **SayHello**.
  - a. Nella scheda Input, immetti **AWS-RunShellScript** per il parametro Nome del documento.
  - b. Per InstanceIds, scegli il valore di input del InstanceId documento dal menu a discesa.
  - c. Espandi il menu a discesa Input aggiuntivi e, dal menu a discesa Nome input, scegli Parametri.
  - d. Nel campo Valore di input, immetti **`{"commands": "echo 'Hello World'"}`**.
13. Controlla il runbook completato nell'area di lavoro e seleziona Crea runbook per salvare il runbook del tutorial.



### Fase 3: Revisione del codice generato automaticamente

Quando sposti le azioni dal browser Azioni all'area di disegno, l'esperienza di progettazione visiva compone automaticamente il contenuto YAML o JSON del tuo runbook in tempo reale. È possibile visualizzare e modificare questo codice. Per visualizzare il codice generato automaticamente, seleziona Codice per Progettazione e l'interruttore Codice.

### Fase 4: Esecuzione del nuovo runbook

Dopo aver creato il runbook, è possibile eseguire l'automazione.

#### Esecuzione del nuovo runbook Automation

1. Apri la console all'indirizzo. AWS Systems Manager <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Automazione, quindi Esegui automazione.
3. Nell'elenco Documento di automazione, scegli un runbook. Scegli una o più opzioni nel pannello Categorie di documenti per filtrare i documenti SSM in base al loro scopo. Per visualizzare un runbook di cui si è proprietari, scegliere la scheda Posseduto da me. Per visualizzare un runbook condiviso con l'account, scegliere la scheda Condiviso con me. Per visualizzare tutti i runbook, scegliere la scheda Tutti i documenti.

#### Note

È possibile visualizzare informazioni su un runbook scegliendo il nome del runbook.

4. Nella sezione Dettagli documento verifica che l'opzione Versione documento sia impostata sulla versione che si desidera eseguire. Il sistema include le seguenti opzioni di versione:
  - Versione predefinita al runtime: scegli questa opzione se il runbook Automation viene aggiornato periodicamente e viene assegnata una nuova versione predefinita.
  - Ultima versione al runtime: scegli questa opzione se il runbook Automation viene aggiornato periodicamente e si desidera che venga eseguita la versione aggiornata più di recente.
  - 1 (predefinita): scegli questa opzione per eseguire la prima versione del documento (quella predefinita).
5. Scegli Avanti.
6. Nella pagina Esegui il runbook Automation, scegli Esecuzione semplice.

7. Nella sezione Input parameters (Parametri di input) specifica i parametri obbligatori. Facoltativamente, puoi scegliere un ruolo del servizio IAM dall'AutomationAssumeRoleelenco.
8. (Facoltativo) Scegli un CloudWatch allarme da applicare all'automazione per il monitoraggio. Se l'allarme entra in ALARM stato, l'automazione viene annullata e vengono eseguiti tutti onCancel i passaggi definiti. Se lo usi AWS CloudTrail, vedrai la chiamata StopAutomationExecution API nel tuo percorso. Per ulteriori informazioni, consulta [Configurazione delle automazioni per monitorare gli allarmi CloudWatch](#).
9. Scegli Esegui.

## Fase 5: rimozione

### Eliminazione del runbook

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Documenti.
3. Scegli la scheda Di mia proprietà.
4. Individua il VisualDesignExperienceTutorial runbook.
5. Seleziona il pulsante nella pagina della scheda documento, quindi scegli Elimina documento dal menu a discesa Operazioni.

### Creazione di runbook del servizio di automazione

Ogni runbook in Automation definisce un'automazione. I runbook del servizio di automazione definiscono le operazioni eseguite durante un'automazione. Nel contenuto del runbook, definisci i parametri di input, gli output e le azioni che Systems Manager esegue sulle istanze e sulle risorse gestite. AWS

Questa sezione contiene gli argomenti seguenti.

- [Creazione di parametri di input che popolano AWS risorse](#)
- [Implementazione di architettura VPC e controller di dominio Microsoft Active Directory](#)
- [Ripristino di un volume radice dall'ultimo snapshot](#)
- [Creazione di un'AMI e una copia tra regioni](#)

Il servizio di automazione include numerosi runbook predefiniti che puoi utilizzare per eseguire processi comuni, ad esempio il riavvio di una o più istanze di Amazon Elastic Compute Cloud (Amazon EC2) o la creazione di un'Amazon Machine Image (AMI). Tuttavia, i casi d'uso potrebbero estendersi oltre le funzionalità dei runbook predefiniti. In questo caso, è possibile creare runbook personalizzati e modificarli in base alle proprie esigenze.

Un runbook è costituito da operazioni di automazione, parametri per tali operazioni e parametri di input specificati. Il contenuto di un runbook viene scritto in YAML o JSON. Se non si ha familiarità con YAML o JSON, consigliamo di utilizzare il visual designer o di documentarsi su entrambi i linguaggi di markup prima di tentare di creare un runbook personalizzato. Per ulteriori informazioni sul visual designer, consulta [Esperienza di progettazione visiva per i runbook Automation](#).

Le sezioni seguenti consentono di creare il primo runbook.

### Identificazione del caso d'uso

La prima fase nella creazione di un runbook consiste nell'identificare il caso d'uso. Ad esempio, è stato pianificato il runbook AWS-CreateImage per l'esecuzione quotidiana su tutte le istanze di Amazon EC2 di produzione. Alla fine del mese, si decide di disporre di più immagini di quante sia necessario per i punti di ripristino. Andando avanti, si desidera eliminare automaticamente l'AMI più vecchia di un'istanza di Amazon EC2 quando viene creata una nuova AMI. A tale scopo, è possibile creare un nuovo runbook che esegue le seguenti operazioni:

1. Esegue l'operazione `aws:createImage` e specifica l'ID di istanza nella descrizione dell'immagine.
2. Esegue l'operazione `aws:waitForAwsResourceProperty` per verificare lo stato dell'immagine fino a quando non è `available`.
3. Dopo che lo stato dell'immagine è `available`, l'operazione `aws:executeScript` esegue uno script Python personalizzato che raccoglie gli ID di tutte le immagini associate all'istanza Amazon EC2. Lo script esegue questa operazione filtrando, utilizzando l'ID di istanza nella descrizione dell'immagine specificata al momento della creazione. Quindi, lo script ordina l'elenco degli ID immagine in base dell'elemento `creationDate` dell'immagine e restituisce l'ID dell'AMI più vecchia.
4. Infine, l'operazione `aws:deleteImage` viene eseguita per eliminare l'AMI più vecchia utilizzando l'ID dell'output della fase precedente.

In questo scenario, si stava già utilizzando il runbook AWS-CreateImage, ma si è scoperto che il caso d'uso richiedeva una maggiore flessibilità. Si tratta di una situazione comune perché possono



esserci sovrapposizioni tra runbook e operazioni di automazione. Di conseguenza, potrebbe essere necessario modificare i runbook o le operazioni da utilizzare per risolvere il caso d'uso.

Ad esempio, le operazioni `aws:executeScript` e `aws:invokeLambdaFunction` permettono entrambe di eseguire script personalizzati come parte dell'automazione. Per scegliere tra di loro, potresti preferire `aws:invokeLambdaFunction` a causa dei linguaggi di runtime aggiuntivi supportati. Tuttavia, potresti preferirlo `aws:executeScript` perché ti consente di creare il contenuto degli script direttamente nei runbook YAML e di fornire il contenuto degli script come allegati per i runbook JSON. Si potrebbe anche considerare più semplice `aws:executeScript` in termini di configurazione di AWS Identity and Access Management (IAM). Poiché utilizza le autorizzazioni fornite in `AutomationAssumeRole`, `aws:executeScript` non richiede un ruolo di esecuzione della funzione aggiuntivo. AWS Lambda

In un determinato scenario, un'operazione potrebbe fornire maggiore flessibilità o funzionalità aggiuntive rispetto a un'altra. Pertanto, si consiglia di esaminare i parametri di input disponibili per il runbook o l'operazione che si desidera utilizzare per determinare il caso d'uso e le preferenze più adatte.

## Configurazione dell'ambiente di sviluppo

Dopo aver identificato il caso d'uso e i runbook predefiniti o le operazioni di automazione che si desidera utilizzare nel runbook, è il momento di configurare l'ambiente di sviluppo per il contenuto del runbook. Per sviluppare il contenuto del runbook, consigliamo di utilizzare AWS Toolkit for Visual Studio Code al posto della console Systems Manager Documents.

Toolkit for VS Code è un'estensione open source per Visual Studio Code (VS Code) che offre più funzionalità rispetto alla console Documenti di Systems Manager. Le funzionalità utili includono la convalida dello schema sia per YAML che per JSON, frammenti per i tipi di operazioni di automazione e il supporto di completamento automatico per varie opzioni sia in YAML che JSON.

Per ulteriori informazioni sull'installazione del Toolkit for VS Code, consulta [Installazione di AWS Toolkit for Visual Studio Code](#). Per ulteriori informazioni su come utilizzare Toolkit for VS Code per lo sviluppo di runbook, consulta [Utilizzo dei documenti del servizio di automazione di Systems Manager](#) nella AWS Toolkit for Visual Studio Code Guida per l'utente di .

## Sviluppo di contenuti del runbook

Con l'identificazione del caso d'uso e la configurazione dell'ambiente, è possibile sviluppare il contenuto per il runbook. Il caso d'uso e le preferenze determinano in gran parte le operazioni di automazione o i runbook utilizzati nel contenuto del runbook. Alcune azioni supportano solo un

sottoinsieme di parametri di input rispetto a un'altra azione che consente di eseguire un'attività simile. Altre operazioni hanno output specifici, come `aws:createImage`, dove alcune operazioni consentono di definire i propri output, come `aws:executeAwsApi`.

Se non si ha la certezza di come utilizzare un'operazione particolare nel runbook, si consiglia di esaminare la voce corrispondente per l'operazione in [Riferimento alle operazioni del servizio di automazione di Systems Manager](#). Si consiglia inoltre di esaminare il contenuto dei runbook predefiniti per visualizzare esempi reali di come queste operazioni vengono utilizzate. Per altri esempi di applicazioni reali dei runbook, consulta [Ulteriori esempi di runbook](#).

Per dimostrare le differenze di semplicità e flessibilità offerte dal contenuto del runbook, le esercitazioni seguenti forniscono un esempio di come applicare patch a gruppi di istanze Amazon EC2 per fasi:

- [Esempio 1: Creazione di runbook padre-figlio](#): in questo esempio vengono utilizzati due runbook in una relazione padre-figlio. Il runbook padre avvia un'automazione del controllo della velocità del runbook figlio.
- [Esempio 2: Runbook con script](#): in questo esempio viene illustrato come eseguire gli stessi processi dell'esempio 1 condensando il contenuto in un singolo runbook e utilizzando script nel runbook.

### Esempio 1: Creazione di runbook padre-figlio

L'esempio seguente illustra come creare due runbook in cui vengono applicate le patch a gruppi taggati di istanze Amazon Elastic Compute Cloud (Amazon EC2) in fasi. Questi runbook vengono utilizzati in una relazione padre-figlio con il runbook padre utilizzato per avviare un'automazione del controllo della velocità del runbook figlio. Per ulteriori informazioni sulle automazioni per il controllo della velocità, consulta [Esegui operazioni automatizzate su larga scala](#). Per ulteriori informazioni sulle operazioni di automazione utilizzate in questo esempio, consulta [Riferimento alle operazioni del servizio di automazione di Systems Manager](#).

#### Creazione del runbook figlio

Questo runbook di esempio si occupa dello scenario riportato di seguito. Emily è ingegnere di sistema presso AnyCompany Consultants, LLC. Deve configurare il servizio di patch per gruppi di istanze Amazon Elastic Compute Cloud (Amazon EC2) che ospitano i database primari e secondari. Le applicazioni accedono a questi database 24 ore al giorno, quindi una delle istanze del database deve essere sempre disponibile.

Decide che applicare patch alle istanze per fasi è l'approccio migliore. Il gruppo primario di istanze di database verrà applicato per primo, seguito dal gruppo secondario di istanze di database. Inoltre, per evitare di incorrere in costi aggiuntivi lasciando le istanze in esecuzione precedentemente arrestate, Emily desidera che le istanze con patch vengano restituite allo stato originale, prima che si verifichi l'applicazione delle patch.

Emily identifica i gruppi primari e secondari delle istanze di database in base ai tag associati alle istanze. Decide di creare un runbook padre che avvia un'automazione del controllo della velocità di un runbook figlio. In questo modo, può definire come destinazione i tag associati ai gruppi primari e secondari delle istanze di database e gestire la simultaneità delle automazioni figlio. Dopo aver esaminato i documenti di Systems Manager (SSM) disponibili per l'applicazione di patch, sceglie il documento `AWS-RunPatchBaseline`. Utilizzando questo documento SSM, i colleghi possono esaminare le informazioni di conformità delle patch associate al termine dell'operazione di applicazione delle patch.

Per iniziare a creare il contenuto del runbook, Emily esamina le operazioni di automazione disponibili e inizia a creare il contenuto per il runbook figlio nel modo seguente:

1. Innanzitutto, fornisce i valori per lo schema e la descrizione del runbook e definisce i parametri di input per il runbook figlio.

Utilizzando il parametro `AutomationAssumeRole`, Emily e i suoi colleghi possono utilizzare un ruolo IAM esistente che consente al servizio di automazione di eseguire le operazioni nel runbook per loro conto. Emily utilizza il parametro `InstanceId` per determinare l'istanza a cui deve essere applicata la patch. Facoltativamente, è possibile utilizzare i parametri `Operation`, `RebootOption` e `SnapshotId` per fornire valori per documentare i parametri per `AWS-RunPatchBaseline`. Per evitare che vengano forniti valori non validi a tali parametri del documento, definisce la proprietà `allowedValues` in base alle esigenze.

## YAML

```
schemaVersion: '0.3'
description: 'An example of an Automation runbook that patches groups of Amazon
 EC2 instances in stages.'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
 AutomationAssumeRole:
 type: String
 description: >-
```

```

 '(Optional) The Amazon Resource Name (ARN) of the IAM role that allows
Automation to perform the
 actions on your behalf. If no role is specified, Systems Manager
Automation uses your IAM permissions to operate this runbook.'
 default: ''
InstanceId:
 type: String
 description: >-
 '(Required) The instance you want to patch.'
SnapshotId:
 type: String
 description: '(Optional) The snapshot ID to use to retrieve a patch baseline
snapshot.'
 default: ''
RebootOption:
 type: String
 description: '(Optional) Reboot behavior after a patch Install operation. If
you choose NoReboot and patches are installed, the instance is marked as non-
compliant until a subsequent reboot and scan.'
 allowedValues:
 - NoReboot
 - RebootIfNeeded
 default: RebootIfNeeded
Operation:
 type: String
 description: '(Optional) The update or configuration to perform on the
instance. The system checks if patches specified in the patch baseline are
installed on the instance. The install operation installs patches missing from
the baseline.'
 allowedValues:
 - Install
 - Scan
 default: Install

```

## JSON

```

{
 "schemaVersion":"0.3",
 "description":"An example of an Automation runbook that patches groups of
Amazon EC2 instances in stages.",
 "assumeRole":"{{AutomationAssumeRole}}",
 "parameters":{
 "AutomationAssumeRole":{

```

```

 "type": "String",
 "description": "(Optional) The Amazon Resource Name (ARN) of the IAM role
that allows Automation to perform the actions on your behalf. If no role is
specified, Systems Manager Automation uses your IAM permissions to operate this
runbook.",
 "default": ""
 },
 "InstanceId": {
 "type": "String",
 "description": "(Required) The instance you want to patch."
 },
 "SnapshotId": {
 "type": "String",
 "description": "(Optional) The snapshot ID to use to retrieve a patch
baseline snapshot.",
 "default": ""
 },
 "RebootOption": {
 "type": "String",
 "description": "(Optional) Reboot behavior after a patch Install
operation. If you choose NoReboot and patches are installed, the instance is
marked as non-compliant until a subsequent reboot and scan.",
 "allowedValues": [
 "NoReboot",
 "RebootIfNeeded"
],
 "default": "RebootIfNeeded"
 },
 "Operation": {
 "type": "String",
 "description": "(Optional) The update or configuration to perform on
the instance. The system checks if patches specified in the patch baseline are
installed on the instance. The install operation installs patches missing from
the baseline.",
 "allowedValues": [
 "Install",
 "Scan"
],
 "default": "Install"
 }
}
},

```

2. Con gli elementi di primo livello definiti, Emily procede con la creazione delle operazioni che compongono i `mainSteps` del runbook. La prima fase restituisce lo stato corrente dell'istanza di destinazione specificata nel parametro di input `InstanceId` utilizzando l'operazione `aws:executeAwsApi`. L'output di questa operazione viene utilizzato nelle operazioni successive.

## YAML

```
mainSteps:
 - name: getInstanceState
 action: 'aws:executeAwsApi'
 onFailure: Abort
 inputs:
 inputs:
 Service: ec2
 Api: DescribeInstances
 InstanceIds:
 - '{{InstanceId}}'
 outputs:
 - Name: instanceState
 Selector: '$.Reservations[0].Instances[0].State.Name'
 Type: String
 nextStep: branchOnInstanceState
```

## JSON

```
"mainSteps": [
 {
 "name": "getInstanceState",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "inputs": null,
 "Service": "ec2",
 "Api": "DescribeInstances",
 "InstanceIds": [
 "{{InstanceId}}"
]
 },
 "outputs": [
 {
 "Name": "instanceState",
 "Selector": "$.Reservations[0].Instances[0].State.Name",
 "Type": "String"
 }
]
 }
]
```

```

 }
],
 "nextStep": "branchOnInstanceState"
},

```

3. Anziché avviare manualmente e tenere traccia dello stato originale di ogni istanza a cui è necessario applicare la patch, Emily utilizza l'output dell'operazione precedente per diramare l'automazione in base allo stato dell'istanza di destinazione. Ciò consente all'automazione di eseguire fasi diverse a seconda delle condizioni definite nell'operazione `aws:branch` e migliora l'efficienza complessiva dell'automazione senza intervento manuale.

Se lo stato dell'istanza è già `running`, l'automazione procede con l'applicazione di patch all'istanza con il documento `AWS-RunPatchBaseline` che utilizza l'operazione `aws:runCommand`.

Se lo stato dell'istanza è `stopping`, l'automazione verifica l'istanza per raggiungere lo stato `stopped` utilizzando l'operazione `aws:waitForAwsResourceProperty`, avvia l'istanza utilizzando l'operazione `executeAwsApi` e verifica l'istanza per raggiungere uno stato `running` prima di applicare patch all'istanza.

Se lo stato dell'istanza è `stopped`, l'automazione avvia l'istanza ed esegue una verifica, affinché l'istanza raggiunga lo stato `running` prima di applicare patch all'istanza utilizzando le stesse operazioni.

## YAML

```

- name: branchOnInstanceState
 action: 'aws:branch'
 onFailure: Abort
 inputs:
 Choices:
 - NextStep: startInstance
 Variable: '{{getInstanceState.instanceState}}'
 StringEquals: stopped
 - NextStep: verifyInstanceStopped
 Variable: '{{getInstanceState.instanceState}}'
 StringEquals: stopping
 - NextStep: patchInstance
 Variable: '{{getInstanceState.instanceState}}'
 StringEquals: running
 isEnd: true
- name: startInstance

```

```
 action: 'aws:executeAwsApi'
 onFailure: Abort
 inputs:
 Service: ec2
 Api: StartInstances
 InstanceIds:
 - '{{InstanceId}}'
 nextStep: verifyInstanceRunning
- name: verifyInstanceRunning
 action: 'aws:waitForAwsResourceProperty'
 timeoutSeconds: 120
 inputs:
 Service: ec2
 Api: DescribeInstances
 InstanceIds:
 - '{{InstanceId}}'
 PropertySelector: '$.Reservations[0].Instances[0].State.Name'
 DesiredValues:
 - running
 nextStep: patchInstance
- name: verifyInstanceStopped
 action: 'aws:waitForAwsResourceProperty'
 timeoutSeconds: 120
 inputs:
 Service: ec2
 Api: DescribeInstances
 InstanceIds:
 - '{{InstanceId}}'
 PropertySelector: '$.Reservations[0].Instances[0].State.Name'
 DesiredValues:
 - stopped
 nextStep: startInstance
- name: patchInstance
 action: 'aws:runCommand'
 onFailure: Abort
 timeoutSeconds: 5400
 inputs:
 DocumentName: 'AWS-RunPatchBaseline'
 InstanceIds:
 - '{{InstanceId}}'
 Parameters:
 SnapshotId: '{{SnapshotId}}'
 RebootOption: '{{RebootOption}}'
```



Operation: '{{Operation}}'

## JSON

```
{
 "name": "branchOnInstanceState",
 "action": "aws:branch",
 "onFailure": "Abort",
 "inputs": {
 "Choices": [
 {
 "NextStep": "startInstance",
 "Variable": "{{getInstanceState.instanceState}}",
 "StringEquals": "stopped"
 },
 {
 "Or": [
 {
 "Variable": "{{getInstanceState.instanceState}}",
 "StringEquals": "stopping"
 }
],
 "NextStep": "verifyInstanceStopped"
 },
 {
 "NextStep": "patchInstance",
 "Variable": "{{getInstanceState.instanceState}}",
 "StringEquals": "running"
 }
]
 },
 "isEnd": true
},
{
 "name": "startInstance",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "StartInstances",
 "InstanceIds": [
 "{{InstanceId}}"
]
 }
}
```

```
 },
 "nextStep": "verifyInstanceRunning"
 },
 {
 "name": "verifyInstanceRunning",
 "action": "aws:waitForAwsResourceProperty",
 "timeoutSeconds": 120,
 "inputs": {
 "Service": "ec2",
 "Api": "DescribeInstances",
 "InstanceIds": [
 "{{InstanceId}}"
],
 "PropertySelector": "$.Reservations[0].Instances[0].State.Name",
 "DesiredValues": [
 "running"
]
 },
 "nextStep": "patchInstance"
 },
 {
 "name": "verifyInstanceStopped",
 "action": "aws:waitForAwsResourceProperty",
 "timeoutSeconds": 120,
 "inputs": {
 "Service": "ec2",
 "Api": "DescribeInstances",
 "InstanceIds": [
 "{{InstanceId}}"
],
 "PropertySelector": "$.Reservations[0].Instances[0].State.Name",
 "DesiredValues": [
 "stopped"
],
 "nextStep": "startInstance"
 }
 },
 {
 "name": "patchInstance",
 "action": "aws:runCommand",
 "onFailure": "Abort",
 "timeoutSeconds": 5400,
 "inputs": {
 "DocumentName": "AWS-RunPatchBaseline",
```

```

 "InstanceIds":[
 "{{InstanceId}}"
],
 "Parameters":{
 "SnapshotId":"{{SnapshotId}}",
 "RebootOption":"{{RebootOption}}",
 "Operation":"{{Operation}}"
 }
 }
},

```

4. Al termine dell'operazione di applicazione delle patch, Emily desidera che l'automazione restituisca l'istanza di destinazione allo stesso stato in cui si trovava prima dell'avvio dell'automazione. Lo fa utilizzando nuovamente l'output della prima operazione. L'automazione si ramifica sulla base dello stato originale dell'istanza di destinazione utilizzando l'operazione `aws:branch`. Se l'istanza si trovava in precedenza in uno stato diverso da `running`, l'istanza viene arrestata. Altrimenti, se lo stato dell'istanza è `running`, l'automazione termina.

#### YAML

```

- name: branchOnOriginalInstanceState
 action: 'aws:branch'
 onFailure: Abort
 inputs:
 Choices:
 - NextStep: stopInstance
 Not:
 Variable: '{{getInstanceState.instanceState}}'
 StringEquals: running
 isEnd: true
- name: stopInstance
 action: 'aws:executeAwsApi'
 onFailure: Abort
 inputs:
 Service: ec2
 Api: StopInstances
 InstanceIds:
 - '{{InstanceId}}'

```

#### JSON

```

{
 "name":"branchOnOriginalInstanceState",

```

```

 "action": "aws:branch",
 "onFailure": "Abort",
 "inputs": {
 "Choices": [
 {
 "NextStep": "stopInstance",
 "Not": {
 "Variable": "{{getInstanceState.instanceState}}",
 "StringEquals": "running"
 }
 }
]
 },
 "isEnd": true
 },
 {
 "name": "stopInstance",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "StopInstances",
 "InstanceIds": [
 "{{InstanceId}}"
]
 }
 }
]
}

```

5. Emily esamina il contenuto completo del runbook per bambini e lo crea nella stessa istanza Account AWS e Regione AWS in quella di destinazione. Ora è pronta a continuare con la creazione del contenuto del runbook padre. Di seguito è riportato il contenuto del runbook figlio completato.

#### YAML

```

schemaVersion: '0.3'
description: 'An example of an Automation runbook that patches groups of Amazon
 EC2 instances in stages.'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
 AutomationAssumeRole:
 type: String

```

```

description: >-
 '(Optional) The Amazon Resource Name (ARN) of the IAM role that allows
Automation to perform the
 actions on your behalf. If no role is specified, Systems Manager
 Automation uses your IAM permissions to operate this runbook.'
default: ''
InstanceId:
 type: String
 description: >-
 '(Required) The instance you want to patch.'
SnapshotId:
 type: String
 description: '(Optional) The snapshot ID to use to retrieve a patch baseline
snapshot.'
 default: ''
RebootOption:
 type: String
 description: '(Optional) Reboot behavior after a patch Install operation. If
you choose NoReboot and patches are installed, the instance is marked as non-
compliant until a subsequent reboot and scan.'
 allowedValues:
 - NoReboot
 - RebootIfNeeded
 default: RebootIfNeeded
Operation:
 type: String
 description: '(Optional) The update or configuration to perform on the
instance. The system checks if patches specified in the patch baseline are
installed on the instance. The install operation installs patches missing from
the baseline.'
 allowedValues:
 - Install
 - Scan
 default: Install
mainSteps:
 - name: getInstanceState
 action: 'aws:executeAwsApi'
 onFailure: Abort
 inputs:
 inputs:
 Service: ec2
 Api: DescribeInstances
 InstanceIds:
 - '{{InstanceId}}'

```

```
outputs:
 - Name: instanceState
 Selector: '$.Reservations[0].Instances[0].State.Name'
 Type: String
nextStep: branchOnInstanceState
- name: branchOnInstanceState
 action: 'aws:branch'
 onFailure: Abort
 inputs:
 Choices:
 - NextStep: startInstance
 Variable: '{{getInstanceState.instanceState}}'
 StringEquals: stopped
 - Or:
 - Variable: '{{getInstanceState.instanceState}}'
 StringEquals: stopping
 NextStep: verifyInstanceStopped
 - NextStep: patchInstance
 Variable: '{{getInstanceState.instanceState}}'
 StringEquals: running
 isEnd: true
- name: startInstance
 action: 'aws:executeAwsApi'
 onFailure: Abort
 inputs:
 Service: ec2
 Api: StartInstances
 InstanceIds:
 - '{{InstanceId}}'
 nextStep: verifyInstanceRunning
- name: verifyInstanceRunning
 action: 'aws:waitForAwsResourceProperty'
 timeoutSeconds: 120
 inputs:
 Service: ec2
 Api: DescribeInstances
 InstanceIds:
 - '{{InstanceId}}'
 PropertySelector: '$.Reservations[0].Instances[0].State.Name'
 DesiredValues:
 - running
 nextStep: patchInstance
- name: verifyInstanceStopped
 action: 'aws:waitForAwsResourceProperty'
```

```
timeoutSeconds: 120
inputs:
 Service: ec2
 Api: DescribeInstances
 InstanceIds:
 - '{{InstanceId}}'
 PropertySelector: '$.Reservations[0].Instances[0].State.Name'
 DesiredValues:
 - stopped
 nextStep: startInstance
- name: patchInstance
 action: 'aws:runCommand'
 onFailure: Abort
 timeoutSeconds: 5400
 inputs:
 DocumentName: 'AWS-RunPatchBaseline'
 InstanceIds:
 - '{{InstanceId}}'
 Parameters:
 SnapshotId: '{{SnapshotId}}'
 RebootOption: '{{RebootOption}}'
 Operation: '{{Operation}}'
- name: branchOnOriginalInstanceState
 action: 'aws:branch'
 onFailure: Abort
 inputs:
 Choices:
 - NextStep: stopInstance
 Not:
 Variable: '{{getInstanceState.instanceState}}'
 StringEquals: running
 isEnd: true
- name: stopInstance
 action: 'aws:executeAwsApi'
 onFailure: Abort
 inputs:
 Service: ec2
 Api: StopInstances
 InstanceIds:
 - '{{InstanceId}}'
```

## JSON

```
{
 "schemaVersion": "0.3",
 "description": "An example of an Automation runbook that patches groups of Amazon EC2 instances in stages.",
 "assumeRole": "{{AutomationAssumeRole}}",
 "parameters": {
 "AutomationAssumeRole": {
 "type": "String",
 "description": "'(Optional) The Amazon Resource Name (ARN) of the IAM role that allows Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses your IAM permissions to operate this runbook.'",
 "default": ""
 },
 "InstanceId": {
 "type": "String",
 "description": "'(Required) The instance you want to patch.'"
 },
 "SnapshotId": {
 "type": "String",
 "description": "(Optional) The snapshot ID to use to retrieve a patch baseline snapshot.",
 "default": ""
 },
 "RebootOption": {
 "type": "String",
 "description": "(Optional) Reboot behavior after a patch Install operation. If you choose NoReboot and patches are installed, the instance is marked as non-compliant until a subsequent reboot and scan.",
 "allowedValues": [
 "NoReboot",
 "RebootIfNeeded"
],
 "default": "RebootIfNeeded"
 },
 "Operation": {
 "type": "String",
 "description": "(Optional) The update or configuration to perform on the instance. The system checks if patches specified in the patch baseline are installed on the instance. The install operation installs patches missing from the baseline.",

```



```

 "allowedValues":[
 "Install",
 "Scan"
],
 "default":"Install"
 }
},
"mainSteps":[
 {
 "name":"getInstanceState",
 "action":"aws:executeAwsApi",
 "onFailure":"Abort",
 "inputs":{"
 "inputs":null,
 "Service":"ec2",
 "Api":"DescribeInstances",
 "InstanceIds":[
 "{{InstanceId}}"
]
 },
 "outputs":[
 {
 "Name":"instanceState",
 "Selector":"$.Reservations[0].Instances[0].State.Name",
 "Type":"String"
 }
],
 "nextStep":"branchOnInstanceState"
 },
 {
 "name":"branchOnInstanceState",
 "action":"aws:branch",
 "onFailure":"Abort",
 "inputs":{"
 "Choices":[
 {
 "NextStep":"startInstance",
 "Variable":"{{getInstanceState.instanceState}}",
 "StringEquals":"stopped"
 },
 {
 "Or":[
 {
 "Variable":"{{getInstanceState.instanceState}}",

```

```

 "StringEquals":"stopping"
 }
],
 "NextStep":"verifyInstanceStopped"
 },
 {
 "NextStep":"patchInstance",
 "Variable":"{{getInstanceState.instanceState}}",
 "StringEquals":"running"
 }
]
},
"isEnd":true
},
{
 "name":"startInstance",
 "action":"aws:executeAwsApi",
 "onFailure":"Abort",
 "inputs":{
 "Service":"ec2",
 "Api":"StartInstances",
 "InstanceIds":[
 "{{InstanceId}}"
]
 },
 "nextStep":"verifyInstanceRunning"
},
{
 "name":"verifyInstanceRunning",
 "action":"aws:waitForAwsResourceProperty",
 "timeoutSeconds":120,
 "inputs":{
 "Service":"ec2",
 "Api":"DescribeInstances",
 "InstanceIds":[
 "{{InstanceId}}"
],
 "PropertySelector":"$.Reservations[0].Instances[0].State.Name",
 "DesiredValues":[
 "running"
]
 },
 "nextStep":"patchInstance"
},

```

```

{
 "name": "verifyInstanceStopped",
 "action": "aws:waitForAwsResourceProperty",
 "timeoutSeconds": 120,
 "inputs": {
 "Service": "ec2",
 "Api": "DescribeInstances",
 "InstanceIds": [
 "{{InstanceId}}"
],
 "PropertySelector": "$.Reservations[0].Instances[0].State.Name",
 "DesiredValues": [
 "stopped"
],
 "nextStep": "startInstance"
 }
},
{
 "name": "patchInstance",
 "action": "aws:runCommand",
 "onFailure": "Abort",
 "timeoutSeconds": 5400,
 "inputs": {
 "DocumentName": "AWS-RunPatchBaseline",
 "InstanceIds": [
 "{{InstanceId}}"
],
 "Parameters": {
 "SnapshotId": "{{SnapshotId}}",
 "RebootOption": "{{RebootOption}}",
 "Operation": "{{Operation}}"
 }
 }
},
{
 "name": "branchOnOriginalInstanceState",
 "action": "aws:branch",
 "onFailure": "Abort",
 "inputs": {
 "Choices": [
 {
 "NextStep": "stopInstance",
 "Not": {
 "Variable": "{{getInstanceState.instanceState}}",

```

```

 "StringEquals": "running"
 }
}
],
},
"isEnd": true
},
{
 "name": "stopInstance",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "StopInstances",
 "InstanceIds": [
 "{{InstanceId}}"
]
 }
}
]
}

```

Per ulteriori informazioni sulle operazioni di automazione utilizzate in questo esempio, consulta [Riferimento alle operazioni del servizio di automazione di Systems Manager](#).

## Creazione del runbook padre

Questo runbook di esempio continua lo scenario descritto nella sezione precedente. Ora che Emily ha creato il runbook figlio, inizia a creare il contenuto per il runbook padre nel modo seguente:

1. Innanzitutto, fornisce i valori per lo schema e la descrizione del runbook e definisce i parametri di input per il runbook padre.

Utilizzando il parametro `AutomationAssumeRole`, Emily e i suoi colleghi possono utilizzare un ruolo IAM esistente che consente al servizio di automazione di eseguire le operazioni nel runbook per loro conto. Emily utilizza i parametri `PatchGroupPrimaryKey` e `PatchGroupPrimaryValue` per specificare il tag associato al gruppo primario di istanze di database a cui verrà applicata la patch. Lei usa i parametri `PatchGroupSecondaryKey` e `PatchGroupSecondaryValue` per specificare il tag associato al gruppo secondario di istanze di database a cui verrà applicata la patch.

## YAML

```
description: 'An example of an Automation runbook that patches groups of Amazon
 EC2 instances in stages.'
schemaVersion: '0.3'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
 AutomationAssumeRole:
 type: String
 description: '(Optional) The Amazon Resource Name (ARN) of the IAM role that
 allows Automation to perform the actions on your behalf. If no role is specified,
 Systems Manager Automation uses your IAM permissions to operate this runbook.'
 default: ''
 PatchGroupPrimaryKey:
 type: String
 description: '(Required) The key of the tag for the primary group of instances
 you want to patch.'
 PatchGroupPrimaryValue:
 type: String
 description: '(Required) The value of the tag for the primary group of
 instances you want to patch.'
 PatchGroupSecondaryKey:
 type: String
 description: '(Required) The key of the tag for the secondary group of
 instances you want to patch.'
 PatchGroupSecondaryValue:
 type: String
 description: '(Required) The value of the tag for the secondary group of
 instances you want to patch.'
```

## JSON

```
{
 "schemaVersion": "0.3",
 "description": "An example of an Automation runbook that patches groups of
Amazon EC2 instances in stages.",
 "assumeRole": "{{AutomationAssumeRole}}",
 "parameters": {
 "AutomationAssumeRole": {
 "type": "String",
 "description": "(Optional) The Amazon Resource Name (ARN) of the IAM
role that allows Automation to perform the actions on your behalf. If no role is
```

```
specified, Systems Manager Automation uses your IAM permissions to operate this
runbook.",
 "default": ""
 },
 "PatchGroupPrimaryKey": {
 "type": "String",
 "description": "(Required) The key of the tag for the primary group of
instances you want to patch."
 },
 "PatchGroupPrimaryValue": {
 "type": "String",
 "description": "(Required) The value of the tag for the primary group of
instances you want to patch."
 },
 "PatchGroupSecondaryKey": {
 "type": "String",
 "description": "(Required) The key of the tag for the secondary group of
instances you want to patch."
 },
 "PatchGroupSecondaryValue": {
 "type": "String",
 "description": "(Required) The value of the tag for the secondary group
of instances you want to patch."
 }
}
},
```

2. Con gli elementi di primo livello definiti, Emily procede con la creazione delle operazioni che compongono i `mainSteps` del runbook.

La prima operazione avvia un'automazione del controllo della velocità utilizzando il runbook figlio appena creato e destinato alle istanze associate al tag specificato nei parametri di input `PatchGroupPrimaryKey` e `PatchGroupPrimaryValue`. Utilizza i valori forniti ai parametri di input per specificare la chiave e il valore del tag associato al gruppo primario di istanze di database a cui desidera applicare patch.

Una volta completata la prima automazione, la seconda operazione avvia un'altra automazione del controllo della velocità utilizzando il runbook figlio che si rivolge alle istanze associate al tag specificato nei parametri di input `PatchGroupSecondaryKey` e `PatchGroupSecondaryValue`. Utilizza i valori forniti ai parametri di input per specificare la chiave e il valore del tag associato al gruppo secondario di istanze di database a cui desidera applicare patch.

## YAML

```
mainSteps:
- name: patchPrimaryTargets
 action: 'aws:executeAutomation'
 onFailure: Abort
 timeoutSeconds: 7200
 inputs:
 DocumentName: RunbookTutorialChildAutomation
 Targets:
 - Key: 'tag:{{PatchGroupPrimaryKey}}'
 Values:
 - '{{PatchGroupPrimaryValue}}'
 TargetParameterName: 'InstanceId'
- name: patchSecondaryTargets
 action: 'aws:executeAutomation'
 onFailure: Abort
 timeoutSeconds: 7200
 inputs:
 DocumentName: RunbookTutorialChildAutomation
 Targets:
 - Key: 'tag:{{PatchGroupSecondaryKey}}'
 Values:
 - '{{PatchGroupSecondaryValue}}'
 TargetParameterName: 'InstanceId'
```

## JSON

```
"mainSteps": [
 {
 "name": "patchPrimaryTargets",
 "action": "aws:executeAutomation",
 "onFailure": "Abort",
 "timeoutSeconds": 7200,
 "inputs": {
 "DocumentName": "RunbookTutorialChildAutomation",
 "Targets": [
 {
 "Key": "tag:{{PatchGroupPrimaryKey}}",
 "Values": [
 "{{PatchGroupPrimaryValue}}"
]
 }
]
 }
 }
]
```

```

],
 "TargetParameterName": "InstanceId"
 }
 },
 {
 "name": "patchSecondaryTargets",
 "action": "aws:executeAutomation",
 "onFailure": "Abort",
 "timeoutSeconds": 7200,
 "inputs": {
 "DocumentName": "RunbookTutorialChildAutomation",
 "Targets": [
 {
 "Key": "tag:{{PatchGroupSecondaryKey}}",
 "Values": [
 "{{PatchGroupSecondaryValue}}"
]
 }
],
 "TargetParameterName": "InstanceId"
 }
 }
]
}

```

- Emily esamina il contenuto completo del runbook principale e crea il runbook nella stessa istanza e in quella di destinazione. Account AWS Regione AWS Ora, è pronta a testare i suoi runbook per assicurarsi che l'automazione funzioni come desiderato prima di implementarli nell'ambiente di produzione. Di seguito è riportato il contenuto del runbook padre completato.

#### YAML

```

description: An example of an Automation runbook that patches groups of Amazon EC2
 instances in stages.
schemaVersion: '0.3'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
 AutomationAssumeRole:
 type: String
 description: '(Optional) The Amazon Resource Name (ARN) of the IAM role that
 allows Automation to perform the actions on your behalf. If no role is specified,
 Systems Manager Automation uses your IAM permissions to operate this runbook.'
 default: ''
 PatchGroupPrimaryKey:

```



```

 type: String
 description: (Required) The key of the tag for the primary group of instances
you want to patch.
 PatchGroupPrimaryValue:
 type: String
 description: '(Required) The value of the tag for the primary group of
instances you want to patch. '
 PatchGroupSecondaryKey:
 type: String
 description: (Required) The key of the tag for the secondary group of
instances you want to patch.
 PatchGroupSecondaryValue:
 type: String
 description: '(Required) The value of the tag for the secondary group of
instances you want to patch. '
 mainSteps:
 - name: patchPrimaryTargets
 action: 'aws:executeAutomation'
 onFailure: Abort
 timeoutSeconds: 7200
 inputs:
 DocumentName: RunbookTutorialChildAutomation
 Targets:
 - Key: 'tag:{{PatchGroupPrimaryKey}}'
 Values:
 - '{{PatchGroupPrimaryValue}}'
 TargetParameterName: 'InstanceId'
 - name: patchSecondaryTargets
 action: 'aws:executeAutomation'
 onFailure: Abort
 timeoutSeconds: 7200
 inputs:
 DocumentName: RunbookTutorialChildAutomation
 Targets:
 - Key: 'tag:{{PatchGroupSecondaryKey}}'
 Values:
 - '{{PatchGroupSecondaryValue}}'
 TargetParameterName: 'InstanceId'

```

## JSON

```
{
```

```

"description":"An example of an Automation runbook that patches groups of
Amazon EC2 instances in stages.",
"schemaVersion":"0.3",
"assumeRole":"{{AutomationAssumeRole}}",
"parameters":{
 "AutomationAssumeRole":{
 "type":"String",
 "description":"(Optional) The Amazon Resource Name (ARN) of the IAM role
that allows Automation to perform the actions on your behalf. If no role is
specified, Systems Manager Automation uses your IAM permissions to operate this
runbook.",
 "default":""
 },
 "PatchGroupPrimaryKey":{
 "type":"String",
 "description":"(Required) The key of the tag for the primary group of
instances you want to patch."
 },
 "PatchGroupPrimaryValue":{
 "type":"String",
 "description":"(Required) The value of the tag for the primary group of
instances you want to patch. "
 },
 "PatchGroupSecondaryKey":{
 "type":"String",
 "description":"(Required) The key of the tag for the secondary group of
instances you want to patch."
 },
 "PatchGroupSecondaryValue":{
 "type":"String",
 "description":"(Required) The value of the tag for the secondary group of
instances you want to patch. "
 }
},
"mainSteps":[
 {
 "name":"patchPrimaryTargets",
 "action":"aws:executeAutomation",
 "onFailure":"Abort",
 "timeoutSeconds":7200,
 "inputs":{
 "DocumentName":"RunbookTutorialChildAutomation",
 "Targets":[
 {

```

```

 "Key": "tag:{{PatchGroupPrimaryKey}}",
 "Values": [
 "{{PatchGroupPrimaryValue}}"
]
 },
 "TargetParameterName": "InstanceId"
},
{
 "name": "patchSecondaryTargets",
 "action": "aws:executeAutomation",
 "onFailure": "Abort",
 "timeoutSeconds": 7200,
 "inputs": {
 "DocumentName": "RunbookTutorialChildAutomation",
 "Targets": [
 {
 "Key": "tag:{{PatchGroupSecondaryKey}}",
 "Values": [
 "{{PatchGroupSecondaryValue}}"
]
 }
],
 "TargetParameterName": "InstanceId"
 }
}
]
}

```

Per ulteriori informazioni sulle operazioni di automazione utilizzate in questo esempio, consulta [Riferimento alle operazioni del servizio di automazione di Systems Manager](#).

## Esempio 2: Runbook con script

Questo runbook di esempio si occupa dello scenario riportato di seguito. Emily è ingegnere di sistema presso AnyCompany Consultants, LLC. In precedenza, ha creato due runbook utilizzati in una relazione padre-figlio a gruppi di patch di istanze Amazon Elastic Compute Cloud (Amazon EC2) che ospitano i database primari e secondari. Le applicazioni accedono a questi database 24 ore al giorno, quindi una delle istanze del database deve essere sempre disponibile.

Sulla base di questo requisito, ha creato una soluzione per l'applicazione di patch alle istanze in fasi utilizzando il documento `AWS-RunPatchBaseline` di Systems Manager (SSM). Utilizzando questo documento SSM, i colleghi possono esaminare le informazioni di conformità delle patch associate al termine dell'operazione di applicazione delle patch.

Il gruppo primario di istanze di database viene applicato per primo, seguito dal gruppo secondario di istanze di database. Inoltre, per evitare di incorrere in costi aggiuntivi lasciando le istanze in esecuzione precedentemente arrestate, Emily si è assicurata che l'automazione restituisse le istanze con patch allo stato originale prima che si verificasse l'applicazione delle patch. Emily ha utilizzato tag associati ai gruppi primari e secondari di istanze di database per identificare quali istanze devono essere applicate le patch nell'ordine desiderato.

La sua soluzione automatizzata esistente funziona, ma vuole migliorare la sua soluzione, se possibile. Per facilitare la manutenzione del contenuto del runbook e facilitare la risoluzione dei problemi, desidera condensare l'automazione in un unico runbook e semplificare il numero di parametri di input. Inoltre, vorrebbe evitare di creare più automazioni figlio.

Dopo aver esaminato le operazioni di automazione disponibili, Emily determina di poter migliorare la sua soluzione utilizzando l'operazione `aws:executeScript` per eseguire i suoi script Python personalizzati. Ora inizia a creare il contenuto per il runbook nel modo seguente:

1. Innanzitutto, fornisce i valori per lo schema e la descrizione del runbook e definisce i parametri di input per il runbook padre.

Utilizzando il parametro `AutomationAssumeRole`, Emily e i suoi colleghi possono utilizzare un ruolo IAM esistente che consente al servizio di automazione di eseguire le operazioni nel runbook per loro conto. A differenza dell'[Esempio 1](#), il parametro `AutomationAssumeRole` è ora richiesto e non è facoltativo. Poiché questo runbook include `aws:executeScript` azioni, è sempre necessario un ruolo di servizio AWS Identity and Access Management (IAM) (o assumi un ruolo). Questo requisito è necessario, perché alcuni degli script Python specificati per le operazioni chiamano operazioni API di AWS .

Emily utilizza i parametri `PrimaryPatchGroupTag` e `SecondaryPatchGroupTag` per specificare i tag associati al gruppo primario e secondario di istanze del database a cui verrà applicata la patch. Per semplificare i parametri di input richiesti, decide di utilizzare i parametri `StringMap` anziché utilizzare più parametri `String` come nel caso del runbook dell'esempio 1. Facoltativamente, è possibile utilizzare i parametri `Operation`, `RebootOption` e `SnapshotId` per fornire valori per documentare i parametri per `AWS-RunPatchBaseline`. Per evitare

che vengano forniti valori non validi a tali parametri del documento, definisce la proprietà `allowedValues` in base alle esigenze.

## YAML

```
description: 'An example of an Automation runbook that patches groups of Amazon
 EC2 instances in stages.'
schemaVersion: '0.3'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
 AutomationAssumeRole:
 type: String
 description: '(Required) The Amazon Resource Name (ARN) of the IAM role that
 allows Automation to perform the actions on your behalf. If no role is specified,
 Systems Manager Automation uses your IAM permissions to operate this runbook.'
 PrimaryPatchGroupTag:
 type: StringMap
 description: '(Required) The tag for the primary group of instances you want
 to patch. Specify a key-value pair. Example: {"key" : "value"}'
 SecondaryPatchGroupTag:
 type: StringMap
 description: '(Required) The tag for the secondary group of instances you want
 to patch. Specify a key-value pair. Example: {"key" : "value"}'
 SnapshotId:
 type: String
 description: '(Optional) The snapshot ID to use to retrieve a patch baseline
 snapshot.'
 default: ''
 RebootOption:
 type: String
 description: '(Optional) Reboot behavior after a patch Install operation. If
 you choose NoReboot and patches are installed, the instance is marked as non-
 compliant until a subsequent reboot and scan.'
 allowedValues:
 - NoReboot
 - RebootIfNeeded
 default: RebootIfNeeded
 Operation:
 type: String
 description: '(Optional) The update or configuration to perform on the
 instance. The system checks if patches specified in the patch baseline are
 installed on the instance. The install operation installs patches missing from
 the baseline.'
 allowedValues:
```

```
- Install
- Scan
default: Install
```

## JSON

```
{
 "description": "An example of an Automation runbook that patches groups of
Amazon EC2 instances in stages.",
 "schemaVersion": "0.3",
 "assumeRole": "{{AutomationAssumeRole}}",
 "parameters": {
 "AutomationAssumeRole": {
 "type": "String",
 "description": "(Required) The Amazon Resource Name (ARN) of the IAM role
that allows Automation to perform the actions on your behalf. If no role is
specified, Systems Manager Automation uses your IAM permissions to operate this
runbook."
 },
 "PrimaryPatchGroupTag": {
 "type": "StringMap",
 "description": "(Required) The tag for the primary group of instances you
want to patch. Specify a key-value pair. Example: {\"key\" : \"value\"}"
 },
 "SecondaryPatchGroupTag": {
 "type": "StringMap",
 "description": "(Required) The tag for the secondary group of instances
you want to patch. Specify a key-value pair. Example: {\"key\" : \"value\"}"
 },
 "SnapshotId": {
 "type": "String",
 "description": "(Optional) The snapshot ID to use to retrieve a patch
baseline snapshot.",
 "default": ""
 },
 "RebootOption": {
 "type": "String",
 "description": "(Optional) Reboot behavior after a patch Install
operation. If you choose NoReboot and patches are installed, the instance is
marked as non-compliant until a subsequent reboot and scan.",
 "allowedValues": [
 "NoReboot",
 "RebootIfNeeded"
]
 }
 }
}
```

```

],
 "default": "RebootIfNeeded"
 },
 "Operation": {
 "type": "String",
 "description": "(Optional) The update or configuration to perform on the instance. The system checks if patches specified in the patch baseline are installed on the instance. The install operation installs patches missing from the baseline.",
 "allowedValues": [
 "Install",
 "Scan"
],
 "default": "Install"
 }
}
},

```

2. Con gli elementi di primo livello definiti, Emily procede con la creazione delle operazioni che compongono i `mainSteps` del runbook. La prima fase raccoglie gli ID di tutte le istanze associate al tag specificato nel parametro `PrimaryPatchGroupTag` e restituisce un parametro `StringMap` contenente l'ID di istanza e lo stato corrente dell'istanza. L'output di questa operazione viene utilizzato nelle operazioni successive.

Il parametro di input dello script non è supportato per i runbook JSON. I runbook JSON devono fornire contenuto di script utilizzando il `attachment` parametro di input allegato.

## YAML

```

mainSteps:
 - name: getPrimaryInstanceState
 action: 'aws:executeScript'
 timeoutSeconds: 120
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: getInstanceStates
 InputPayload:
 primaryTag: '{{PrimaryPatchGroupTag}}'
 Script: |-
 def getInstanceStates(events, context):
 import boto3

```

```

#Initialize client
ec2 = boto3.client('ec2')
tag = events['primaryTag']
tagKey, tagValue = list(tag.items())[0]
instanceQuery = ec2.describe_instances(
 Filters=[
 {
 "Name": "tag:" + tagKey,
 "Values": [tagValue]
 }
]
)
if not instanceQuery['Reservations']:
 noInstancesForTagString = "No instances found for specified tag."
 return({ 'noInstancesFound' : noInstancesForTagString })
else:
 queryResponse = instanceQuery['Reservations']
 originalInstanceStates = {}
 for results in queryResponse:
 instanceSet = results['Instances']
 for instance in instanceSet:
 instanceId = instance['InstanceId']
 originalInstanceStates[instanceId] = instance['State']

['Name']

 return originalInstanceStates

outputs:
 - Name: originalInstanceStates
 Selector: $.Payload
 Type: StringMap
 nextStep: verifyPrimaryInstancesRunning

```

## JSON

```

"mainSteps":[
 {
 "name":"getPrimaryInstanceState",
 "action":"aws:executeScript",
 "timeoutSeconds":120,
 "onFailure":"Abort",
 "inputs":{
 "Runtime":"python3.11",
 "Handler":"getInstanceStates",
 "InputPayload":{
 "primaryTag":"{{PrimaryPatchGroupTag}}"
 }
 }
 }
]

```



```

 },
 "Script": "...",
 },
 "outputs": [
 {
 "Name": "originalInstanceStates",
 "Selector": "$.Payload",
 "Type": "StringMap"
 }
],
 "nextStep": "verifyPrimaryInstancesRunning"
},

```

- Emily utilizza l'output dell'operazione precedente in un'altra operazione `aws:executeScript` per verificare che tutte le istanze associate al tag specificato nel parametro `PrimaryPatchGroupTag` siano nello stato `running`.

Se lo stato dell'istanza è già `running` o `shutting-down`, lo script continua a scorrere le istanze rimanenti.

Se lo stato dell'istanza è `stopping`, lo script esegue la verifica per l'istanza perché raggiunga lo stato `stopped` e avvia l'istanza.

Se lo stato dell'istanza è `stopped`, lo script avvia l'istanza.

## YAML

```

- name: verifyPrimaryInstancesRunning
 action: 'aws:executeScript'
 timeoutSeconds: 600
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: verifyInstancesRunning
 InputPayload:
 targetInstances: '{{getPrimaryInstanceState.originalInstanceStates}}'
 Script: |-
 def verifyInstancesRunning(events, context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 instanceDict = events['targetInstances']

```

```

 for instance in instanceDict:
 if instanceDict[instance] == 'stopped':
 print("The target instance " + instance + " is stopped. The
instance will now be started.")
 ec2.start_instances(
 InstanceIds=[instance]
)
 elif instanceDict[instance] == 'stopping':
 print("The target instance " + instance + " is stopping. Polling
for instance to reach stopped state.")
 while instanceDict[instance] != 'stopped':
 poll = ec2.get_waiter('instance_stopped')
 poll.wait(
 InstanceIds=[instance]
)
 ec2.start_instances(
 InstanceIds=[instance]
)
 else:
 pass
 nextStep: waitForPrimaryRunningInstances

```

## JSON

```

{
 "name": "verifyPrimaryInstancesRunning",
 "action": "aws:executeScript",
 "timeoutSeconds": 600,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "verifyInstancesRunning",
 "InputPayload": {

 "targetInstances": "{{getPrimaryInstanceState.originalInstanceStates}}"
 },
 "Script": "...",
 },
 "nextStep": "waitForPrimaryRunningInstances"
},

```

- Emily verifica che tutte le istanze associate al tag specificato nel parametro `PrimaryPatchGroupTag` siano stati avviati o già in uno stato running. Quindi utilizza un altro

script per verificare che tutte le istanze, incluse quelle avviate nell'operazione precedente, abbiano raggiunto lo stato `running`.

## YAML

```
- name: waitForPrimaryRunningInstances
 action: 'aws:executeScript'
 timeoutSeconds: 300
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: waitForRunningInstances
 InputPayload:
 targetInstances: '{{getPrimaryInstanceState.originalInstanceStates}}'
 Script: |-
 def waitForRunningInstances(events, context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 instanceDict = events['targetInstances']
 for instance in instanceDict:
 poll = ec2.get_waiter('instance_running')
 poll.wait(
 InstanceIds=[instance]
)
 nextStep: returnPrimaryTagKey
```

## JSON

```
{
 "name": "waitForPrimaryRunningInstances",
 "action": "aws:executeScript",
 "timeoutSeconds": 300,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "waitForRunningInstances",
 "InputPayload": {
 "targetInstances": "{{getPrimaryInstanceState.originalInstanceStates}}",
 },
 "Script": "..."
 }
```

```
 },
 "nextStep": "returnPrimaryTagKey"
 },
}
```

5. Emily usa altri due script per restituire valori singoli della chiave `String` e del valore del tag specificato nel parametro `PrimaryPatchGroupTag`. I valori restituiti da queste operazioni le permettono di fornire i valori direttamente al parametro `Targets` per il documento `AWS-RunPatchBaseline`. L'automazione procede quindi con l'applicazione di patch all'istanza con il documento `AWS-RunPatchBaseline` tramite l'operazione `aws:runCommand`.

## YAML

```
- name: returnPrimaryTagKey
 action: 'aws:executeScript'
 timeoutSeconds: 120
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: returnTagValues
 InputPayload:
 primaryTag: '{{PrimaryPatchGroupTag}}'
 Script: |-
 def returnTagValues(events,context):
 tag = events['primaryTag']
 tagKey = list(tag)[0]
 stringKey = "tag:" + tagKey
 return {'tagKey' : stringKey}
 outputs:
 - Name: Payload
 Selector: $.Payload
 Type: StringMap
 - Name: primaryPatchGroupKey
 Selector: $.Payload.tagKey
 Type: String
 nextStep: returnPrimaryTagValue
- name: returnPrimaryTagValue
 action: 'aws:executeScript'
 timeoutSeconds: 120
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: returnTagValues
 InputPayload:
```

```

 primaryTag: '{{PrimaryPatchGroupTag}}'
Script: |-
 def returnTagValues(events,context):
 tag = events['primaryTag']
 tagKey = list(tag)[0]
 tagValue = tag[tagKey]
 return {'tagValue' : tagValue}
outputs:
 - Name: Payload
 Selector: $.Payload
 Type: StringMap
 - Name: primaryPatchGroupValue
 Selector: $.Payload.tagValue
 Type: String
nextStep: patchPrimaryInstances
- name: patchPrimaryInstances
 action: 'aws:runCommand'
 onFailure: Abort
 timeoutSeconds: 7200
 inputs:
 DocumentName: AWS-RunPatchBaseline
 Parameters:
 SnapshotId: '{{SnapshotId}}'
 RebootOption: '{{RebootOption}}'
 Operation: '{{Operation}}'
 Targets:
 - Key: '{{returnPrimaryTagKey.primaryPatchGroupKey}}'
 Values:
 - '{{returnPrimaryTagValue.primaryPatchGroupValue}}'
 MaxConcurrency: 10%
 MaxErrors: 10%
 nextStep: returnPrimaryToOriginalState

```

## JSON

```

{
 "name": "returnPrimaryTagKey",
 "action": "aws:executeScript",
 "timeoutSeconds": 120,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "returnTagValues",

```

```

 "InputPayload":{
 "primaryTag":"{{PrimaryPatchGroupTag}}"
 },
 "Script":"..."
 },
 "outputs":[
 {
 "Name":"Payload",
 "Selector":"$.Payload",
 "Type":"StringMap"
 },
 {
 "Name":"primaryPatchGroupKey",
 "Selector":"$.Payload.tagKey",
 "Type":"String"
 }
],
 "nextStep":"returnPrimaryTagValue"
},
{
 "name":"returnPrimaryTagValue",
 "action":"aws:executeScript",
 "timeoutSeconds":120,
 "onFailure":"Abort",
 "inputs":{
 "Runtime":"python3.11",
 "Handler":"returnTagValues",
 "InputPayload":{
 "primaryTag":"{{PrimaryPatchGroupTag}}"
 },
 "Script":"..."
 },
 "outputs":[
 {
 "Name":"Payload",
 "Selector":"$.Payload",
 "Type":"StringMap"
 },
 {
 "Name":"primaryPatchGroupValue",
 "Selector":"$.Payload.tagValue",
 "Type":"String"
 }
]
},

```

```

 "nextStep": "patchPrimaryInstances"
 },
 {
 "name": "patchPrimaryInstances",
 "action": "aws:runCommand",
 "onFailure": "Abort",
 "timeoutSeconds": 7200,
 "inputs": {
 "DocumentName": "AWS-RunPatchBaseline",
 "Parameters": {
 "SnapshotId": "${SnapshotId}",
 "RebootOption": "${RebootOption}",
 "Operation": "${Operation}"
 }
 },
 "Targets": [
 {
 "Key": "${returnPrimaryTagKey.primaryPatchGroupKey}",
 "Values": [
 "${returnPrimaryTagValue.primaryPatchGroupValue}"
]
 }
],
 "MaxConcurrency": "10%",
 "MaxErrors": "10%"
 },
 {
 "nextStep": "returnPrimaryToOriginalState"
 }
],

```

6. Al termine dell'operazione di applicazione delle patch, Emily desidera che l'automazione restituisca le istanze di destinazione associate al tag specificato nel parametro `PrimaryPatchGroupTag` allo stesso stato in cui si trovavano prima dell'avvio dell'automazione. Lo fa utilizzando nuovamente l'output della prima operazione in uno script. In base allo stato originale dell'istanza di destinazione, se l'istanza si trovava in precedenza in uno stato diverso da `running`, l'istanza viene arrestata. Altrimenti, se lo stato dell'istanza è `running`, lo script continua a scorrere le istanze rimanenti.

## YAML

```

- name: returnPrimaryToOriginalState
 action: 'aws:executeScript'
 timeoutSeconds: 600
 onFailure: Abort
 inputs:

```

```

Runtime: python3.11
Handler: returnToOriginalState
InputPayload:
 targetInstances: '{{getPrimaryInstanceState.originalInstanceStates}}'
Script: |-
 def returnToOriginalState(events,context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 instanceDict = events['targetInstances']
 for instance in instanceDict:
 if instanceDict[instance] == 'stopped' or instanceDict[instance] ==
'stopping':
 ec2.stop_instances(
 InstanceIds=[instance]
)
 else:
 pass
 nextStep: getSecondaryInstanceState

```

## JSON

```

{
 "name": "returnPrimaryToOriginalState",
 "action": "aws:executeScript",
 "timeoutSeconds": 600,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "returnToOriginalState",
 "InputPayload": {

 "targetInstances": "{{getPrimaryInstanceState.originalInstanceStates}}"
 },
 "Script": "...",
 },
 "nextStep": "getSecondaryInstanceState"
},

```

7. L'operazione di applicazione delle patch viene completata per le istanze associate al tag specificato nel parametro `PrimaryPatchGroupTag`. Ora Emily duplica tutte le operazioni



precedenti nel contenuto del runbook per definire come destinazione le istanze associate al tag specificato nel parametro `SecondaryPatchGroupTag`.

## YAML

```
- name: getSecondaryInstanceState
 action: 'aws:executeScript'
 timeoutSeconds: 120
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: getInstanceStates
 InputPayload:
 secondaryTag: '{{SecondaryPatchGroupTag}}'
 Script: |-
 def getInstanceStates(events,context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 tag = events['secondaryTag']
 tagKey, tagValue = list(tag.items())[0]
 instanceQuery = ec2.describe_instances(
 Filters=[
 {
 "Name": "tag:" + tagKey,
 "Values": [tagValue]
 }
]
)
 if not instanceQuery['Reservations']:
 noInstancesForTagString = "No instances found for specified tag."
 return({ 'noInstancesFound' : noInstancesForTagString })
 else:
 queryResponse = instanceQuery['Reservations']
 originalInstanceStates = {}
 for results in queryResponse:
 instanceSet = results['Instances']
 for instance in instanceSet:
 instanceId = instance['InstanceId']
 originalInstanceStates[instanceId] = instance['State']

 return originalInstanceStates

 outputs:
 - Name: originalInstanceStates
```

```

 Selector: $.Payload
 Type: StringMap
 nextStep: verifySecondaryInstancesRunning
- name: verifySecondaryInstancesRunning
 action: 'aws:executeScript'
 timeoutSeconds: 600
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: verifyInstancesRunning
 InputPayload:
 targetInstances: '{{getSecondaryInstanceState.originalInstanceStates}}'
 Script: |-
 def verifyInstancesRunning(events,context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 instanceDict = events['targetInstances']
 for instance in instanceDict:
 if instanceDict[instance] == 'stopped':
 print("The target instance " + instance + " is stopped. The
instance will now be started.")
 ec2.start_instances(
 InstanceIds=[instance]
)
 elif instanceDict[instance] == 'stopping':
 print("The target instance " + instance + " is stopping. Polling
for instance to reach stopped state.")
 while instanceDict[instance] != 'stopped':
 poll = ec2.get_waiter('instance_stopped')
 poll.wait(
 InstanceIds=[instance]
)
 ec2.start_instances(
 InstanceIds=[instance]
)
 else:
 pass
 nextStep: waitForSecondaryRunningInstances
- name: waitForSecondaryRunningInstances
 action: 'aws:executeScript'
 timeoutSeconds: 300
 onFailure: Abort

```

```

inputs:
 Runtime: python3.11
 Handler: waitForRunningInstances
 InputPayload:
 targetInstances: '{{getSecondaryInstanceState.originalInstanceStates}}'
 Script: |-
 def waitForRunningInstances(events,context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 instanceDict = events['targetInstances']
 for instance in instanceDict:
 poll = ec2.get_waiter('instance_running')
 poll.wait(
 InstanceIds=[instance]
)
 nextStep: returnSecondaryTagKey
- name: returnSecondaryTagKey
 action: 'aws:executeScript'
 timeoutSeconds: 120
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: returnTagValues
 InputPayload:
 secondaryTag: '{{SecondaryPatchGroupTag}}'
 Script: |-
 def returnTagValues(events,context):
 tag = events['secondaryTag']
 tagKey = list(tag)[0]
 stringKey = "tag:" + tagKey
 return {'tagKey' : stringKey}
 outputs:
 - Name: Payload
 Selector: $.Payload
 Type: StringMap
 - Name: secondaryPatchGroupKey
 Selector: $.Payload.tagKey
 Type: String
 nextStep: returnSecondaryTagValue
- name: returnSecondaryTagValue
 action: 'aws:executeScript'
 timeoutSeconds: 120

```

```

onFailure: Abort
inputs:
 Runtime: python3.11
 Handler: returnTagValues
 InputPayload:
 secondaryTag: '{{SecondaryPatchGroupTag}}'
 Script: |-
 def returnTagValues(events,context):
 tag = events['secondaryTag']
 tagKey = list(tag)[0]
 tagValue = tag[tagKey]
 return {'tagValue' : tagValue}
outputs:
 - Name: Payload
 Selector: $.Payload
 Type: StringMap
 - Name: secondaryPatchGroupValue
 Selector: $.Payload.tagValue
 Type: String
nextStep: patchSecondaryInstances
- name: patchSecondaryInstances
 action: 'aws:runCommand'
 onFailure: Abort
 timeoutSeconds: 7200
 inputs:
 DocumentName: AWS-RunPatchBaseline
 Parameters:
 SnapshotId: '{{SnapshotId}}'
 RebootOption: '{{RebootOption}}'
 Operation: '{{Operation}}'
 Targets:
 - Key: '{{returnSecondaryTagKey.secondaryPatchGroupKey}}'
 Values:
 - '{{returnSecondaryTagValue.secondaryPatchGroupValue}}'
 MaxConcurrency: 10%
 MaxErrors: 10%
 nextStep: returnSecondaryToOriginalState
- name: returnSecondaryToOriginalState
 action: 'aws:executeScript'
 timeoutSeconds: 600
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: returnToOriginalState

```

```

InputPayload:
 targetInstances: '{{getSecondaryInstanceState.originalInstanceStates}}'
Script: |-
 def returnToOriginalState(events,context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 instanceDict = events['targetInstances']
 for instance in instanceDict:
 if instanceDict[instance] == 'stopped' or instanceDict[instance] ==
'stopping':
 ec2.stop_instances(
 InstanceIds=[instance]
)
 else:
 pass

```

## JSON

```

{
 "name": "getSecondaryInstanceState",
 "action": "aws:executeScript",
 "timeoutSeconds": 120,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "getInstanceStates",
 "InputPayload": {
 "secondaryTag": "{{SecondaryPatchGroupTag}}"
 },
 "Script": "..."
 },
 "outputs": [
 {
 "Name": "originalInstanceStates",
 "Selector": "$.Payload",
 "Type": "StringMap"
 }
],
 "nextStep": "verifySecondaryInstancesRunning"
},
{

```

```

 "name": "verifySecondaryInstancesRunning",
 "action": "aws:executeScript",
 "timeoutSeconds": 600,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "verifyInstancesRunning",
 "InputPayload": {

"targetInstances": "{{getSecondaryInstanceState.originalInstanceStates}}"
 },
 "Script": "...
 },
 "nextStep": "waitForSecondaryRunningInstances"
 },
 {
 "name": "waitForSecondaryRunningInstances",
 "action": "aws:executeScript",
 "timeoutSeconds": 300,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "waitForRunningInstances",
 "InputPayload": {

"targetInstances": "{{getSecondaryInstanceState.originalInstanceStates}}"
 },
 "Script": "...
 },
 "nextStep": "returnSecondaryTagKey"
 },
 {
 "name": "returnSecondaryTagKey",
 "action": "aws:executeScript",
 "timeoutSeconds": 120,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "returnTagValues",
 "InputPayload": {
 "secondaryTag": "{{SecondaryPatchGroupTag}}"
 },
 "Script": "...
 },
 },

```

```

 "outputs": [
 {
 "Name": "Payload",
 "Selector": "$.Payload",
 "Type": "StringMap"
 },
 {
 "Name": "secondaryPatchGroupKey",
 "Selector": "$.Payload.tagKey",
 "Type": "String"
 }
],
 "nextStep": "returnSecondaryTagValue"
 },
 {
 "name": "returnSecondaryTagValue",
 "action": "aws:executeScript",
 "timeoutSeconds": 120,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "returnTagValues",
 "InputPayload": {
 "secondaryTag": "{{SecondaryPatchGroupTag}}"
 },
 "Script": "..."
 },
 "outputs": [
 {
 "Name": "Payload",
 "Selector": "$.Payload",
 "Type": "StringMap"
 },
 {
 "Name": "secondaryPatchGroupValue",
 "Selector": "$.Payload.tagValue",
 "Type": "String"
 }
],
 "nextStep": "patchSecondaryInstances"
 },
 {
 "name": "patchSecondaryInstances",
 "action": "aws:runCommand",

```

```

 "onFailure": "Abort",
 "timeoutSeconds": 7200,
 "inputs": {
 "DocumentName": "AWS-RunPatchBaseline",
 "Parameters": {
 "SnapshotId": "{{SnapshotId}}",
 "RebootOption": "{{RebootOption}}",
 "Operation": "{{Operation}}"
 },
 "Targets": [
 {
 "Key": "{{returnSecondaryTagKey.secondaryPatchGroupKey}}",
 "Values": [
 "{{returnSecondaryTagValue.secondaryPatchGroupValue}}"
]
 }
],
 "MaxConcurrency": "10%",
 "MaxErrors": "10%"
 },
 "nextStep": "returnSecondaryToOriginalState"
 },
 {
 "name": "returnSecondaryToOriginalState",
 "action": "aws:executeScript",
 "timeoutSeconds": 600,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "returnToOriginalState",
 "InputPayload": {

 "targetInstances": "{{getSecondaryInstanceState.originalInstanceStates}}",
 },
 "Script": "..."
 }
 }
]
}

```

8. Emily esamina il contenuto del runbook completato con script e crea il runbook nella stessa istanza Account AWS e Regione AWS in quella di destinazione. Ora è pronta a testare il runbook per



assicurarsi che l'automazione funzioni come desiderato prima di implementarla nell'ambiente di produzione. Di seguito è riportato il contenuto completato del runbook con script.

## YAML

```
description: An example of an Automation runbook that patches groups of Amazon EC2
 instances in stages.
schemaVersion: '0.3'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
 AutomationAssumeRole:
 type: String
 description: '(Required) The Amazon Resource Name (ARN) of the IAM role that
 allows Automation to perform the actions on your behalf. If no role is specified,
 Systems Manager Automation uses your IAM permissions to operate this runbook.'
 PrimaryPatchGroupTag:
 type: StringMap
 description: '(Required) The tag for the primary group of instances you want
 to patch. Specify a key-value pair. Example: {"key" : "value"}'
 SecondaryPatchGroupTag:
 type: StringMap
 description: '(Required) The tag for the secondary group of instances you want
 to patch. Specify a key-value pair. Example: {"key" : "value"}'
 SnapshotId:
 type: String
 description: '(Optional) The snapshot ID to use to retrieve a patch baseline
 snapshot.'
 default: ''
 RebootOption:
 type: String
 description: '(Optional) Reboot behavior after a patch Install operation. If
 you choose NoReboot and patches are installed, the instance is marked as non-
 compliant until a subsequent reboot and scan.'
 allowedValues:
 - NoReboot
 - RebootIfNeeded
 default: RebootIfNeeded
 Operation:
 type: String
 description: '(Optional) The update or configuration to perform on the
 instance. The system checks if patches specified in the patch baseline are
 installed on the instance. The install operation installs patches missing from
 the baseline.'
 allowedValues:
```

```

 - Install
 - Scan
 default: Install
mainSteps:
 - name: getPrimaryInstanceState
 action: 'aws:executeScript'
 timeoutSeconds: 120
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: getInstanceStates
 InputPayload:
 primaryTag: '{{PrimaryPatchGroupTag}}'
 Script: |-
 def getInstanceStates(events,context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 tag = events['primaryTag']
 tagKey, tagValue = list(tag.items())[0]
 instanceQuery = ec2.describe_instances(
 Filters=[
 {
 "Name": "tag:" + tagKey,
 "Values": [tagValue]
 }
]
)
 if not instanceQuery['Reservations']:
 noInstancesForTagString = "No instances found for specified tag."
 return({ 'noInstancesFound' : noInstancesForTagString })
 else:
 queryResponse = instanceQuery['Reservations']
 originalInstanceStates = {}
 for results in queryResponse:
 instanceSet = results['Instances']
 for instance in instanceSet:
 instanceId = instance['InstanceId']
 originalInstanceStates[instanceId] = instance['State']

['Name']

 return originalInstanceStates
 outputs:
 - Name: originalInstanceStates
 Selector: $.Payload

```

```

 Type: StringMap
 nextStep: verifyPrimaryInstancesRunning
- name: verifyPrimaryInstancesRunning
 action: 'aws:executeScript'
 timeoutSeconds: 600
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: verifyInstancesRunning
 InputPayload:
 targetInstances: '{{getPrimaryInstanceState.originalInstanceStates}}'
 Script: |-
 def verifyInstancesRunning(events, context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 instanceDict = events['targetInstances']
 for instance in instanceDict:
 if instanceDict[instance] == 'stopped':
 print("The target instance " + instance + " is stopped. The
instance will now be started.")
 ec2.start_instances(
 InstanceIds=[instance]
)
 elif instanceDict[instance] == 'stopping':
 print("The target instance " + instance + " is stopping. Polling
for instance to reach stopped state.")
 while instanceDict[instance] != 'stopped':
 poll = ec2.get_waiter('instance_stopped')
 poll.wait(
 InstanceIds=[instance]
)
 ec2.start_instances(
 InstanceIds=[instance]
)
 else:
 pass
 nextStep: waitForPrimaryRunningInstances
- name: waitForPrimaryRunningInstances
 action: 'aws:executeScript'
 timeoutSeconds: 300
 onFailure: Abort
 inputs:

```

```

Runtime: python3.11
Handler: waitForRunningInstances
InputPayload:
 targetInstances: '{{getPrimaryInstanceState.originalInstanceStates}}'
Script: |-
 def waitForRunningInstances(events,context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 instanceDict = events['targetInstances']
 for instance in instanceDict:
 poll = ec2.get_waiter('instance_running')
 poll.wait(
 InstanceIds=[instance]
)
 nextStep: returnPrimaryTagKey
- name: returnPrimaryTagKey
 action: 'aws:executeScript'
 timeoutSeconds: 120
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: returnTagValues
 InputPayload:
 primaryTag: '{{PrimaryPatchGroupTag}}'
 Script: |-
 def returnTagValues(events,context):
 tag = events['primaryTag']
 tagKey = list(tag)[0]
 stringKey = "tag:" + tagKey
 return {'tagKey' : stringKey}
 outputs:
 - Name: Payload
 Selector: $.Payload
 Type: StringMap
 - Name: primaryPatchGroupKey
 Selector: $.Payload.tagKey
 Type: String
 nextStep: returnPrimaryTagValue
- name: returnPrimaryTagValue
 action: 'aws:executeScript'
 timeoutSeconds: 120
 onFailure: Abort

```

```

inputs:
 Runtime: python3.11
 Handler: returnTagValues
 InputPayload:
 primaryTag: '{{PrimaryPatchGroupTag}}'
 Script: |-
 def returnTagValues(events,context):
 tag = events['primaryTag']
 tagKey = list(tag)[0]
 tagValue = tag[tagKey]
 return {'tagValue' : tagValue}
outputs:
 - Name: Payload
 Selector: $.Payload
 Type: StringMap
 - Name: primaryPatchGroupValue
 Selector: $.Payload.tagValue
 Type: String
nextStep: patchPrimaryInstances
- name: patchPrimaryInstances
 action: 'aws:runCommand'
 onFailure: Abort
 timeoutSeconds: 7200
 inputs:
 DocumentName: AWS-RunPatchBaseline
 Parameters:
 SnapshotId: '{{SnapshotId}}'
 RebootOption: '{{RebootOption}}'
 Operation: '{{Operation}}'
 Targets:
 - Key: '{{returnPrimaryTagKey.primaryPatchGroupKey}}'
 Values:
 - '{{returnPrimaryTagValue.primaryPatchGroupValue}}'
 MaxConcurrency: 10%
 MaxErrors: 10%
 nextStep: returnPrimaryToOriginalState
- name: returnPrimaryToOriginalState
 action: 'aws:executeScript'
 timeoutSeconds: 600
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: returnToOriginalState
 InputPayload:

```

```

 targetInstances: '{{getPrimaryInstanceState.originalInstanceStates}}'
Script: |-
 def returnToOriginalState(events,context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 instanceDict = events['targetInstances']
 for instance in instanceDict:
 if instanceDict[instance] == 'stopped' or instanceDict[instance] ==
'stopping':
 ec2.stop_instances(
 InstanceIds=[instance]
)
 else:
 pass
 nextStep: getSecondaryInstanceState
- name: getSecondaryInstanceState
 action: 'aws:executeScript'
 timeoutSeconds: 120
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: getInstanceStates
 InputPayload:
 secondaryTag: '{{SecondaryPatchGroupTag}}'
 Script: |-
 def getInstanceStates(events,context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 tag = events['secondaryTag']
 tagKey, tagValue = list(tag.items())[0]
 instanceQuery = ec2.describe_instances(
 Filters=[
 {
 "Name": "tag:" + tagKey,
 "Values": [tagValue]
 }
]
)
 if not instanceQuery['Reservations']:
 noInstancesForTagString = "No instances found for specified tag."
 return({ 'noInstancesFound' : noInstancesForTagString })

```

```

 else:
 queryResponse = instanceQuery['Reservations']
 originalInstanceStates = {}
 for results in queryResponse:
 instanceSet = results['Instances']
 for instance in instanceSet:
 instanceId = instance['InstanceId']
 originalInstanceStates[instanceId] = instance['State']

['Name']
 return originalInstanceStates
 outputs:
 - Name: originalInstanceStates
 Selector: $.Payload
 Type: StringMap
 nextStep: verifySecondaryInstancesRunning
- name: verifySecondaryInstancesRunning
 action: 'aws:executeScript'
 timeoutSeconds: 600
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: verifyInstancesRunning
 InputPayload:
 targetInstances: '{{getSecondaryInstanceState.originalInstanceStates}}'
 Script: |-
 def verifyInstancesRunning(events,context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 instanceDict = events['targetInstances']
 for instance in instanceDict:
 if instanceDict[instance] == 'stopped':
 print("The target instance " + instance + " is stopped. The
instance will now be started.")
 ec2.start_instances(
 InstanceIds=[instance]
)
 elif instanceDict[instance] == 'stopping':
 print("The target instance " + instance + " is stopping. Polling
for instance to reach stopped state.")
 while instanceDict[instance] != 'stopped':
 poll = ec2.get_waiter('instance_stopped')
 poll.wait(

```

```

 InstanceIds=[instance]
)
 ec2.start_instances(
 InstanceIds=[instance]
)
else:
 pass
nextStep: waitForSecondaryRunningInstances
- name: waitForSecondaryRunningInstances
 action: 'aws:executeScript'
 timeoutSeconds: 300
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: waitForRunningInstances
 InputPayload:
 targetInstances: '{{getSecondaryInstanceState.originalInstanceStates}}'
 Script: |-
 def waitForRunningInstances(events,context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 instanceDict = events['targetInstances']
 for instance in instanceDict:
 poll = ec2.get_waiter('instance_running')
 poll.wait(
 InstanceIds=[instance]
)
 nextStep: returnSecondaryTagKey
- name: returnSecondaryTagKey
 action: 'aws:executeScript'
 timeoutSeconds: 120
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: returnTagValues
 InputPayload:
 secondaryTag: '{{SecondaryPatchGroupTag}}'
 Script: |-
 def returnTagValues(events,context):
 tag = events['secondaryTag']
 tagKey = list(tag)[0]
 stringKey = "tag:" + tagKey

```



```

 return {'tagKey' : stringKey}
outputs:
 - Name: Payload
 Selector: $.Payload
 Type: StringMap
 - Name: secondaryPatchGroupKey
 Selector: $.Payload.tagKey
 Type: String
nextStep: returnSecondaryTagValue
- name: returnSecondaryTagValue
 action: 'aws:executeScript'
 timeoutSeconds: 120
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: returnTagValues
 InputPayload:
 secondaryTag: '{{SecondaryPatchGroupTag}}'
 Script: |-
 def returnTagValues(events,context):
 tag = events['secondaryTag']
 tagKey = list(tag)[0]
 tagValue = tag[tagKey]
 return {'tagValue' : tagValue}
 outputs:
 - Name: Payload
 Selector: $.Payload
 Type: StringMap
 - Name: secondaryPatchGroupValue
 Selector: $.Payload.tagValue
 Type: String
 nextStep: patchSecondaryInstances
- name: patchSecondaryInstances
 action: 'aws:runCommand'
 onFailure: Abort
 timeoutSeconds: 7200
 inputs:
 DocumentName: AWS-RunPatchBaseline
 Parameters:
 SnapshotId: '{{SnapshotId}}'
 RebootOption: '{{RebootOption}}'
 Operation: '{{Operation}}'
 Targets:
 - Key: '{{returnSecondaryTagKey.secondaryPatchGroupKey}}'

```

```

 Values:
 - '{{returnSecondaryTagValue.secondaryPatchGroupValue}}'
 MaxConcurrency: 10%
 MaxErrors: 10%
 nextStep: returnSecondaryToOriginalState
- name: returnSecondaryToOriginalState
 action: 'aws:executeScript'
 timeoutSeconds: 600
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: returnToOriginalState
 InputPayload:
 targetInstances: '{{getSecondaryInstanceState.originalInstanceStates}}'
 Script: |-
 def returnToOriginalState(events,context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2')
 instanceDict = events['targetInstances']
 for instance in instanceDict:
 if instanceDict[instance] == 'stopped' or instanceDict[instance] ==
'stopping':
 ec2.stop_instances(
 InstanceIds=[instance]
)
 else:
 pass

```

## JSON

```

{
 "description": "An example of an Automation runbook that patches groups of
Amazon EC2 instances in stages.",
 "schemaVersion": "0.3",
 "assumeRole": "{{AutomationAssumeRole}}",
 "parameters": {
 "AutomationAssumeRole": {
 "type": "String",
 "description": "(Required) The Amazon Resource Name (ARN) of the IAM role
that allows Automation to perform the actions on your behalf. If no role is

```

```

specified, Systems Manager Automation uses your IAM permissions to operate this
runbook."
 },
 "PrimaryPatchGroupTag":{
 "type":"StringMap",
 "description":"(Required) The tag for the primary group of instances you
want to patch. Specify a key-value pair. Example: {\"key\" : \"value\"}"
 },
 "SecondaryPatchGroupTag":{
 "type":"StringMap",
 "description":"(Required) The tag for the secondary group of instances
you want to patch. Specify a key-value pair. Example: {\"key\" : \"value\"}"
 },
 "SnapshotId":{
 "type":"String",
 "description":"(Optional) The snapshot ID to use to retrieve a patch
baseline snapshot.",
 "default":""
 },
 "RebootOption":{
 "type":"String",
 "description":"(Optional) Reboot behavior after a patch Install
operation. If you choose NoReboot and patches are installed, the instance is
marked as non-compliant until a subsequent reboot and scan.",
 "allowedValues":[
 "NoReboot",
 "RebootIfNeeded"
],
 "default":"RebootIfNeeded"
 },
 "Operation":{
 "type":"String",
 "description":"(Optional) The update or configuration to perform on
the instance. The system checks if patches specified in the patch baseline are
installed on the instance. The install operation installs patches missing from
the baseline.",
 "allowedValues":[
 "Install",
 "Scan"
],
 "default":"Install"
 }
},
"mainSteps":[

```

```

{
 "name": "getPrimaryInstanceState",
 "action": "aws:executeScript",
 "timeoutSeconds": 120,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "getInstanceStates",
 "InputPayload": {
 "primaryTag": "{{PrimaryPatchGroupTag}}"
 },
 "Script": "..."
 },
 "outputs": [
 {
 "Name": "originalInstanceStates",
 "Selector": "$.Payload",
 "Type": "StringMap"
 }
],
 "nextStep": "verifyPrimaryInstancesRunning"
},
{
 "name": "verifyPrimaryInstancesRunning",
 "action": "aws:executeScript",
 "timeoutSeconds": 600,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "verifyInstancesRunning",
 "InputPayload": {
 "targetInstances": "{{getPrimaryInstanceState.originalInstanceStates}}",
 "Script": "..."
 }
 },
 "nextStep": "waitForPrimaryRunningInstances"
},
{
 "name": "waitForPrimaryRunningInstances",
 "action": "aws:executeScript",
 "timeoutSeconds": 300,
 "onFailure": "Abort",
 "inputs": {

```

```

 "Runtime": "python3.11",
 "Handler": "waitForRunningInstances",
 "InputPayload": {

"targetInstances": "{{getPrimaryInstanceState.originalInstanceStates}}"
 },
 "Script": "...",
 },
 "nextStep": "returnPrimaryTagKey"
},
{
 "name": "returnPrimaryTagKey",
 "action": "aws:executeScript",
 "timeoutSeconds": 120,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "returnTagValues",
 "InputPayload": {
 "primaryTag": "{{PrimaryPatchGroupTag}}"
 },
 "Script": "...",
 },
 "outputs": [
 {
 "Name": "Payload",
 "Selector": "$.Payload",
 "Type": "StringMap"
 },
 {
 "Name": "primaryPatchGroupKey",
 "Selector": "$.Payload.tagKey",
 "Type": "String"
 }
],
 "nextStep": "returnPrimaryTagValue"
},
{
 "name": "returnPrimaryTagValue",
 "action": "aws:executeScript",
 "timeoutSeconds": 120,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",

```

```

 "Handler": "returnTagValues",
 "InputPayload": {
 "primaryTag": "{{PrimaryPatchGroupTag}}"
 },
 "Script": "...",
 },
 "outputs": [
 {
 "Name": "Payload",
 "Selector": "$.Payload",
 "Type": "StringMap"
 },
 {
 "Name": "primaryPatchGroupValue",
 "Selector": "$.Payload.tagValue",
 "Type": "String"
 }
],
 "nextStep": "patchPrimaryInstances"
},
{
 "name": "patchPrimaryInstances",
 "action": "aws:runCommand",
 "onFailure": "Abort",
 "timeoutSeconds": 7200,
 "inputs": {
 "DocumentName": "AWS-RunPatchBaseline",
 "Parameters": {
 "SnapshotId": "{{SnapshotId}}",
 "RebootOption": "{{RebootOption}}",
 "Operation": "{{Operation}}"
 }
 },
 "Targets": [
 {
 "Key": "{{returnPrimaryTagKey.primaryPatchGroupKey}}",
 "Values": [
 "{{returnPrimaryTagValue.primaryPatchGroupValue}}"
]
 }
],
 "MaxConcurrency": "10%",
 "MaxErrors": "10%",
},
"nextStep": "returnPrimaryToOriginalState"

```

```

 },
 {
 "name": "returnPrimaryToOriginalState",
 "action": "aws:executeScript",
 "timeoutSeconds": 600,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "returnToOriginalState",
 "InputPayload": {

"targetInstances": "{{getPrimaryInstanceState.originalInstanceStates}}"
 },
 "Script": "..."
 },
 "nextStep": "getSecondaryInstanceState"
 },
 {
 "name": "getSecondaryInstanceState",
 "action": "aws:executeScript",
 "timeoutSeconds": 120,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "getInstanceStates",
 "InputPayload": {
 "secondaryTag": "{{SecondaryPatchGroupTag}}"
 },
 "Script": "..."
 },
 "outputs": [
 {
 "Name": "originalInstanceStates",
 "Selector": "$.Payload",
 "Type": "StringMap"
 }
],
 "nextStep": "verifySecondaryInstancesRunning"
 },
 {
 "name": "verifySecondaryInstancesRunning",
 "action": "aws:executeScript",
 "timeoutSeconds": 600,
 "onFailure": "Abort",

```

```

 "inputs":{
 "Runtime":"python3.11",
 "Handler":"verifyInstancesRunning",
 "InputPayload":{

"targetInstances":"{{getSecondaryInstanceState.originalInstanceStates}}"
 },
 "Script":"..."
 },
 "nextStep":"waitForSecondaryRunningInstances"
 },
 {
 "name":"waitForSecondaryRunningInstances",
 "action":"aws:executeScript",
 "timeoutSeconds":300,
 "onFailure":"Abort",
 "inputs":{
 "Runtime":"python3.11",
 "Handler":"waitForRunningInstances",
 "InputPayload":{

"targetInstances":"{{getSecondaryInstanceState.originalInstanceStates}}"
 },
 "Script":"..."
 },
 "nextStep":"returnSecondaryTagKey"
 },
 {
 "name":"returnSecondaryTagKey",
 "action":"aws:executeScript",
 "timeoutSeconds":120,
 "onFailure":"Abort",
 "inputs":{
 "Runtime":"python3.11",
 "Handler":"returnTagValues",
 "InputPayload":{
 "secondaryTag":"{{SecondaryPatchGroupTag}}"
 },
 "Script":"..."
 },
 "outputs":[
 {
 "Name":"Payload",
 "Selector":"$.Payload",

```



```

 "Type": "StringMap"
 },
 {
 "Name": "secondaryPatchGroupKey",
 "Selector": "$.Payload.tagKey",
 "Type": "String"
 }
],
"nextStep": "returnSecondaryTagValue"
},
{
 "name": "returnSecondaryTagValue",
 "action": "aws:executeScript",
 "timeoutSeconds": 120,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "returnTagValues",
 "InputPayload": {
 "secondaryTag": "{{SecondaryPatchGroupTag}}"
 },
 "Script": "..."
 },
 "outputs": [
 {
 "Name": "Payload",
 "Selector": "$.Payload",
 "Type": "StringMap"
 },
 {
 "Name": "secondaryPatchGroupValue",
 "Selector": "$.Payload.tagValue",
 "Type": "String"
 }
],
 "nextStep": "patchSecondaryInstances"
},
{
 "name": "patchSecondaryInstances",
 "action": "aws:runCommand",
 "onFailure": "Abort",
 "timeoutSeconds": 7200,
 "inputs": {
 "DocumentName": "AWS-RunPatchBaseline",

```

```

 "Parameters":{
 "SnapshotId":"{{SnapshotId}}",
 "RebootOption":"{{RebootOption}}",
 "Operation":"{{Operation}}"
 },
 "Targets":[
 {
 "Key":"{{returnSecondaryTagKey.secondaryPatchGroupKey}}",
 "Values":[
 "{{returnSecondaryTagValue.secondaryPatchGroupValue}}"
]
 }
],
 "MaxConcurrency":"10%",
 "MaxErrors":"10%"
 },
 "nextStep":"returnSecondaryToOriginalState"
},
{
 "name":"returnSecondaryToOriginalState",
 "action":"aws:executeScript",
 "timeoutSeconds":600,
 "onFailure":"Abort",
 "inputs":{
 "Runtime":"python3.11",
 "Handler":"returnToOriginalState",
 "InputPayload":{

 "targetInstances":"{{getSecondaryInstanceState.originalInstanceStates}}"
 },
 "Script":"..."
 }
}
]
}

```

Per ulteriori informazioni sulle operazioni di automazione utilizzate in questo esempio, consulta [Riferimento alle operazioni del servizio di automazione di Systems Manager](#).

## Ulteriori esempi di runbook

Il seguente runbook di esempio mostra come utilizzare le azioni di AWS Systems Manager automazione per automatizzare le attività comuni di distribuzione, risoluzione dei problemi e manutenzione.

### Note

Gli esempi di runbook in questa sezione vengono forniti per illustrare come creare runbook personalizzati per supportare le specifiche esigenze operative. Questi runbook non sono destinati all'uso in ambienti di produzione così come sono. Tuttavia, è possibile personalizzarli per uso personale.

## Esempi

- [Implementazione di architettura VPC e controller di dominio Microsoft Active Directory](#)
- [Ripristino di un volume radice dall'ultimo snapshot](#)
- [Creazione di un'AMI e una copia tra regioni](#)

### Implementazione di architettura VPC e controller di dominio Microsoft Active Directory

Per aumentare l'efficienza e standardizzare i processi comuni, è possibile scegliere di automatizzare le implementazioni. Ciò è utile se si distribuisce regolarmente la stessa architettura su più account e Regioni AWS. L'automazione delle implementazioni dell'architettura può anche ridurre il rischio di errori umani che possono verificarsi durante l'implementazione manuale dell'architettura. AWS Systems Manager Le azioni di automazione possono aiutarti a raggiungere questo obiettivo. L'automazione è uno strumento di AWS Systems Manager.

Il AWS Systems Manager runbook di esempio seguente esegue queste azioni:

- Recupera l'Amazon Machine Image (AMI) per Windows Server 2016 più recente mediante Parameter Store di Systems Manager per l'utilizzo durante l'avvio delle istanze di EC2, che verranno configurate come controller di dominio. Parameter Store è uno strumento di AWS Systems Manager.
- Utilizza l'azione di `aws:executeAwsApi` automazione per richiamare diverse operazioni AWS API per creare l'architettura VPC. Le istanze del controller di dominio vengono avviate in sottoreti private e si connettono a Internet tramite un gateway NAT. Ciò consente allo strumento SSM Agent sulle istanze di accedere agli endpoint necessari di Systems Manager.

- Utilizza l'azione di `aws:waitForAwsResourceProperty` automazione per confermare che le istanze avviate dall'azione precedente sono Online destinate. AWS Systems Manager
- Utilizza l'operazione di automazione `aws:runCommand` per configurare le istanze avviate come controller di dominio Microsoft Active Directory.

## YAML

```

description: Custom Automation Deployment Example
schemaVersion: '0.3'
parameters:
 AutomationAssumeRole:
 type: String
 default: ''
 description: >-
 (Optional) The ARN of the role that allows Automation to perform the
 actions on your behalf. If no role is specified, Systems Manager
 Automation uses your IAM permissions to run this runbook.
mainSteps:
 - name: getLatestWindowsAmi
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ssm
 Api: GetParameter
 Name: >-
 /aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base
 outputs:
 - Name: amiId
 Selector: $.Parameter.Value
 Type: String
 nextStep: createSSMInstanceRole
 - name: createSSMInstanceRole
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: iam
 Api: CreateRole
 AssumeRolePolicyDocument: >-
```

```

 {"Version": "2012-10-17", "Statement":
[{"Effect": "Allow", "Principal": {"Service": ["ec2.amazonaws.com"]}, "Action":
["sts:AssumeRole"]}]}
 RoleName: sampleSSMInstanceRole
 nextStep: attachManagedSSMPolicy
 - name: attachManagedSSMPolicy
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: iam
 Api: AttachRolePolicy
 PolicyArn: 'arn:aws:iam::aws:policy/service-role/
AmazonSSMManagedInstanceCore'
 RoleName: sampleSSMInstanceRole
 nextStep: createSSMInstanceProfile
 - name: createSSMInstanceProfile
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: iam
 Api: CreateInstanceProfile
 InstanceProfileName: sampleSSMInstanceRole
 outputs:
 - Name: instanceProfileArn
 Selector: $.InstanceProfile.Arn
 Type: String
 nextStep: addSSMInstanceRoleToProfile
 - name: addSSMInstanceRoleToProfile
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: iam
 Api: AddRoleToInstanceProfile
 InstanceProfileName: sampleSSMInstanceRole
 RoleName: sampleSSMInstanceRole
 nextStep: createVpc
 - name: createVpc
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: CreateVpc
 CidrBlock: 10.0.100.0/22
 outputs:

```

```
- Name: vpcId
 Selector: $.Vpc.VpcId
 Type: String
nextStep: getMainRtb
- name: getMainRtb
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: DescribeRouteTables
 Filters:
 - Name: vpc-id
 Values:
 - '{{ createVpc.vpcId }}'
 outputs:
 - Name: mainRtbId
 Selector: '$.RouteTables[0].RouteTableId'
 Type: String
 nextStep: verifyMainRtb
- name: verifyMainRtb
 action: aws:assertAwsResourceProperty
 onFailure: Abort
 inputs:
 Service: ec2
 Api: DescribeRouteTables
 RouteTableIds:
 - '{{ getMainRtb.mainRtbId }}'
 PropertySelector: '$.RouteTables[0].Associations[0].Main'
 DesiredValues:
 - 'True'
 nextStep: createPubSubnet
- name: createPubSubnet
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: CreateSubnet
 CidrBlock: 10.0.103.0/24
 AvailabilityZone: us-west-2c
 VpcId: '{{ createVpc.vpcId }}'
 outputs:
 - Name: pubSubnetId
 Selector: $.Subnet.SubnetId
 Type: String
```

```
 nextStep: createPubRtb
 - name: createPubRtb
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: CreateRouteTable
 VpcId: '{{ createVpc.vpcId }}'
 outputs:
 - Name: pubRtbId
 Selector: $.RouteTable.RouteTableId
 Type: String
 nextStep: createIgw
 - name: createIgw
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: CreateInternetGateway
 outputs:
 - Name: igwId
 Selector: $.InternetGateway.InternetGatewayId
 Type: String
 nextStep: attachIgw
 - name: attachIgw
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: AttachInternetGateway
 InternetGatewayId: '{{ createIgw.igwId }}'
 VpcId: '{{ createVpc.vpcId }}'
 nextStep: allocateEip
 - name: allocateEip
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: AllocateAddress
 Domain: vpc
 outputs:
 - Name: eipAllocationId
 Selector: $.AllocationId
 Type: String
```

```
 nextStep: createNatGw
 - name: createNatGw
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: CreateNatGateway
 AllocationId: '{{ allocateEip.eipAllocationId }}'
 SubnetId: '{{ createPubSubnet.pubSubnetId }}'
 outputs:
 - Name: natGwId
 Selector: $.NatGateway.NatGatewayId
 Type: String
 nextStep: verifyNatGwAvailable
 - name: verifyNatGwAvailable
 action: aws:waitForAwsResourceProperty
 timeoutSeconds: 150
 inputs:
 Service: ec2
 Api: DescribeNatGateways
 NatGatewayIds:
 - '{{ createNatGw.natGwId }}'
 PropertySelector: '$.NatGateways[0].State'
 DesiredValues:
 - available
 nextStep: createNatRoute
 - name: createNatRoute
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: CreateRoute
 DestinationCidrBlock: 0.0.0.0/0
 NatGatewayId: '{{ createNatGw.natGwId }}'
 RouteTableId: '{{ getMainRtb.mainRtbId }}'
 nextStep: createPubRoute
 - name: createPubRoute
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: CreateRoute
 DestinationCidrBlock: 0.0.0.0/0
 GatewayId: '{{ createIgw.igwId }}'
```



```

 RouteTableId: '{{ createPubRtb.pubRtbId }}'
 nextStep: setPubSubAssoc
- name: setPubSubAssoc
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: AssociateRouteTable
 RouteTableId: '{{ createPubRtb.pubRtbId }}'
 SubnetId: '{{ createPubSubnet.pubSubnetId }}'
- name: createDhcpOptions
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: CreateDhcpOptions
 DhcpConfigurations:
 - Key: domain-name-servers
 Values:
 - '10.0.100.50,10.0.101.50'
 - Key: domain-name
 Values:
 - sample.com
 outputs:
 - Name: dhcpOptionsId
 Selector: $.DhcpOptions.DhcpOptionsId
 Type: String
 nextStep: createDCSubnet1
- name: createDCSubnet1
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: CreateSubnet
 CidrBlock: 10.0.100.0/24
 AvailabilityZone: us-west-2a
 VpcId: '{{ createVpc.vpcId }}'
 outputs:
 - Name: firstSubnetId
 Selector: $.Subnet.SubnetId
 Type: String
 nextStep: createDCSubnet2
- name: createDCSubnet2
 action: aws:executeAwsApi

```

```
onFailure: Abort
inputs:
 Service: ec2
 Api: CreateSubnet
 CidrBlock: 10.0.101.0/24
 AvailabilityZone: us-west-2b
 VpcId: '{{ createVpc.vpcId }}'
outputs:
 - Name: secondSubnetId
 Selector: $.Subnet.SubnetId
 Type: String
nextStep: createDCSecGroup
- name: createDCSecGroup
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: CreateSecurityGroup
 GroupName: SampleDCSecGroup
 Description: Security Group for Sample Domain Controllers
 VpcId: '{{ createVpc.vpcId }}'
 outputs:
 - Name: dcSecGroupId
 Selector: $.GroupId
 Type: String
 nextStep: authIngressDCTraffic
- name: authIngressDCTraffic
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: AuthorizeSecurityGroupIngress
 GroupId: '{{ createDCSecGroup.dcSecGroupId }}'
 IpPermissions:
 - FromPort: -1
 IpProtocol: '-1'
 IpRanges:
 - CidrIp: 0.0.0.0/0
 Description: Allow all traffic between Domain Controllers
 nextStep: verifyInstanceProfile
- name: verifyInstanceProfile
 action: aws:waitForAwsResourceProperty
 maxAttempts: 5
 onFailure: Abort
```

```
inputs:
 Service: iam
 Api: ListInstanceProfilesForRole
 RoleName: sampleSSMInstanceRole
 PropertySelector: '$.InstanceProfiles[0].Arn'
 DesiredValues:
 - '{{ createSSMInstanceProfile.instanceProfileArn }}'
nextStep: iamEventualConsistency
- name: iamEventualConsistency
 action: aws:sleep
 inputs:
 Duration: PT2M
 nextStep: launchDC1
- name: launchDC1
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: RunInstances
 BlockDeviceMappings:
 - DeviceName: /dev/sda1
 Ebs:
 DeleteOnTermination: true
 VolumeSize: 50
 VolumeType: gp2
 - DeviceName: xvdf
 Ebs:
 DeleteOnTermination: true
 VolumeSize: 100
 VolumeType: gp2
 IamInstanceProfile:
 Arn: '{{ createSSMInstanceProfile.instanceProfileArn }}'
 ImageId: '{{ getLatestWindowsAmi.amiId }}'
 InstanceType: t2.micro
 MaxCount: 1
 MinCount: 1
 PrivateIpAddress: 10.0.100.50
 SecurityGroupIds:
 - '{{ createDCSecGroup.dcSecGroupId }}'
 SubnetId: '{{ createDCSubnet1.firstSubnetId }}'
 TagSpecifications:
 - ResourceType: instance
 Tags:
 - Key: Name
```

```

 Value: SampleDC1
 outputs:
 - Name: pdcInstanceId
 Selector: '$.Instances[0].InstanceId'
 Type: String
 nextStep: launchDC2
- name: launchDC2
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: RunInstances
 BlockDeviceMappings:
 - DeviceName: /dev/sda1
 Ebs:
 DeleteOnTermination: true
 VolumeSize: 50
 VolumeType: gp2
 - DeviceName: xvdf
 Ebs:
 DeleteOnTermination: true
 VolumeSize: 100
 VolumeType: gp2
 IamInstanceProfile:
 Arn: '{{ createSSMInstanceProfile.instanceProfileArn }}'
 ImageId: '{{ getLatestWindowsAmi.amiId }}'
 InstanceType: t2.micro
 MaxCount: 1
 MinCount: 1
 PrivateIpAddress: 10.0.101.50
 SecurityGroupIds:
 - '{{ createDCSecGroup.dcSecGroupId }}'
 SubnetId: '{{ createDCSubnet2.secondSubnetId }}'
 TagSpecifications:
 - ResourceType: instance
 Tags:
 - Key: Name
 Value: SampleDC2
 outputs:
 - Name: adcInstanceId
 Selector: '$.Instances[0].InstanceId'
 Type: String
 nextStep: verifyDCInstanceState
- name: verifyDCInstanceState

```

```

 action: aws:waitForAwsResourceProperty
 inputs:
 Service: ec2
 Api: DescribeInstanceStatus
 IncludeAllInstances: true
 InstanceIds:
 - '{{ launchDC1.pdcInstanceId }}'
 - '{{ launchDC2.adcInstanceId }}'
 PropertySelector: '$.InstanceStatuses..InstanceState.Name'
 DesiredValues:
 - running
 nextStep: verifyInstancesOnlineSSM
 - name: verifyInstancesOnlineSSM
 action: aws:waitForAwsResourceProperty
 timeoutSeconds: 600
 inputs:
 Service: ssm
 Api: DescribeInstanceInformation
 InstanceInformationFilterList:
 - key: InstanceIds
 valueSet:
 - '{{ launchDC1.pdcInstanceId }}'
 - '{{ launchDC2.adcInstanceId }}'
 PropertySelector: '$.InstanceInformationList..PingStatus'
 DesiredValues:
 - Online
 nextStep: installADRoles
 - name: installADRoles
 action: aws:runCommand
 inputs:
 DocumentName: AWS-RunPowerShellScript
 InstanceIds:
 - '{{ launchDC1.pdcInstanceId }}'
 - '{{ launchDC2.adcInstanceId }}'
 Parameters:
 commands: |-
 try {
 Install-WindowsFeature -Name AD-Domain-Services -
IncludeManagementTools
 }
 catch {
 Write-Error "Failed to install ADDS Role."
 }
 nextStep: setAdminPassword

```

```

- name: setAdminPassword
 action: aws:runCommand
 inputs:
 DocumentName: AWS-RunPowerShellScript
 InstanceIds:
 - '{{ launchDC1.pdcInstanceId }}'
 Parameters:
 commands:
 - net user Administrator "sampleAdminPass123!"
 nextStep: createForest
- name: createForest
 action: aws:runCommand
 inputs:
 DocumentName: AWS-RunPowerShellScript
 InstanceIds:
 - '{{ launchDC1.pdcInstanceId }}'
 Parameters:
 commands: |-
 $dsrmPass = 'sample123!' | ConvertTo-SecureString -asPlainText -Force
 try {
 Install-ADDSForest -DomainName "sample.com" -DomainMode 6
 } catch {
 Write-Error $_
 }
 try {
 Add-DnsServerForwarder -IPAddress "10.0.100.2"
 } catch {
 Write-Error $_
 }
 nextStep: associateDhcpOptions
- name: associateDhcpOptions
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: AssociateDhcpOptions
 DhcpOptionsId: '{{ createDhcpOptions.dhcpOptionsId }}'
 VpcId: '{{ createVpc.vpcId }}'
 nextStep: waitForADServices
- name: waitForADServices

```

```

 action: aws:sleep
 inputs:
 Duration: PT1M
 nextStep: promoteADC
 - name: promoteADC
 action: aws:runCommand
 inputs:
 DocumentName: AWS-RunPowerShellScript
 InstanceIds:
 - '{{ launchDC2.adcInstanceId }}'
 Parameters:
 commands: |-
 ipconfig /renew
 $dsrmPass = 'sample123!' | ConvertTo-SecureString -asPlainText -Force
 $domAdminUser = "sample\Administrator"
 $domAdminPass = "sampleAdminPass123!" | ConvertTo-SecureString -
asPlainText -Force
 $domAdminCred = New-Object
System.Management.Automation.PSCredential($domAdminUser,$domAdminPass)

 try {
 Install-ADDSDomainController -DomainName "sample.com" -InstallDNS
-DatabasePath "D:\NTDS" -SysvolPath "D:\SYSVOL" -SafeModeAdministratorPassword
$dsrmPass -Credential $domAdminCred -Force
 }
 catch {
 Write-Error $_
 }

```

## JSON

```

{
 "description": "Custom Automation Deployment Example",
 "schemaVersion": "0.3",
 "assumeRole": "{{ AutomationAssumeRole }}",
 "parameters": {
 "AutomationAssumeRole": {
 "type": "String",
 "description": "(Optional) The ARN of the role that allows Automation
to perform the actions on your behalf. If no role is specified, Systems Manager
Automation uses your IAM permissions to run this runbook.",
 "default": ""
 }
 }
}

```

```

 },
 "mainSteps": [
 {
 "name": "getLatestWindowsAmi",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ssm",
 "Api": "GetParameter",
 "Name": "/aws/service/ami-windows-latest/Windows_Server-2016-English-
Full-Base"
 },
 "outputs": [
 {
 "Name": "amiId",
 "Selector": "$.Parameter.Value",
 "Type": "String"
 }
],
 "nextStep": "createSSMInstanceRole"
 },
 {
 "name": "createSSMInstanceRole",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "iam",
 "Api": "CreateRole",
 "AssumeRolePolicyDocument": "{\"Version\":\"2012-10-17\",\"Statement\":
[{\n\"Effect\": \"Allow\", \"Principal\": {\n\"Service\": [\n\"ec2.amazonaws.com\"]}, \"Action
\": [\n\"sts:AssumeRole\"]}]}",
 "RoleName": "sampleSSMInstanceRole"
 },
 "nextStep": "attachManagedSSMPolicy"
 },
 {
 "name": "attachManagedSSMPolicy",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "iam",
 "Api": "AttachRolePolicy",
 "PolicyArn": "arn:aws:iam::aws:policy/service-role/
AmazonSSMManagedInstanceCore",

```



```
 "RoleName": "sampleSSMInstanceRole"
 },
 "nextStep": "createSSMInstanceProfile"
},
{
 "name": "createSSMInstanceProfile",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "iam",
 "Api": "CreateInstanceProfile",
 "InstanceProfileName": "sampleSSMInstanceRole"
 },
 "outputs": [
 {
 "Name": "instanceProfileArn",
 "Selector": "$.InstanceProfile.Arn",
 "Type": "String"
 }
],
 "nextStep": "addSSMInstanceRoleToProfile"
},
{
 "name": "addSSMInstanceRoleToProfile",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "iam",
 "Api": "AddRoleToInstanceProfile",
 "InstanceProfileName": "sampleSSMInstanceRole",
 "RoleName": "sampleSSMInstanceRole"
 },
 "nextStep": "createVpc"
},
{
 "name": "createVpc",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "CreateVpc",
 "CidrBlock": "10.0.100.0/22"
 },
 "outputs": [
```

```

 {
 "Name": "vpcId",
 "Selector": "$.Vpc.VpcId",
 "Type": "String"
 }
],
 "nextStep": "getMainRtb"
},
{
 "name": "getMainRtb",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "DescribeRouteTables",
 "Filters": [
 {
 "Name": "vpc-id",
 "Values": ["{{ createVpc.vpcId }}"]
 }
]
 },
 "outputs": [
 {
 "Name": "mainRtbId",
 "Selector": "$.RouteTables[0].RouteTableId",
 "Type": "String"
 }
],
 "nextStep": "verifyMainRtb"
},
{
 "name": "verifyMainRtb",
 "action": "aws:assertAwsResourceProperty",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "DescribeRouteTables",
 "RouteTableIds": ["{{ getMainRtb.mainRtbId }}"],
 "PropertySelector": "$.RouteTables[0].Associations[0].Main",
 "DesiredValues": ["True"]
 },
 "nextStep": "createPubSubnet"
},

```

```
{
 "name": "createPubSubnet",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "CreateSubnet",
 "CidrBlock": "10.0.103.0/24",
 "AvailabilityZone": "us-west-2c",
 "VpcId": "{{ createVpc.vpcId }}"
 },
 "outputs": [
 {
 "Name": "pubSubnetId",
 "Selector": "$.Subnet.SubnetId",
 "Type": "String"
 }
],
 "nextStep": "createPubRtb"
},
{
 "name": "createPubRtb",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "CreateRouteTable",
 "VpcId": "{{ createVpc.vpcId }}"
 },
 "outputs": [
 {
 "Name": "pubRtbId",
 "Selector": "$.RouteTable.RouteTableId",
 "Type": "String"
 }
],
 "nextStep": "createIgw"
},
{
 "name": "createIgw",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
```

```
 "Api": "CreateInternetGateway"
 },
 "outputs": [
 {
 "Name": "igwId",
 "Selector": "$.InternetGateway.InternetGatewayId",
 "Type": "String"
 }
],
 "nextStep": "attachIgw"
},
{
 "name": "attachIgw",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "AttachInternetGateway",
 "InternetGatewayId": "{{ createIgw.igwId }}",
 "VpcId": "{{ createVpc.vpcId }}"
 },
 "nextStep": "allocateEip"
},
{
 "name": "allocateEip",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "AllocateAddress",
 "Domain": "vpc"
 },
 "outputs": [
 {
 "Name": "eipAllocationId",
 "Selector": "$.AllocationId",
 "Type": "String"
 }
],
 "nextStep": "createNatGw"
},
{
 "name": "createNatGw",
 "action": "aws:executeAwsApi",
```

```

 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "CreateNatGateway",
 "AllocationId": "{{ allocateEip.eipAllocationId }}",
 "SubnetId": "{{ createPubSubnet.pubSubnetId }}"
 },
 "outputs": [
 {
 "Name": "natGwId",
 "Selector": "$.NatGateway.NatGatewayId",
 "Type": "String"
 }
],
 "nextStep": "verifyNatGwAvailable"
 },
 {
 "name": "verifyNatGwAvailable",
 "action": "aws:waitForAwsResourceProperty",
 "timeoutSeconds": 150,
 "inputs": {
 "Service": "ec2",
 "Api": "DescribeNatGateways",
 "NatGatewayIds": [
 "{{ createNatGw.natGwId }}"
],
 "PropertySelector": "$.NatGateways[0].State",
 "DesiredValues": [
 "available"
]
 },
 "nextStep": "createNatRoute"
 },
 {
 "name": "createNatRoute",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "CreateRoute",
 "DestinationCidrBlock": "0.0.0.0/0",
 "NatGatewayId": "{{ createNatGw.natGwId }}",
 "RouteTableId": "{{ getMainRtb.mainRtbId }}"
 }
 },

```

```

 "nextStep": "createPubRoute"
 },
 {
 "name": "createPubRoute",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "CreateRoute",
 "DestinationCidrBlock": "0.0.0.0/0",
 "GatewayId": "{{ createIgw.igwId }}",
 "RouteTableId": "{{ createPubRtb.pubRtbId }}"
 },
 "nextStep": "setPubSubAssoc"
 },
 {
 "name": "setPubSubAssoc",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "AssociateRouteTable",
 "RouteTableId": "{{ createPubRtb.pubRtbId }}",
 "SubnetId": "{{ createPubSubnet.pubSubnetId }}"
 }
 },
 {
 "name": "createDhcpOptions",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "CreateDhcpOptions",
 "DhcpConfigurations": [
 {
 "Key": "domain-name-servers",
 "Values": ["10.0.100.50", "10.0.101.50"]
 },
 {
 "Key": "domain-name",
 "Values": ["sample.com"]
 }
]
 }
 },
 },

```

```
 "outputs": [
 {
 "Name": "dhcpOptionsId",
 "Selector": "$.DhcpOptions.DhcpOptionsId",
 "Type": "String"
 }
],
 "nextStep": "createDCSubnet1"
 },
 {
 "name": "createDCSubnet1",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "CreateSubnet",
 "CidrBlock": "10.0.100.0/24",
 "AvailabilityZone": "us-west-2a",
 "VpcId": "{{ createVpc.vpcId }}"
 },
 "outputs": [
 {
 "Name": "firstSubnetId",
 "Selector": "$.Subnet.SubnetId",
 "Type": "String"
 }
],
 "nextStep": "createDCSubnet2"
 },
 {
 "name": "createDCSubnet2",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "CreateSubnet",
 "CidrBlock": "10.0.101.0/24",
 "AvailabilityZone": "us-west-2b",
 "VpcId": "{{ createVpc.vpcId }}"
 },
 "outputs": [
 {
 "Name": "secondSubnetId",
 "Selector": "$.Subnet.SubnetId",
```

```

 "Type": "String"
 }
],
"nextStep": "createDCSecGroup"
},
{
 "name": "createDCSecGroup",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "CreateSecurityGroup",
 "GroupName": "SampleDCSecGroup",
 "Description": "Security Group for Example Domain Controllers",
 "VpcId": "{{ createVpc.vpcId }}"
 },
 "outputs": [
 {
 "Name": "dcSecGroupId",
 "Selector": "$.GroupId",
 "Type": "String"
 }
],
 "nextStep": "authIngressDCTraffic"
},
{
 "name": "authIngressDCTraffic",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "AuthorizeSecurityGroupIngress",
 "GroupId": "{{ createDCSecGroup.dcSecGroupId }}",
 "IpPermissions": [
 {
 "FromPort": -1,
 "IpProtocol": "-1",
 "IpRanges": [
 {
 "CidrIp": "0.0.0.0/0",
 "Description": "Allow all traffic between Domain Controllers"
 }
]
 }
]
 }
}

```



```

],
 },
 "nextStep": "verifyInstanceProfile"
 },
 {
 "name": "verifyInstanceProfile",
 "action": "aws:waitForAwsResourceProperty",
 "maxAttempts": 5,
 "onFailure": "Abort",
 "inputs": {
 "Service": "iam",
 "Api": "ListInstanceProfilesForRole",
 "RoleName": "sampleSSMInstanceRole",
 "PropertySelector": "$.InstanceProfiles[0].Arn",
 "DesiredValues": [
 "{{ createSSMInstanceProfile.instanceProfileArn }}"
]
 },
 "nextStep": "iamEventualConsistency"
 },
 {
 "name": "iamEventualConsistency",
 "action": "aws:sleep",
 "inputs": {
 "Duration": "PT2M"
 },
 "nextStep": "launchDC1"
 },
 {
 "name": "launchDC1",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "RunInstances",
 "BlockDeviceMappings": [
 {
 "DeviceName": "/dev/sda1",
 "Ebs": {
 "DeleteOnTermination": true,
 "VolumeSize": 50,
 "VolumeType": "gp2"
 }
 }
]
 },
 },

```

```

 {
 "DeviceName": "xvdf",
 "Ebs": {
 "DeleteOnTermination": true,
 "VolumeSize": 100,
 "VolumeType": "gp2"
 }
 }
],
 "IamInstanceProfile": {
 "Arn": "{{ createSSMInstanceProfile.instanceProfileArn }}"
 },
 "ImageId": "{{ getLatestWindowsAmi.amiId }}",
 "InstanceType": "t2.micro",
 "MaxCount": 1,
 "MinCount": 1,
 "PrivateIpAddress": "10.0.100.50",
 "SecurityGroupIds": [
 "{{ createDCSecGroup.dcSecGroupId }}"
],
 "SubnetId": "{{ createDCSubnet1.firstSubnetId }}",
 "TagSpecifications": [
 {
 "ResourceType": "instance",
 "Tags": [
 {
 "Key": "Name",
 "Value": "SampleDC1"
 }
]
 }
]
},
"outputs": [
 {
 "Name": "pdcInstanceId",
 "Selector": "$.Instances[0].InstanceId",
 "Type": "String"
 }
],
"nextStep": "launchDC2"
},
{
 "name": "launchDC2",

```

```
"action": "aws:executeAwsApi",
"onFailure": "Abort",
"inputs": {
 "Service": "ec2",
 "Api": "RunInstances",
 "BlockDeviceMappings": [
 {
 "DeviceName": "/dev/sda1",
 "Ebs": {
 "DeleteOnTermination": true,
 "VolumeSize": 50,
 "VolumeType": "gp2"
 }
 },
 {
 "DeviceName": "xvdf",
 "Ebs": {
 "DeleteOnTermination": true,
 "VolumeSize": 100,
 "VolumeType": "gp2"
 }
 }
],
 "IamInstanceProfile": {
 "Arn": "{{ createSSMInstanceProfile.instanceProfileArn }}"
 },
 "ImageId": "{{ getLatestWindowsAmi.amiId }}",
 "InstanceType": "t2.micro",
 "MaxCount": 1,
 "MinCount": 1,
 "PrivateIpAddress": "10.0.101.50",
 "SecurityGroupIds": [
 "{{ createDCSecGroup.dcSecGroupId }}"
],
 "SubnetId": "{{ createDCSubnet2.secondSubnetId }}",
 "TagSpecifications": [
 {
 "ResourceType": "instance",
 "Tags": [
 {
 "Key": "Name",
 "Value": "SampleDC2"
 }
]
 }
]
}
```

```

 }
]
},
"outputs": [
 {
 "Name": "adcInstanceId",
 "Selector": "$.Instances[0].InstanceId",
 "Type": "String"
 }
],
"nextStep": "verifyDCInstanceState"
},
{
 "name": "verifyDCInstanceState",
 "action": "aws:waitForAwsResourceProperty",
 "inputs": {
 "Service": "ec2",
 "Api": "DescribeInstanceStatus",
 "IncludeAllInstances": true,
 "InstanceIds": [
 "{{ launchDC1.pdcInstanceId }}",
 "{{ launchDC2.adcInstanceId }}"
],
 "PropertySelector": "$.InstanceStatuses[0].InstanceState.Name",
 "DesiredValues": [
 "running"
]
 },
 "nextStep": "verifyInstancesOnlineSSM"
},
{
 "name": "verifyInstancesOnlineSSM",
 "action": "aws:waitForAwsResourceProperty",
 "timeoutSeconds": 600,
 "inputs": {
 "Service": "ssm",
 "Api": "DescribeInstanceInformation",
 "InstanceInformationFilterList": [
 {
 "key": "InstanceIds",
 "valueSet": [
 "{{ launchDC1.pdcInstanceId }}",
 "{{ launchDC2.adcInstanceId }}"
]
 }
]
 }
}

```

```

 }
],
 "PropertySelector": "$.InstanceInformationList[0].PingStatus",
 "DesiredValues": [
 "Online"
]
 },
 "nextStep": "installADRoles"
 },
 {
 "name": "installADRoles",
 "action": "aws:runCommand",
 "inputs": {
 "DocumentName": "AWS-RunPowerShellScript",
 "InstanceIds": [
 "{{ launchDC1.pdcInstanceId }}",
 "{{ launchDC2.adcInstanceId }}"
],
 "Parameters": {
 "commands": [
 "try {",
 " Install-WindowsFeature -Name AD-Domain-Services -",
IncludeManagementTools",
 "}",
 "catch {",
 " Write-Error \"Failed to install ADDS Role.\"\"",
 "}"
]
 }
 },
 "nextStep": "setAdminPassword"
 },
 {
 "name": "setAdminPassword",
 "action": "aws:runCommand",
 "inputs": {
 "DocumentName": "AWS-RunPowerShellScript",
 "InstanceIds": [
 "{{ launchDC1.pdcInstanceId }}"
],
 "Parameters": {
 "commands": [
 "net user Administrator \"sampleAdminPass123!\""
]
 }
 }
 }
}

```

```

 }
 },
 "nextStep": "createForest"
},
{
 "name": "createForest",
 "action": "aws:runCommand",
 "inputs": {
 "DocumentName": "AWS-RunPowerShellScript",
 "InstanceIds": [
 "{{ launchDC1.pdcInstanceId }}"
],
 "Parameters": {
 "commands": [
 "$dsrmPass = 'sample123!' | ConvertTo-SecureString -asPlainText -
Force",
 "try {",
 " Install-ADDSForest -DomainName \"sample.com\" -DomainMode 6 -
ForestMode 6 -InstallDNS -DatabasePath \"D:\\\\NTDS\\\\" -SysvolPath \"D:\\\\SYSVOL\\\\" -
SafeModeAdministratorPassword $dsrmPass -Force",
 "}",
 "catch {",
 " Write-Error $_",
 "}",
 "try {",
 " Add-DnsServerForwarder -IPAddress \"10.0.100.2\"",
 "}",
 "catch {",
 " Write-Error $_",
 "}"
]
 }
 }
},
 "nextStep": "associateDhcpOptions"
},
{
 "name": "associateDhcpOptions",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "AssociateDhcpOptions",
 "DhcpOptionsId": "{{ createDhcpOptions.dhcpOptionsId }}",
 "VpcId": "{{ createVpc.vpcId }}"
 }
}

```

```

 },
 "nextStep": "waitForADServices"
 },
 {
 "name": "waitForADServices",
 "action": "aws:sleep",
 "inputs": {
 "Duration": "PT1M"
 },
 "nextStep": "promoteADC"
 },
 {
 "name": "promoteADC",
 "action": "aws:runCommand",
 "inputs": {
 "DocumentName": "AWS-RunPowerShellScript",
 "InstanceIds": [
 "{{ launchDC2.adcInstanceId }}"
],
 "Parameters": {
 "commands": [
 "ipconfig /renew",
 "$dsrmPass = 'sample123!' | ConvertTo-SecureString -asPlainText -
Force",
 "$domAdminUser = \"sample\\Administrator\\\"",
 "$domAdminPass = \"sampleAdminPass123!\" | ConvertTo-SecureString -
asPlainText -Force",
 "$domAdminCred = New-Object
System.Management.Automation.PSCredential($domAdminUser,$domAdminPass)",
 "try {",
 " Install-ADDSDomainController -DomainName \"sample.com
\" -InstallDNS -DatabasePath \"D:\\NTDS\\\" -SysvolPath \"D:\\SYSVOL\\\" -
SafeModeAdministratorPassword $dsrmPass -Credential $domAdminCred -Force",
 "}",
 "catch {",
 " Write-Error $_",
 "}"
]
 }
 }
 }
]
}

```

## Ripristino di un volume radice dall'ultimo snapshot

Il sistema operativo su un volume radice può danneggiarsi per vari motivi. Ad esempio, a seguito di un'operazione di patch, le istanze potrebbero non riuscire ad avviarsi correttamente a causa di un kernel o di un registro di sistema danneggiato. L'automazione delle attività di risoluzione dei problemi più comuni, come il ripristino di un volume root dall'ultima istantanea scattata prima dell'operazione di patching, può ridurre i tempi di inattività e accelerare le attività di risoluzione dei problemi. AWS Systems Manager Le azioni di automazione possono aiutarti a raggiungere questo obiettivo. L'automazione è uno strumento di AWS Systems Manager.

Il AWS Systems Manager runbook di esempio seguente esegue queste azioni:

- Utilizza l'operazione di automazione `aws:executeAwsApi` per recuperare i dettagli dal volume principale dell'istanza.
- Utilizza l'operazione di automazione `aws:executeScript` per recuperare lo snapshot più recente per il volume radice.
- Utilizza l'operazione di automazione `aws:branch` per continuare l'automazione se viene trovato uno snapshot per il volume radice.

## YAML

```

description: Custom Automation Troubleshooting Example
schemaVersion: '0.3'
assumeRole: "{{ AutomationAssumeRole }}"
parameters:
 AutomationAssumeRole:
 type: String
 description: "(Required) The ARN of the role that allows Automation to
perform
the actions on your behalf. If no role is specified, Systems Manager
Automation
uses your IAM permissions to use this runbook."
 default: ''
 InstanceId:
 type: String
 description: "(Required) The Instance Id whose root EBS volume you want to
restore the latest Snapshot."
 default: ''
```



```

mainSteps:
- name: getInstanceDetails
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: DescribeInstances
 InstanceIds:
 - "{{ InstanceId }}"
 outputs:
 - Name: availabilityZone
 Selector: "$.Reservations[0].Instances[0].Placement.AvailabilityZone"
 Type: String
 - Name: rootDeviceName
 Selector: "$.Reservations[0].Instances[0].RootDeviceName"
 Type: String
 nextStep: getRootVolumeId
- name: getRootVolumeId
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: DescribeVolumes
 Filters:
 - Name: attachment.device
 Values: ["{{ getInstanceDetails.rootDeviceName }}"]
 - Name: attachment.instance-id
 Values: ["{{ InstanceId }}"]
 outputs:
 - Name: rootVolumeId
 Selector: "$.Volumes[0].VolumeId"
 Type: String
 nextStep: getSnapshotsByStartTime
- name: getSnapshotsByStartTime
 action: aws:executeScript
 timeoutSeconds: 45
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: getSnapshotsByStartTime
 InputPayload:
 rootVolumeId : "{{ getRootVolumeId.rootVolumeId }}"
 Script: |-
 def getSnapshotsByStartTime(events, context):

```

```

import boto3

#Initialize client
ec2 = boto3.client('ec2')
rootVolumeId = events['rootVolumeId']
snapshotsQuery = ec2.describe_snapshots(
 Filters=[
 {
 "Name": "volume-id",
 "Values": [rootVolumeId]
 }
]
)
if not snapshotsQuery['Snapshots']:
 noSnapshotFoundString = "NoSnapshotFound"
 return { 'noSnapshotFound' : noSnapshotFoundString }
else:
 jsonSnapshots = snapshotsQuery['Snapshots']
 sortedSnapshots = sorted(jsonSnapshots, key=lambda k: k['StartTime'],
reverse=True)
 latestSortedSnapshotId = sortedSnapshots[0]['SnapshotId']
 return { 'latestSnapshotId' : latestSortedSnapshotId }

outputs:
- Name: Payload
 Selector: $.Payload
 Type: StringMap
- Name: latestSnapshotId
 Selector: $.Payload.latestSnapshotId
 Type: String
- Name: noSnapshotFound
 Selector: $.Payload.noSnapshotFound
 Type: String
nextStep: branchFromResults
- name: branchFromResults
 action: aws:branch
 onFailure: Abort
inputs:
 Choices:
 - NextStep: createNewRootVolumeFromSnapshot
 Not:
 Variable: "{{ getSnapshotsByStartTime.noSnapshotFound }}"
 StringEquals: "NoSnapshotFound"
isEnd: true
- name: createNewRootVolumeFromSnapshot

```

```
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: CreateVolume
 AvailabilityZone: "{{ getInstanceDetails.availabilityZone }}"
 SnapshotId: "{{ getSnapshotsByStartTime.latestSnapshotId }}"
 outputs:
 - Name: newRootVolumeId
 Selector: "$.VolumeId"
 Type: String
 nextStep: stopInstance
- name: stopInstance
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: StopInstances
 InstanceIds:
 - "{{ InstanceId }}"
 nextStep: verifyVolumeAvailability
- name: verifyVolumeAvailability
 action: aws:waitForAwsResourceProperty
 timeoutSeconds: 120
 inputs:
 Service: ec2
 Api: DescribeVolumes
 VolumeIds:
 - "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
 PropertySelector: "$.Volumes[0].State"
 DesiredValues:
 - "available"
 nextStep: verifyInstanceStopped
- name: verifyInstanceStopped
 action: aws:waitForAwsResourceProperty
 timeoutSeconds: 120
 inputs:
 Service: ec2
 Api: DescribeInstances
 InstanceIds:
 - "{{ InstanceId }}"
 PropertySelector: "$.Reservations[0].Instances[0].State.Name"
 DesiredValues:
 - "stopped"
```

```
 nextStep: detachRootVolume
- name: detachRootVolume
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: DetachVolume
 VolumeId: "{{ getRootVolumeId.rootVolumeId }}"
 nextStep: verifyRootVolumeDetached
- name: verifyRootVolumeDetached
 action: aws:waitForAwsResourceProperty
 timeoutSeconds: 30
 inputs:
 Service: ec2
 Api: DescribeVolumes
 VolumeIds:
 - "{{ getRootVolumeId.rootVolumeId }}"
 PropertySelector: "$.Volumes[0].State"
 DesiredValues:
 - "available"
 nextStep: attachNewRootVolume
- name: attachNewRootVolume
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: AttachVolume
 Device: "{{ getInstanceDetails.rootDeviceName }}"
 InstanceId: "{{ InstanceId }}"
 VolumeId: "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
 nextStep: verifyNewRootVolumeAttached
- name: verifyNewRootVolumeAttached
 action: aws:waitForAwsResourceProperty
 timeoutSeconds: 30
 inputs:
 Service: ec2
 Api: DescribeVolumes
 VolumeIds:
 - "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
 PropertySelector: "$.Volumes[0].Attachments[0].State"
 DesiredValues:
 - "attached"
 nextStep: startInstance
- name: startInstance
```

```
action: aws:executeAwsApi
onFailure: Abort
inputs:
 Service: ec2
 Api: StartInstances
 InstanceIds:
 - "{{ InstanceId }}"
```

## JSON

```
{
 "description": "Custom Automation Troubleshooting Example",
 "schemaVersion": "0.3",
 "assumeRole": "{{ AutomationAssumeRole }}",
 "parameters": {
 "AutomationAssumeRole": {
 "type": "String",
 "description": "(Required) The ARN of the role that allows Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses your IAM permissions to run this runbook.",
 "default": ""
 },
 "InstanceId": {
 "type": "String",
 "description": "(Required) The Instance Id whose root EBS volume you want to restore the latest Snapshot.",
 "default": ""
 }
 },
 "mainSteps": [
 {
 "name": "getInstanceDetails",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "DescribeInstances",
 "InstanceIds": [
 "{{ InstanceId }}"
]
 },
 "outputs": [
```

```

 {
 "Name": "availabilityZone",
 "Selector":
"$$.Reservations[0].Instances[0].Placement.AvailabilityZone",
 "Type": "String"
 },
 {
 "Name": "rootDeviceName",
 "Selector": "$$.Reservations[0].Instances[0].RootDeviceName",
 "Type": "String"
 }
],
 "nextStep": "getRootVolumeId"
},
{
 "name": "getRootVolumeId",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "DescribeVolumes",
 "Filters": [
 {
 "Name": "attachment.device",
 "Values": [
 "{{ getInstanceDetails.rootDeviceName }}"
]
 },
 {
 "Name": "attachment.instance-id",
 "Values": [
 "{{ InstanceId }}"
]
 }
]
 },
 "outputs": [
 {
 "Name": "rootVolumeId",
 "Selector": "$$.Volumes[0].VolumeId",
 "Type": "String"
 }
],
 "nextStep": "getSnapshotsByStartTime"
}

```

```

 },
 {
 "name": "getSnapshotsByStartTime",
 "action": "aws:executeScript",
 "timeoutSeconds": 45,
 "onFailure": "Continue",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "getSnapshotsByStartTime",
 "InputPayload": {
 "rootVolumeId": "{{ getRootVolumeId.rootVolumeId }}"
 },
 "Attachment": "getSnapshotsByStartTime.py"
 },
 "outputs": [
 {
 "Name": "Payload",
 "Selector": "$.Payload",
 "Type": "StringMap"
 },
 {
 "Name": "latestSnapshotId",
 "Selector": "$.Payload.latestSnapshotId",
 "Type": "String"
 },
 {
 "Name": "noSnapshotFound",
 "Selector": "$.Payload.noSnapshotFound",
 "Type": "String"
 }
],
 "nextStep": "branchFromResults"
 },
 {
 "name": "branchFromResults",
 "action": "aws:branch",
 "onFailure": "Abort",
 "inputs": {
 "Choices": [
 {
 "NextStep": "createNewRootVolumeFromSnapshot",
 "Not": {
 "Variable":
 "{{ getSnapshotsByStartTime.noSnapshotFound }}"
 }
 }
]
 }
 }
]
}

```

```

 "StringEquals": "NoSnapshotFound"
 }
 }
],
 },
 "isEnd": true
},
{
 "name": "createNewRootVolumeFromSnapshot",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "CreateVolume",
 "AvailabilityZone": "{{ getInstanceDetails.availabilityZone }}",
 "SnapshotId": "{{ getSnapshotsByStartTime.latestSnapshotId }}"
 },
 "outputs": [
 {
 "Name": "newRootVolumeId",
 "Selector": "$.VolumeId",
 "Type": "String"
 }
],
 "nextStep": "stopInstance"
},
{
 "name": "stopInstance",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "StopInstances",
 "InstanceIds": [
 "{{ InstanceId }}"
]
 },
 "nextStep": "verifyVolumeAvailability"
},
{
 "name": "verifyVolumeAvailability",
 "action": "aws:waitForAwsResourceProperty",
 "timeoutSeconds": 120,
 "inputs": {

```



```

 "Service": "ec2",
 "Api": "DescribeVolumes",
 "VolumeIds": [
 "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
],
 "PropertySelector": "$.Volumes[0].State",
 "DesiredValues": [
 "available"
]
 },
 "nextStep": "verifyInstanceStopped"
},
{
 "name": "verifyInstanceStopped",
 "action": "aws:waitForAwsResourceProperty",
 "timeoutSeconds": 120,
 "inputs": {
 "Service": "ec2",
 "Api": "DescribeInstances",
 "InstanceIds": [
 "{{ InstanceId }}"
],
 "PropertySelector": "$.Reservations[0].Instances[0].State.Name",
 "DesiredValues": [
 "stopped"
]
 },
 "nextStep": "detachRootVolume"
},
{
 "name": "detachRootVolume",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "DetachVolume",
 "VolumeId": "{{ getRootVolumeId.rootVolumeId }}"
 },
 "nextStep": "verifyRootVolumeDetached"
},
{
 "name": "verifyRootVolumeDetached",
 "action": "aws:waitForAwsResourceProperty",
 "timeoutSeconds": 30,

```

```

 "inputs": {
 "Service": "ec2",
 "Api": "DescribeVolumes",
 "VolumeIds": [
 "{{ getRootVolumeId.rootVolumeId }}"
],
 "PropertySelector": "$.Volumes[0].State",
 "DesiredValues": [
 "available"
]
 },
 "nextStep": "attachNewRootVolume"
 },
 {
 "name": "attachNewRootVolume",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "AttachVolume",
 "Device": "{{ getInstanceDetails.rootDeviceName }}",
 "InstanceId": "{{ InstanceId }}",
 "VolumeId": "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
 },
 "nextStep": "verifyNewRootVolumeAttached"
 },
 {
 "name": "verifyNewRootVolumeAttached",
 "action": "aws:waitForAwsResourceProperty",
 "timeoutSeconds": 30,
 "inputs": {
 "Service": "ec2",
 "Api": "DescribeVolumes",
 "VolumeIds": [
 "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
],
 "PropertySelector": "$.Volumes[0].Attachments[0].State",
 "DesiredValues": [
 "attached"
]
 },
 "nextStep": "startInstance"
 },
 {

```

```
 "name": "startInstance",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "StartInstances",
 "InstanceIds": [
 "{{ InstanceId }}"
]
 }
 },
],
 "files": {
 "getSnapshotsByStartTime.py": {
 "checksums": {
 "sha256": "sampleETagValue"
 }
 }
 }
}
```

## Creazione di un'AMI e una copia tra regioni

La creazione di un'Amazon Machine Image (AMI) di un'istanza è un processo comune utilizzato nel backup e nel ripristino. È inoltre possibile scegliere di copiare un'AMI in un'altra Regione AWS come parte di un'architettura di disaster recovery. L'automazione delle attività di manutenzione comuni può ridurre i tempi di inattività se un problema richiede il failover. AWS Systems Manager Le azioni di automazione possono aiutarti a raggiungere questo obiettivo. L'automazione è uno strumento di AWS Systems Manager.

Il AWS Systems Manager runbook di esempio seguente esegue queste azioni:

- Utilizza l'operazione di automazione `aws:executeAwsApi` per creare un'AMI.
- Utilizza l'operazione di automazione `aws:waitForAwsResourceProperty` per confermare la disponibilità dell'AMI.
- Utilizza l'operazione di automazione `aws:executeScript` per copiare l'AMI nella regione di destinazione.

## YAML

```

description: Custom Automation Backup and Recovery Example
schemaVersion: '0.3'
assumeRole: "{{ AutomationAssumeRole }}"
parameters:
 AutomationAssumeRole:
 type: String
 description: "(Required) The ARN of the role that allows Automation to
perform
the actions on your behalf. If no role is specified, Systems Manager
Automation
uses your IAM permissions to use this runbook."
 default: ''
 InstanceId:
 type: String
 description: "(Required) The ID of the EC2 instance."
 default: ''
mainSteps:
- name: createImage
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: CreateImage
 InstanceId: "{{ InstanceId }}"
 Name: "Automation Image for {{ InstanceId }}"
 NoReboot: false
 outputs:
 - Name: newImageId
 Selector: "$.ImageId"
 Type: String
 nextStep: verifyImageAvailability
- name: verifyImageAvailability
 action: aws:waitForAwsResourceProperty
 timeoutSeconds: 600
 inputs:
 Service: ec2
 Api: DescribeImages
 ImageIds:
 - "{{ createImage.newImageId }}"
 PropertySelector: "$.Images[0].State"

```

```

 DesiredValues:
 - available
 nextStep: copyImage
 - name: copyImage
 action: aws:executeScript
 timeoutSeconds: 45
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: crossRegionImageCopy
 InputPayload:
 newImageId : "{{ createImage.newImageId }}"
 Script: |-
 def crossRegionImageCopy(events,context):
 import boto3

 #Initialize client
 ec2 = boto3.client('ec2', region_name='us-east-1')
 newImageId = events['newImageId']

 ec2.copy_image(
 Name='DR Copy for ' + newImageId,
 SourceImageId=newImageId,
 SourceRegion='us-west-2'
)

```

## JSON

```

{
 "description": "Custom Automation Backup and Recovery Example",
 "schemaVersion": "0.3",
 "assumeRole": "{{ AutomationAssumeRole }}",
 "parameters": {
 "AutomationAssumeRole": {
 "type": "String",
 "description": "(Required) The ARN of the role that allows Automation to perform\nthe actions on your behalf. If no role is specified, Systems Manager Automation\nuses your IAM permissions to run this runbook.",
 "default": ""
 },
 "InstanceId": {
 "type": "String",

```

```

 "description": "(Required) The ID of the EC2 instance.",
 "default": ""
 },
 },
 "mainSteps": [
 {
 "name": "createImage",
 "action": "aws:executeAwsApi",
 "onFailure": "Abort",
 "inputs": {
 "Service": "ec2",
 "Api": "CreateImage",
 "InstanceId": "{{ InstanceId }}",
 "Name": "Automation Image for {{ InstanceId }}",
 "NoReboot": false
 },
 },
 "outputs": [
 {
 "Name": "newImageId",
 "Selector": "$.ImageId",
 "Type": "String"
 }
],
 "nextStep": "verifyImageAvailability"
 },
 {
 "name": "verifyImageAvailability",
 "action": "aws:waitForAwsResourceProperty",
 "timeoutSeconds": 600,
 "inputs": {
 "Service": "ec2",
 "Api": "DescribeImages",
 "ImageIds": [
 "{{ createImage.newImageId }}"
],
 "PropertySelector": "$.Images[0].State",
 "DesiredValues": [
 "available"
]
 },
 "nextStep": "copyImage"
 },
 {
 "name": "copyImage",

```

```

 "action": "aws:executeScript",
 "timeoutSeconds": 45,
 "onFailure": "Abort",
 "inputs": {
 "Runtime": "python3.11",
 "Handler": "crossRegionImageCopy",
 "InputPayload": {
 "newImageId": "{{ createImage.newImageId }}"
 },
 "Attachment": "crossRegionImageCopy.py"
 }
 },
 "files": {
 "crossRegionImageCopy.py": {
 "checksums": {
 "sha256": "sampleETagValue"
 }
 }
 }
}

```

## Creazione di parametri di input che popolano AWS risorse

L'automazione popola AWS le risorse Console di gestione AWS che corrispondono al tipo di risorsa definito per un parametro di input. Le risorse nel tuo Account AWS che corrispondono al tipo di risorsa vengono visualizzati in un menu a tendina da cui scegliere. Puoi definire i tipi di parametri di input per le istanze Amazon Elastic Compute Cloud (Amazon EC2), i bucket Amazon Simple Storage Service (Amazon S3) e i ruoli (IAM). AWS Identity and Access Management Le definizioni dei tipi supportate e le espressioni regolari utilizzate per individuare le risorse corrispondenti sono le seguenti:

- `AWS::EC2::Instance::Id - ^m?i-([a-z0-9]{8}|[a-z0-9]{17})$`
- `List<AWS::EC2::Instance::Id> - ^m?i-([a-z0-9]{8}|[a-z0-9]{17})$`
- `AWS::S3::Bucket::Name - ^[0-9a-z][a-z0-9\\-\\.]{3,63}$`
- `List<AWS::S3::Bucket::Name> - ^[0-9a-z][a-z0-9\\-\\.]{3,63}$`
- `AWS::IAM::Role::Arn - ^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

- `List<AWS::IAM::Role::Arn> - ^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Di seguito è riportato un esempio di tipi di parametri di input definiti nel contenuto del runbook.

## YAML

```
description: Enables encryption on an Amazon S3 bucket
schemaVersion: '0.3'
assumeRole: '{{ AutomationAssumeRole }}'
parameters:
 BucketName:
 type: 'AWS::S3::Bucket::Name'
 description: (Required) The name of the Amazon S3 bucket you want to encrypt.
 SSEAlgorithm:
 type: String
 description: (Optional) The server-side encryption algorithm to use for the
 default encryption.
 default: AES256
 AutomationAssumeRole:
 type: 'AWS::IAM::Role::Arn'
 description: (Optional) The Amazon Resource Name (ARN) of the role that allows
 Automation to perform the actions on your behalf.
 default: ''
mainSteps:
 - name: enableBucketEncryption
 action: 'aws:executeAwsApi'
 inputs:
 Service: s3
 Api: PutBucketEncryption
 Bucket: '{{BucketName}}'
 ServerSideEncryptionConfiguration:
 Rules:
 - ApplyServerSideEncryptionByDefault:
 SSEAlgorithm: '{{SSEAlgorithm}}'
 isEnd: true
```

## JSON

```
{
 "description": "Enables encryption on an Amazon S3 bucket",
 "schemaVersion": "0.3",
```



```

 "assumeRole": "{{ AutomationAssumeRole }}",
 "parameters": {
 "BucketName": {
 "type": "AWS::S3::Bucket::Name",
 "description": "(Required) The name of the Amazon S3 bucket you want to
encrypt."
 },
 "SSEAlgorithm": {
 "type": "String",
 "description": "(Optional) The server-side encryption algorithm to use for
the default encryption.",
 "default": "AES256"
 },
 "AutomationAssumeRole": {
 "type": "AWS::IAM::Role::Arn",
 "description": "(Optional) The Amazon Resource Name (ARN) of the role that
allows Automation to perform the actions on your behalf.",
 "default": ""
 }
 },
 "mainSteps": [
 {
 "name": "enableBucketEncryption",
 "action": "aws:executeAwsApi",
 "inputs": {
 "Service": "s3",
 "Api": "PutBucketEncryption",
 "Bucket": "{{BucketName}}",
 "ServerSideEncryptionConfiguration": {
 "Rules": [
 {
 "ApplyServerSideEncryptionByDefault": {
 "SSEAlgorithm": "{{SSEAlgorithm}}"
 }
 }
]
 }
 },
 "isEnd": true
 }
]
 }
}

```

## Utilizzo di Generatore di documenti per la creazione di runbook

Se i runbook AWS Systems Manager pubblici non supportano tutte le azioni che desideri eseguire sulle tue AWS risorse, puoi creare i tuoi runbook. Per creare un runbook personalizzato, puoi creare manualmente un file locale in formato YAML o JSON con le operazioni di automazione appropriate. In alternativa, puoi utilizzare Generatore di documenti nella console di Automazione Systems Manager per creare un runbook personalizzato.

Utilizzando Generatore di documenti, puoi aggiungere operazioni di automazione al runbook personalizzato e fornire i parametri richiesti senza dover utilizzare la sintassi JSON o YAML. Dopo aver aggiunto fasi e creato il runbook, il sistema converte le operazioni aggiunte nel formato YAML che Systems Manager può utilizzare per eseguire l'automazione.

I runbook supportano l'uso di Markdown, un linguaggio di markup, che consente di aggiungere descrizioni in stile wiki ai runbook e ai singoli passaggi all'interno del runbook. Per ulteriori informazioni sull'utilizzo di Markdown, consulta [Utilizzo di Markdown in AWS](#).

### Creazione di un runbook utilizzando Generatore di documenti

#### Prima di iniziare

Ti consigliamo di leggere le diverse operazioni che è possibile utilizzare all'interno di un runbook. Per ulteriori informazioni, consulta [Riferimento alle operazioni del servizio di automazione di Systems Manager](#).

#### Per creare un runbook utilizzando Generatore di documenti

1. Apri <https://console.aws.amazon.com/systems-manager/> la console all'indirizzo. AWS Systems Manager
2. Nel pannello di navigazione, scegli Documenti.
3. Scegli Crea automazione.
4. Per Nome, inserisci un nome descrittivo per il runbook.
5. Per Descrizione documento, specificare la descrizione dello stile markdown per il runbook. È possibile fornire istruzioni per l'utilizzo del runbook, delle fasi numerate o di qualsiasi altro tipo di informazioni per descrivere il runbook. Fare riferimento al testo predefinito per informazioni sulla formattazione del contenuto.

 Tip

Passare da Nascondi anteprima a Mostra anteprima e viceversa per vedere come appare il contenuto della descrizione durante la composizione.

6. (Facoltativo) Per Ruolo presunto, inserisci il nome o l'ARN di un ruolo di servizio per eseguire operazioni per tuo conto. Se non si specifica un ruolo, il servizio di automazione utilizza le autorizzazioni di accesso dell'utente che esegue l'automazione.

 Important

Per i runbook non di proprietà di Amazon che utilizzano l'operazione `aws:executeScript`, è necessario specificare un ruolo. Per informazioni, consulta [Autorizzazioni per l'utilizzo di runbook](#).

7. (Facoltativo) Per Output, inserisci eventuali output per l'automazione di questo runbook per renderli disponibili per altri processi.

Ad esempio, se il runbook crea una nuova AMI, puoi specificare [» `CreateImage.ImageId` «] e quindi utilizzare questo output per creare nuove istanze in un'automazione successiva.

8. (Facoltativo) Espandi la sezione Parametri di input ed effettua le seguenti operazioni.
  1. Per Nome parametro, inserisci un nome descrittivo per il parametro del runbook che si sta creando.
  2. Per Tipo, scegli un tipo per il parametro, ad esempio `String` o `MapList`.
  3. Per Obbligatorio, effettua una delle seguenti operazioni:
    - Seleziona Sì, se per questo parametro del runbook deve essere fornito un valore durante il runtime.
    - Seleziona No, se il parametro non è richiesto e (facoltativo) inserire un valore di parametro predefinito in Valore predefinito.
  4. Per Descrizione, inserisci una descrizione per il parametro del runbook.

 Note

Per aggiungere altri parametri del runbook, scegli **Aggiungi un parametro**. Per rimuovere un parametro del runbook, seleziona il pulsante **X (Rimuovi)**.

9. (Facoltativo) Espandi la sezione **Tipo di destinazione** e scegli un tipo di destinazione per definire i tipi di risorse su cui è possibile eseguire l'automazione. Ad esempio, per utilizzare un runbook sulle istanze di EC2, scegli `/AWS::EC2::Instance`.

 Note

Se si specifica un valore di `/`, il runbook può essere eseguito su tutti i tipi di risorse. Per un elenco dei tipi di risorse validi, consulta [Informazioni di riferimento sui tipi di proprietà e di risorse di AWS](#) nella Guida per l'utente di AWS CloudFormation .

10. (Facoltativo) Espandi la sezione **Tag documento** e inserisci una o più coppie chiave-valore tag da applicare al runbook. I tag semplificano l'identificazione, l'organizzazione e la ricerca delle risorse.

11. Nella sezione **Fase 1** fornisci le seguenti informazioni.

- Per **Nome fase**, inserisci un nome descrittivo per la prima fase dell'automazione.
- Per **Tipo di operazione**, seleziona il tipo di operazione da utilizzare per questa fase.

Per un elenco e informazioni sui tipi di operazione disponibili, consulta [Riferimento alle operazioni del servizio di automazione di Systems Manager](#).

- In **Descrizione**, inserisci una descrizione per la fase di automazione. È possibile utilizzare Markdown per formattare il testo.
- A seconda del **Tipo di operazione** selezionato, inserisci gli input necessari per il tipo di operazione nella sezione **Input** della fase. Ad esempio, se è stata selezionata l'operazione `aws:approve`, è necessario specificare un valore per la proprietà `Approvers`.

Per informazioni sui campi di input della fase, consulta la voce in [Riferimento alle operazioni del servizio di automazione di Systems Manager](#) relativa al tipo di operazione selezionato. Ad esempio: [aws:executeStateMachine— Esegui una macchina a AWS Step Functions stati](#).

- (Facoltativo) Per Input aggiuntivi, fornisci eventuali valori di input aggiuntivi necessari per il runbook. I tipi di input disponibili dipendono dal tipo di operazione selezionato per la fase. (Si noti che alcuni tipi di operazione richiedono valori di input.)

 Note

Per aggiungere altri input, selezionare Aggiungi input facoltativo. Per rimuovere un input, scegli il pulsante X (Rimuovi).

- (Facoltativo) Per Output, inserisci eventuali output per questa fase per renderli disponibili per altri processi.

 Note

Output non è disponibile per tutti i tipi di operazione.

- (Facoltativo) Espandi la sezione Proprietà comuni e specifica le proprietà per le operazioni comuni a tutte le operazioni di automazione. Ad esempio, per i Secondi di timeout, è possibile fornire un valore in secondi per specificare per quanto tempo è possibile eseguire la fase prima che venga arrestata.

Per ulteriori informazioni, consulta [Proprietà condivise da tutte le operazioni](#).

 Note

Per aggiungere altre fasi, seleziona Aggiungi fase e ripeti la procedura per la creazione di una fase. Per rimuovere una fase, seleziona Rimuovi fase.

## 12. Scegli Crea automazione per salvare il runbook.

### Creazione di un runbook che esegue script

La procedura seguente mostra come utilizzare Generatore di documenti nella console di Automazione AWS Systems Manager per creare un runbook personalizzato che esegue uno script.

La prima fase del runbook creato esegue uno script per avviare un'istanza Amazon Elastic Compute Cloud (Amazon EC2). Nella seconda fase viene eseguito un altro script per monitorare il controllo

dello stato dell'istanza da modificare in ok. Quindi, viene riportato uno stato generale di Success per l'automazione.

Prima di iniziare

Effettuare le operazioni seguenti:

- Verificare di disporre dei privilegi di amministratore o di disporre delle autorizzazioni appropriate per accedere a Systems Manager in AWS Identity and Access Management (IAM).

Per informazioni, consulta [Verifica dell'accesso utente per runbook](#).

- Verificare di disporre di un ruolo di servizio IAM per il servizio di automazione (noto anche come ruolo presunto) nell' Account AWS. Il ruolo è necessario perché questa procedura dettagliata utilizza l'operazione `aws:executeScript`.

Per ulteriori informazioni sulla creazione di questo ruolo, consulta [Configurazione di un accesso al ruolo di servizio \(ruolo presunto\) per le automazioni](#).

Per informazioni sul requisito del ruolo di servizio IAM per l'esecuzione di `aws:executeScript`, consulta [Autorizzazioni per l'utilizzo di runbook](#).

- Accertati di disporre dell'autorizzazione per avviare le istanze EC2.

Per ulteriori informazioni, consulta [IAM e Amazon EC2](#) nella Guida per l'utente di Amazon EC2.

Per creare un runbook personalizzato che esegue script utilizzando Generatore di documenti

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Documenti.
3. Scegli Crea automazione.
4. Per Nome, digita questo nome descrittivo per il runbook: **LaunchInstanceAndCheckStatus**.
5. (Facoltativo) Per Descrizione documento, sostituisci il testo predefinito con una descrizione per questo runbook, utilizzando Markdown. Di seguito è riportato un esempio di :

```
##Title: LaunchInstanceAndCheckState

Purpose: This runbook first launches an EC2 instance using the AMI
ID provided in the parameter ``imageId``. The second step of this runbook
```

continuously checks the instance status check value for the launched instance until the status ``ok`` is returned.

```
##Parameters:

Name	Type	Description	Default Value
assumeRole | String | (Optional) The ARN of the role that allows Automation to
perform the actions on your behalf. | -
imageId | String | (Optional) The AMI ID to use for launching the instance.
The default value uses the latest Amazon Linux 2023 AMI ID available. | {{ ssm:/
aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-arm64 }}
```

6. In Ruolo presunto, inserisci l'ARN del ruolo di servizio IAM per il servizio di automazione (Ruolo presunto) per l'automazione, nel formato **arn:aws:iam::111122223333:role/AutomationServiceRole**. Sostituisci il tuo Account AWS ID con 111122223333.

Il ruolo specificato viene utilizzato per fornire le autorizzazioni necessarie per avviare l'automazione.

#### Important

Per i runbook non di proprietà di Amazon che utilizzano l'operazione `aws:executeScript`, è necessario specificare un ruolo. Per informazioni, consulta [Autorizzazioni per l'utilizzo di runbook](#).

7. Espandi Parametri di input e procedi come segue.

1. Per Nome parametro, inserisci **imageId**.
2. In Tipo, scegli **String**.
3. Per Obbligatorio, scegli No.
4. Per Valore predefinito, inserisci quanto segue.

```
{{ ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-arm64 }}
```

 Note

Questo valore avvia un'istanza Amazon EC2 utilizzando l'ID Amazon Linux 2023 () più recente. Amazon Machine Image AMI Se si desidera utilizzare un AMI diverso, sostituire il valore con il proprio ID AMI.

5. Per Descrizione, inserisci quanto segue.

(Optional) The AMI ID to use for launching the instance. The default value uses the latest released Amazon Linux 2023 AMI ID.

8. Scegli Aggiungi un parametro per creare il secondo parametro, **tagValue** e inserisci quanto segue.

1. Per Nome parametro, inserisci **tagValue**.
2. In Tipo, scegli **String**.
3. Per Obbligatorio, scegli No.
4. In Valore predefinito, inserisci **LaunchedBySsmAutomation**. Questo aggiunge il valore di coppia di chiavi tag Name : LaunchedBySsmAutomation all'istanza.
5. Per Descrizione, inserisci quanto segue.

(Optional) The tag value to add to the instance. The default value is LaunchedBySsmAutomation.

9. Scegli Aggiungi un parametro per creare il terzo parametro, **instanceType** e inserisci le informazioni seguenti.

1. Per Nome parametro, inserisci **instanceType**.
2. In Tipo, scegli **String**.
3. Per Obbligatorio, scegli No.
4. In Valore predefinito, inserisci **t2.micro**.
5. Per Descrizione parametro, inserisci quanto segue.

(Optional) The instance type to use for the instance. The default value is t2.micro.

10. Espandi Tipo di destinazione e scegli **"/**.



11. (Facoltativo) Espandi Tag documento per applicare i tag delle risorse al runbook. Per Chiave tag, inserisci **Purpose** e per Valore tag, inserisci **LaunchInstanceAndCheckState**.
12. Nella sezione Fase 1, completa i passaggi seguenti.
  1. Per Nome della fase, inserisci questo nome descrittivo di fase per la prima fase dell'automazione: **LaunchEc2Instance**.
  2. Per Tipo operazione, scegli Esegui uno script (**aws:executeScript**).
  3. In Descrizione, inserisci una descrizione per la fase di automazione, ad esempio la seguente.

**\*\*About This Step\*\***

This step first launches an EC2 instance using the `aws:executeScript` action and the provided script.

4. Espandi Input.
5. In Runtime, scegli il linguaggio di runtime da utilizzare per eseguire lo script fornito.
6. Per Gestore, inserisci **launch\_instance**. Questo è il nome della funzione dichiarato nello script seguente.

 **Note**

Questo non è richiesto per. PowerShell

7. Per Script, sostituire i contenuti predefiniti con i seguenti. Assicurarsi di abbinare lo script con il valore di runtime corrispondente.

Python

```
def launch_instance(events, context):
 import boto3
 ec2 = boto3.client('ec2')

 image_id = events['image_id']
 tag_value = events['tag_value']
 instance_type = events['instance_type']

 tag_config = {'ResourceType': 'instance', 'Tags': [{'Key': 'Name',
 'Value': tag_value}]}
```

```

 res = ec2.run_instances(ImageId=image_id, InstanceType=instance_type,
MaxCount=1, MinCount=1, TagSpecifications=[tag_config])

 instance_id = res['Instances'][0]['InstanceId']

 print('[INFO] 1 EC2 instance is successfully launched', instance_id)

 return { 'InstanceId' : instance_id }

```

## PowerShell

```

Install-Module AWS.Tools.EC2 -Force
Import-Module AWS.Tools.EC2

$payload = $env:InputPayload | ConvertFrom-Json

$imageid = $payload.image_id

$tagvalue = $payload.tag_value

$instanceType = $payload.instance_type

$type = New-Object Amazon.EC2.InstanceType -ArgumentList $instanceType

$resource = New-Object Amazon.EC2.ResourceType -ArgumentList 'instance'

$tag = @{'Key'='Name';Value=$tagValue}

$tagSpecs = New-Object Amazon.EC2.Model.TagSpecification

$tagSpecs.ResourceType = $resource

$tagSpecs.Tags.Add($tag)

$res = New-EC2Instance -ImageId $imageId -MinCount 1 -MaxCount 1 -
InstanceType $type -TagSpecification $tagSpecs

return @{'InstanceId'=$res.Instances.InstanceId}

```

8. Espandi Input aggiuntivi.
9. Per Nome di input, scegli InputPayload. Per Valore di input, inserisci i seguenti dati YAML.

```
image_id: "{{ imageId }}"
```

```
tag_value: "{{ tagValue }}"
instance_type: "{{ instanceType }}"
```

13. Espandi Output ed effettua le seguenti operazioni:

- In Nome, inserisci **payload**.
- Per Selettore, inserisci **\$.Payload**.
- In Tipo, scegli **StringMap**.

14. Scegli Aggiungi fase per aggiungere una seconda fase al runbook. La seconda fase interroga lo stato dell'istanza avviata nella fase 1 e attende fino a quando lo stato restituito è ok.

15. Nella sezione Fase 2 effettua le seguenti operazioni.

1. Per Nome fase, inserisci questo nome descrittivo per la seconda fase dell'automazione:  
**WaitForInstanceStatusOk**.
2. Per Tipo operazione, scegli Esegui uno script (**aws:executeScript**).
3. In Descrizione, inserisci una descrizione per la fase di automazione, ad esempio la seguente.

**\*\*About This Step\*\***

The script continuously polls the instance status check value for the instance launched in Step 1 until the ``ok`` status is returned.

4. In Runtime, scegli il linguaggio di runtime da utilizzare per l'esecuzione dello script fornito.
5. Per Gestore, inserisci **poll\_instance**. Questo è il nome della funzione dichiarato nello script seguente.

 **Note**

Questo non è richiesto per PowerShell.

6. Per Script, sostituire i contenuti predefiniti con i seguenti. Assicurarsi di abbinare lo script con il valore di runtime corrispondente.

Python

```
def poll_instance(events, context):
 import boto3
 import time
```

```
ec2 = boto3.client('ec2')

instance_id = events['InstanceId']

print('[INFO] Waiting for instance status check to report ok',
instance_id)

instance_status = "null"

while True:
 res = ec2.describe_instance_status(InstanceIds=[instance_id])

 if len(res['InstanceStatuses']) == 0:
 print("Instance status information is not available yet")
 time.sleep(5)
 continue

 instance_status = res['InstanceStatuses'][0]['InstanceStatus']
['Status']

 print('[INFO] Polling to get status of the instance', instance_status)

 if instance_status == 'ok':
 break

 time.sleep(10)

return {'Status': instance_status, 'InstanceId': instance_id}
```

## PowerShell

```
Install-Module AWS.Tools.EC2 -Force

$inputPayload = $env:InputPayload | ConvertFrom-Json

$instanceId = $inputPayload.payload.InstanceId

$status = Get-EC2InstanceStatus -InstanceId $instanceId

while ($status.Status.Status -ne 'ok'){
 Write-Host 'Polling get status of the instance', $instanceId
```

```
Start-Sleep -Seconds 5

$status = Get-EC2InstanceStatus -InstanceId $instanceId
}

return @{Status = $status.Status.Status; InstanceId = $instanceId}
```

7. Espandi Input aggiuntivi.

8. Per Nome di input, scegli InputPayload. Per Valore di input, inserisci quanto segue:

```
{{ LaunchEc2Instance.payload }}
```

16. Scegliere Create automation (Crea automazione) per salvare il runbook.

## Utilizzo di script nei runbook

I runbook di automazione supportano l'esecuzione di script come parte dell'automazione.

L'automazione è uno strumento di AWS Systems Manager. Utilizzando i runbook, è possibile eseguire script direttamente in AWS senza dover creare un ambiente di calcolo separato per eseguire gli script. Poiché i runbook possono eseguire passaggi di script insieme ad altri tipi di fasi di automazione, ad esempio le approvazioni, è possibile intervenire manualmente in situazioni critiche o ambigue. Puoi inviare l'output delle `aws:executeScript` azioni nei tuoi runbook ad Amazon Logs. CloudWatch Per ulteriori informazioni, consulta [Uscita dell'azione Logging Automation con Logs CloudWatch](#).

## Autorizzazioni per l'utilizzo di runbook

Per utilizzare un runbook, Systems Manager deve utilizzare le autorizzazioni di un ruolo AWS Identity and Access Management (IAM). Il metodo utilizzato dal servizio di automazione per stabilire quali autorizzazioni del ruolo utilizzare dipende da alcuni fattori e dal fatto che una fase utilizza o meno l'operazione `aws:executeScript`.

Per i runbook che non utilizzano `aws:executeScript`, il servizio di automazione utilizza una delle due fonti di autorizzazione:

- Le autorizzazioni di un ruolo di servizio IAM, o ruolo presunto, specificate nel runbook o passate come parametro.
- Se non viene specificato alcun ruolo di servizio IAM, le autorizzazioni dell'utente che ha avviato l'automazione.

Quando una fase di un runbook include l'aws:executeScriptazione, tuttavia, è sempre richiesto un ruolo di servizio IAM (Assume role) se il Python o PowerShell lo script specificato per l'azione richiama qualsiasi operazione API. AWS Il servizio di automazione verifica questo ruolo nell'ordine seguente:

- Le autorizzazioni di un ruolo di servizio IAM, o ruolo presunto, specificate nel runbook o passate come parametro.
- Se non viene trovato alcun ruolo, Automation tenta di eseguire il Python o PowerShell lo script specificato aws:executeScript senza alcuna autorizzazione. Se lo script chiama un'operazione AWS API (ad esempio l'operazione Amazon EC2CreateImage) o tenta di agire su una AWS risorsa (come un'istanza EC2), il passaggio contenente lo script ha esito negativo e Systems Manager restituisce un messaggio di errore che segnala l'errore.

### Aggiunta di script ai runbook

È possibile aggiungere script ai runbook includendo lo script in linea come parte di una fase nel runbook. È inoltre possibile allegare script al runbook caricando gli script dal computer locale o specificando un bucket di Amazon Simple Storage Service (Amazon S3) in cui si trovano gli script. Al termine di una fase che esegue uno script, l'output dello script è disponibile come oggetto JSON, che è possibile utilizzare come input per le fasi successive nel runbook. Per ulteriori informazioni sull'operazione aws:executeScript e su come utilizzare gli allegati per gli script, consulta [aws:ExecuteScript – Esegue uno script](#).

### Vincoli di script per i runbook

I runbook applicano un limite di cinque file allegati. Gli script possono essere sotto forma di script Python (.py), script PowerShell Core (.ps1) o allegati come contenuti all'interno di un file .zip.

### Utilizzo di istruzioni condizionali nei runbook

Per impostazione predefinita, le fasi definite nella sezione mainSteps di un runbook vengono eseguite in ordine sequenziale. Al completamento di un'operazione viene avviata l'esecuzione dell'operazione successiva specificata nella sezione mainSteps. Inoltre, se l'esecuzione di un'operazione ha esito negativo, l'intera automazione avrà esito negativo (per impostazione predefinita). È possibile utilizzare l'operazione di automazione aws:branch e le opzioni disponibili nel runbook descritte in questa sezione per creare automazioni che eseguono il branching condizionale. Ciò significa che è possibile creare automazioni che passano a una fase diversa dopo aver valutato le diverse scelte disponibili o che rispondono in modo dinamico alle modifiche in

seguito al completamento di una fase. Ecco un elenco di opzioni che è possibile utilizzare per creare automazioni dinamiche:

- **aws:branch**: questa azione di automazione consente di creare un'automazione dinamica che valuta più scelte in un unico passaggio e quindi passa a una fase diversa del runbook in base ai risultati di tale valutazione.
- **nextStep**: questa opzione specifica la successiva fase in un'automazione da elaborare dopo il completamento di una fase.
- **isEnd**: questa opzione arresta l'automazione alla fine di una fase specifica. Il valore predefinito di questa opzione è "false".
- **isCritical**: questa opzione designa una fase come fase critica per il corretto completamento dell'automazione. Se una fase con questa definizione ha esito negativo, il servizio di automazione restituisce come stato finale dell'automazione il valore Failed. Il valore predefinito per questa opzione è true.
- **onFailure**: questa opzione indica se, in caso di errore, l'automazione deve interrompersi, continuare o passare a un'altra fase. Il valore predefinito di questa opzione è "abort".

Nella sezione seguente viene descritto l'operazione di automazione `aws:branch`. Per ulteriori informazioni sulle opzioni `nextStep`, `isEnd`, `isCritical` e `onFailure`, consulta [Esempio aws:branch runbooks](#).

### Utilizzo dell'azione `aws:branch`

L'operazione `aws:branch` rende disponibile la maggior parte delle opzioni di branching condizionale per le automazioni. Come indicato in precedenza, questa operazione consente all'automazione di valutare più condizioni in un'unica fase e quindi di passare a una nuova fase in base ai risultati di tale valutazione. L'operazione `aws:branch` è simile a un'istruzione IF-ELIF-ELSE in un ambiente di programmazione.

Di seguito viene riportato un esempio YAML di una fase `aws:branch`:

```
- name: ChooseOSforCommands
 action: aws:branch
 inputs:
 Choices:
 - NextStep: runPowerShellCommand
 Variable: "{{GetInstance.platform}}"
 StringEquals: Windows
```

```
- NextStep: runShellCommand
 Variable: "{{GetInstance.platform}}"
 StringEquals: Linux
Default:
 PostProcessing
```

Quando per una fase viene specificata l'operazione `aws:branch`, è necessario specificare l'elemento `Choices` che l'automazione deve valutare. L'automazione può valutare l'elemento `Choices` in base al valore di un parametro specificato nella sezione `Parameters` del runbook. L'automazione può inoltre valutare l'elemento `Choices` in base all'output di una fase precedente.

L'automazione valuta ogni scelta utilizzando un'espressione booleana. Se la valutazione stabilisce che la prima scelta abbia il valore `true`, l'automazione passa alla fase definita per tale scelta. Se la valutazione stabilisce che la prima scelta abbia il valore `false`, l'automazione valuta la scelta successiva. Se la fase include tre o più elementi `Choices`, l'automazione valuta ogni scelta in ordine sequenziale finché la valutazione di una scelta non restituisce `true`. L'automazione passa quindi alla fase definita per la scelta di tipo `true`.

Se nessuna delle `Choices` restituisce `true`, l'automazione controlla se la fase contiene un valore `Default`. Un valore `Default` definisce una fase a cui l'automazione deve passare se nessuna delle scelte restituisce `true`. Se non è stato specificato alcun valore di `Default` per la fase, l'automazione elabora la fase successiva nel runbook.

Ecco un `aws:branch` passaggio in YAML chiamato `chooseOSfromParameter`. La fase include due elementi `Choices`: (`NextStep: runWindowsCommand`) e (`NextStep: runLinuxCommand`). L'automazione valuta questi elementi `Choices` per determinare il comando da eseguire per il sistema operativo appropriato. L'elemento `Variable` per ciascuna scelta usa `{{OSName}}`, ovvero un parametro che l'autore del runbook ha definito nella sezione `Parameters` del runbook.

```
mainSteps:
- name: chooseOSfromParameter
 action: aws:branch
 inputs:
 Choices:
 - NextStep: runWindowsCommand
 Variable: "{{OSName}}"
 StringEquals: Windows
 - NextStep: runLinuxCommand
 Variable: "{{OSName}}"
 StringEquals: Linux
```



Ecco un `aws:branch` passaggio in YAML chiamato `chooseOSfromOutput`. La fase include due elementi `Choices`: (`NextStep: runPowerShellCommand`) e (`NextStep: runShellCommand`). L'automazione valuta questi elementi `Choices` per determinare il comando da eseguire per il sistema operativo appropriato. L'elemento `Variable` per ciascuna scelta usa `{{GetInstance.platform}}`, ovvero l'output da una fase precedente nel runbook. Questo esempio include anche un'opzione denominata `Default`. Se l'automazione valuta entrambi gli elementi `Choices` e nessuna delle due scelte restituisce `true`, l'automazione passa alla fase denominata `PostProcessing`.

```
mainSteps:
- name: chooseOSfromOutput
 action: aws:branch
 inputs:
 Choices:
 - NextStep: runPowerShellCommand
 Variable: "{{GetInstance.platform}}"
 StringEquals: Windows
 - NextStep: runShellCommand
 Variable: "{{GetInstance.platform}}"
 StringEquals: Linux
 Default:
 PostProcessing
```

## Creare una fase **aws:branch** in un runbook

Quando in un runbook viene creata una fase `aws:branch`, viene definito l'elemento `Choices` che l'automazione deve valutare per determinare a quale fase successiva deve passare. Come specificato precedentemente, gli elementi `Choices` vengono valutati utilizzando un'espressione booleana. Ogni scelta deve definire le seguenti opzioni:

- `NextStep`: La fase successiva del runbook da elaborare se la scelta designata è `true`
- `Variable`: specifica il nome di un parametro definito nella sezione `Parameters` del runbook, una variabile definita nella sezione `Variables`, oppure specifica un oggetto di output da una fase precedente.

Specifica i valori delle variabili utilizzando il formato seguente.

`Variable: "{{variable name}}"`

Specifica i valori dei parametri utilizzando il formato seguente.

Variable: "{{*parameter name*}}"

Specificare le variabili degli oggetti di output utilizzando il formato seguente:

Variable: "{{*previousStepName.outputName*}}"

 Note

La creazione della variabile di output è descritta in dettaglio nella sezione successiva, [Informazioni sulla creazione della variabile di output](#).

- Operation: i criteri utilizzati per valutare la scelta, ad esempio StringEquals: Linux. L'operazione aws:branch supporta le operazioni seguenti:

Operazioni di stringa

- StringEquals
- EqualsIgnoreCase
- StartsWith
- EndsWith
- Contiene

Operazioni numeriche

- NumericEquals
- NumericGreater
- NumericLesser
- NumericGreaterOrEquals
- NumericLesser
- NumericLesserOrEquals

Operazioni booleane

- BooleanEquals

**⚠ Important**

Quando si crea un runbook, il sistema convalida ogni operazione nel runbook. Se un'operazione non è supportata, il sistema restituisce un errore quando si tenta di creare il runbook.

- Default: specificare una fase di fallback (alternativa) a cui l'automazione deve passare, se nessuno degli elementi Choices restituisce true.

**ℹ Note**

Se non si desidera specificare un valore Default, è possibile specificare l'opzione `isEnd`. Se nessuno degli elementi Choices restituisce true e non viene specificato alcun valore Default, l'automazione viene arrestata alla fine della fase.

Utilizza i seguenti modelli per creare la fase `aws:branch` nei runbook: Sostituisci ogni *example resource placeholder* con le tue informazioni.

**YAML**

```
mainSteps:
- name: step name
 action: aws:branch
 inputs:
 Choices:
 - NextStep: step to jump to if evaluation for this choice is true
 Variable: "{{parameter name or output from previous step}}"
 Operation type: Operation value
 - NextStep: step to jump to if evaluation for this choice is true
 Variable: "{{parameter name or output from previous step}}"
 Operation type: Operation value
 Default:
 step to jump to if all choices are false
```

**JSON**

```
{
 "mainSteps":[
 {
```

```

 "name": "a name for the step",
 "action": "aws:branch",
 "inputs": {
 "Choices": [
 {
 "NextStep": "step to jump to if evaluation for this choice is
true",
 "Variable": "{{parameter name or output from previous step}}",
 "Operation type": "Operation value"
 },
 {
 "NextStep": "step to jump to if evaluation for this choice is
true",
 "Variable": "{{parameter name or output from previous step}}",
 "Operation type": "Operation value"
 }
],
 "Default": "step to jump to if all choices are false"
 }
]
}

```

## Informazioni sulla creazione della variabile di output

Per creare una scelta `aws:branch` che fa riferimento all'output restituito da una fase precedente, è necessario identificare il nome della fase precedente e il nome del campo di output. È quindi possibile combinare i nomi della fase e del campo utilizzando il formato seguente.

Variable: "`{{previousStepName.outputName}}`"

Ad esempio, la prima fase dell'esempio riportato di seguito è denominata `GetInstance`. In `outputs` è presente un campo denominato `platform`. Nella seconda fase (`ChooseOSforCommands`), l'autore vuole fare riferimento all'output del campo "platform" come variabile. Per creare la variabile, è sufficiente combinare il nome del passaggio (`GetInstance`) e il nome del campo di output (piattaforma) per creare `Variable: "{{GetInstance.platform}}"`.

```

mainSteps:
- Name: GetInstance
 action: aws:executeAwsApi
 inputs:
 Service: ssm

```

```

 Api: DescribeInstanceInformation
 Filters:
 - Key: InstanceIds
 Values: ["{{ InstanceId }}"]
 outputs:
 - Name: myInstance
 Selector: "$.InstanceInformationList[0].InstanceId"
 Type: String
 - Name: platform
 Selector: "$.InstanceInformationList[0].PlatformType"
 Type: String
- name: ChooseOSforCommands
 action: aws:branch
 inputs:
 Choices:
 - NextStep: runPowerShellCommand
 Variable: "{{GetInstance.platform}}"
 StringEquals: Windows
 - NextStep: runShellCommand
 Variable: "{{GetInstance.platform}}"
 StringEquals: Linux
 Default:
 Sleep

```

Ecco un esempio che mostra come *"Variable": "{{ describeInstance.Platform }}"* viene creata dal passaggio precedente e dall'output.

```

- name: describeInstance
 action: aws:executeAwsApi
 onFailure: Abort
 inputs:
 Service: ec2
 Api: DescribeInstances
 InstanceIds:
 - "{{ InstanceId }}"
 outputs:
 - Name: Platform
 Selector: "$.Reservations[0].Instances[0].Platform"
 Type: String
 nextStep: branchOnInstancePlatform
- name: branchOnInstancePlatform
 action: aws:branch
 inputs:

```

```
Choices:
- NextStep: runEC2RescueForWindows
 Variable: "{{ describeInstance.Platform }}"
 StringEquals: windows
Default: runEC2RescueForLinux
```

## Esempio **aws:branch** runbooks

Di seguito sono elencati alcuni runbook di esempio che utilizzano **aws:branch**.

Esempio 1: utilizzo di **aws:branch** con una variabile di output per eseguire comandi in base al tipo di sistema operativo

Nella prima fase di questo esempio (**GetInstance**), l'autore del runbook utilizza l'operazione **aws:executeAwsApi** per chiamare l'operazione API **ssm DescribeInstanceInformation**. L'autore usa questa operazione per determinare il tipo di sistema operativo utilizzato da un'istanza. L'operazione **aws:executeAwsApi** restituisce l'ID dell'istanza e il tipo di piattaforma.

Nella seconda fase (**ChooseOSforCommands**) l'autore usa l'operazione **aws:branch** con due elementi **Choices** (**NextStep: runPowerShellCommand**) e (**NextStep: runShellCommand**). L'automazione valuta il sistema operativo dell'istanza utilizzando l'output della fase precedente (**Variable: "{{GetInstance.platform}}"**). L'automazione passa a una fase relativa al sistema operativo designato.

```

schemaVersion: '0.3'
assumeRole: "{{AutomationAssumeRole}}"
parameters:
 AutomationAssumeRole:
 default: ""
 type: String
mainSteps:
- name: GetInstance
 action: aws:executeAwsApi
 inputs:
 Service: ssm
 Api: DescribeInstanceInformation
 outputs:
- Name: myInstance
 Selector: "$.InstanceInformationList[0].InstanceId"
 Type: String
```

```
- Name: platform
 Selector: "$.InstanceInformationList[0].PlatformType"
 Type: String
- name: ChooseOSforCommands
 action: aws:branch
 inputs:
 Choices:
 - NextStep: runPowerShellCommand
 Variable: "{{GetInstance.platform}}"
 StringEquals: Windows
 - NextStep: runShellCommand
 Variable: "{{GetInstance.platform}}"
 StringEquals: Linux
 Default:
 Sleep
- name: runShellCommand
 action: aws:runCommand
 inputs:
 DocumentName: AWS-RunShellScript
 InstanceIds:
 - "{{GetInstance.myInstance}}"
 Parameters:
 commands:
 - ls
 isEnd: true
- name: runPowerShellCommand
 action: aws:runCommand
 inputs:
 DocumentName: AWS-RunPowerShellScript
 InstanceIds:
 - "{{GetInstance.myInstance}}"
 Parameters:
 commands:
 - ls
 isEnd: true
- name: Sleep
 action: aws:sleep
 inputs:
 Duration: PT3S
```

Esempio 2: utilizzo di **aws:branch** con una variabile di parametro per eseguire comandi in base al tipo di sistema operativo

L'autore del runbook definisce diverse opzioni di parametro all'inizio del documento nella sezione `parameters`. Uno dei parametri è denominato `OperatingSystemName`. Nella prima fase (`ChooseOS`) l'autore usa l'operazione `aws:branch` con due `Choices` (`NextStep: runWindowsCommand`) e (`NextStep: runLinuxCommand`). La variabile per questi elementi `Choices` fa riferimento all'opzione di parametro specificato nella sezione parametri (`Variable: "{{OperatingSystemName}}"`). Quando l'utente esegue questo runbook, deve specificare un valore di runtime per `OperatingSystemName`. L'automazione utilizza il parametro di runtime durante la valutazione di `Choices`. L'automazione passa a una fase per il sistema operativo designato in base al parametro di runtime specificato per `OperatingSystemName`.

```

schemaVersion: '0.3'
assumeRole: "{{AutomationAssumeRole}}"
parameters:
 AutomationAssumeRole:
 default: ""
 type: String
 OperatingSystemName:
 type: String
 LinuxInstanceId:
 type: String
 WindowsInstanceId:
 type: String
mainSteps:
- name: ChooseOS
 action: aws:branch
 inputs:
 Choices:
 - NextStep: runWindowsCommand
 Variable: "{{OperatingSystemName}}"
 StringEquals: windows
 - NextStep: runLinuxCommand
 Variable: "{{OperatingSystemName}}"
 StringEquals: linux
 Default:
 Sleep
- name: runLinuxCommand
 action: aws:runCommand
 inputs:
 DocumentName: "AWS-RunShellScript"
 InstanceIds:
 - "{{LinuxInstanceId}}"
```



```
Parameters:
 commands:
 - ls
 isEnd: true
- name: runWindowsCommand
 action: aws:runCommand
 inputs:
 DocumentName: "AWS-RunPowerShellScript"
 InstanceIds:
 - "{{WindowsInstanceId}}"
 Parameters:
 commands:
 - date
 isEnd: true
- name: Sleep
 action: aws:sleep
 inputs:
 Duration: PT3S
```

## Creazione di automazioni con branching complesso con operatori

Puoi creare automazioni con branching complesso utilizzando gli operatori And, Or e Not nelle fasi `aws:branch`.

### Operatore "And"

Utilizza l'operatore And quando vuoi che più variabili restituiscano `true` per una scelta. Nell'esempio seguente la prima scelta valuta se un'istanza è `running` e usa il sistema operativo `Windows`. Se la valutazione di entrambe le variabili restituisce `"true"`, l'automazione passa alla fase `runPowerShellCommand`. Se una o più variabili restituisce `false`, l'automazione valuta le variabili della seconda scelta.

```
mainSteps:
- name: switch2
 action: aws:branch
 inputs:
 Choices:
 - And:
 - Variable: "{{GetInstance.pingStatus}}"
 StringEquals: running
 - Variable: "{{GetInstance.platform}}"
 StringEquals: Windows
 NextStep: runPowerShellCommand
```

```

- And:
 - Variable: "{{GetInstance.pingStatus}}"
 StringEquals: running
 - Variable: "{{GetInstance.platform}}"
 StringEquals: Linux
 NextStep: runShellCommand
Default:
 sleep3

```

## Operatore "Or"

Utilizza l'operatore `Or` quando vuoi che una qualsiasi di più variabili restituisca `"true"` per una scelta. Nell'esempio seguente la prima scelta valuta se una stringa di parametro è `Windows` e se l'output da una fase AWS Lambda è `"true"`. Se la valutazione determina che una di queste variabili restituisce `"true"`, l'automazione passa alla fase `RunPowerShellCommand`. Se entrambe le variabili restituiscono `"false"`, l'automazione valuta le variabili della seconda scelta.

```

- Or:
 - Variable: "{{parameter1}}"
 StringEquals: Windows
 - Variable: "{{BooleanParam1}}"
 BooleanEquals: true
 NextStep: RunPowershellCommand
- Or:
 - Variable: "{{parameter2}}"
 StringEquals: Linux
 - Variable: "{{BooleanParam2}}"
 BooleanEquals: true
 NextStep: RunShellScript

```

## Operatore "Not"

Utilizza l'operatore `Not` quando vuoi passare a una fase definita quando una variabile non restituisce `"true"`. Nell'esempio seguente la prima scelta valuta se una stringa di parametro è `Not Linux`. Se la valutazione determina che la variabile non è `Linux`, l'automazione passa alla fase `sleep2`. Se la valutazione della prima scelta determina che è `Linux`, l'automazione valuta la scelta successiva.

```

mainSteps:
- name: switch
 action: aws:branch
 inputs:

```

```

Choices:
- NextStep: sleep2
 Not:
 Variable: "{{testParam}}"
 StringEquals: Linux
- NextStep: sleep1
 Variable: "{{testParam}}"
 StringEquals: Windows
Default:
 sleep3

```

## Esempi di utilizzo delle opzioni condizionali

In questa sezione sono riportati diversi esempi di come utilizzare le opzioni dinamiche in un runbook. Ogni esempio in questa sezione estende le funzionalità del runbook seguente. Il runbook include due operazioni. La prima operazione è denominata `InstallMsiPackage`. Utilizza l'operazione `aws:runCommand` per installare un'applicazione su un'istanza di Windows Server. La seconda operazione è denominata `TestInstall`. Utilizza l'operazione `aws:invokeLambdaFunction` per eseguire un test dell'applicazione installata se l'applicazione è stata installata correttamente. La fase una specifica `onFailure: Abort`. Ciò significa che se l'applicazione non è stata installata correttamente, l'automazione viene interrotta prima della fase due.

### Esempio 1: runbook con due operazioni lineari

```

schemaVersion: '0.3'
description: Install MSI package and run validation.
assumeRole: "{{automationAssumeRole}}"
parameters:
 automationAssumeRole:
 type: String
 description: "(Required) Assume role."
 packageName:
 type: String
 description: "(Required) MSI package to be installed."
 instanceIds:
 type: String
 description: "(Required) Comma separated list of instances."
mainSteps:
- name: InstallMsiPackage
 action: aws:runCommand
 maxAttempts: 2

```

```
onFailure: Abort
inputs:
 InstanceIds:
 - "{{instanceIds}}"
 DocumentName: AWS-RunPowerShellScript
 Parameters:
 commands:
 - msixexec /i {{packageName}}
- name: TestInstall
 action: aws:invokeLambdaFunction
 maxAttempts: 1
 timeoutSeconds: 500
 inputs:
 FunctionName: TestLambdaFunction
...
```

Creazione di un'automazione dinamica che passa a fasi diverse mediante l'opzione **onFailure**

L'esempio seguente utilizza le opzioni `onFailure: step:step name`, `nextStep` e `isEnd` per creare un'automazione dinamica. In questo esempio, se l'InstallMsiPackageazione fallisce, l'automazione passa a un'azione chiamata PostFailure (`onFailure: step:PostFailure`) per eseguire una AWS Lambda funzione per eseguire alcune azioni nel caso in cui l'installazione non riesca. Se l'installazione ha esito positivo, l'automazione passa all' TestInstall azione (). `nextStep: TestInstall` Le fasi TestInstall e PostFailure usano entrambe l'opzione `isEnd` (`isEnd: true`) in modo tale che l'automazione termini al completamento di una di queste due fasi.

#### Note

L'uso dell'opzione `isEnd` nell'ultima fase della sezione `mainSteps` è facoltativo. Se l'ultima fase non passa ad altre fasi, l'automazione viene interrotta dopo l'esecuzione dell'operazione nell'ultima fase.

Esempio 2: un'automazione dinamica che passa a diverse fasi

```
mainSteps
- name: InstallMsiPackage
 action: aws:runCommand
 onFailure: step:PostFailure
 maxAttempts: 2
 inputs:
```

```

 InstanceIds:
 - "{{instanceIds}}"
 DocumentName: AWS-RunPowerShellScript
 Parameters:
 commands:
 - msixec /i {{packageName}}
 nextStep: TestInstall
- name: TestInstall
 action: aws:invokeLambdaFunction
 maxAttempts: 1
 timeoutSeconds: 500
 inputs:
 FunctionName: TestLambdaFunction
 isEnd: true
- name: PostFailure
 action: aws:invokeLambdaFunction
 maxAttempts: 1
 timeoutSeconds: 500
 inputs:
 FunctionName: PostFailureRecoveryLambdaFunction
 isEnd: true
...

```

#### Note

Prima di elaborare un runbook, il sistema verifica che il runbook non crei un loop infinito. Se viene rilevato un loop infinito, il servizio di automazione restituisce un errore e una traccia a forma di cerchio che evidenzia le fasi che causano il loop.

## Creazione di un'automazione dinamica che definisce le fasi critiche

È possibile specificare una fase come fase critica per il successo complessivo dell'automazione. Se una fase critica ha esito negativo, il servizio di automazione indica lo stato dell'automazione come `Failed`, anche se una o più fasi sono state eseguite correttamente. Nell'esempio seguente, l'utente identifica il `VerifyDependencies` passaggio in caso di esito negativo (). `InstallMsiPackage` onFailure: `step:VerifyDependencies` L'utente specifica che la fase `InstallMsiPackage` non è una fase critica (`isCritical: false`). In questo esempio, se l'applicazione non viene installata, il servizio di automazione elabora la fase `VerifyDependencies` per determinare se mancano una o più dipendenze; è proprio la mancanza di una dipendenza il motivo che ha causato la mancata installazione dell'applicazione.

### Esempio 3: definizione delle fasi critiche per l'automazione

```

name: InstallMsiPackage
action: aws:runCommand
onFailure: step:VerifyDependencies
isCritical: false
maxAttempts: 2
inputs:
 InstanceIds:
 - "{{instanceIds}}"
 DocumentName: AWS-RunPowerShellScript
 Parameters:
 commands:
 - msixexec /i {{packageName}}
nextStep: TestPackage
...
```

#### Utilizzo degli output delle operazioni come input

Diverse operazioni di automazione restituiscono output predefiniti. Puoi passare questi output come input ai passaggi successivi nel runbook usando il formato `{{stepName.outputName}}`. Puoi inoltre definire output personalizzati per varie operazioni di automazione nei tuoi runbook. Ciò consente di eseguire script o richiamare operazioni API per un'altra Servizi AWS volta in modo da poter riutilizzare i valori come input nelle azioni successive. I tipi di parametri nei runbook sono statici. Ciò significa che il tipo di parametro non può essere modificato dopo che è stato definito. Per definire l'output di un passaggio, completa i seguenti campi:

- Nome (obbligatorio): il nome dell'output utilizzato per fare riferimento al valore di output nei passaggi successivi.
- Selettore (obbligatorio): l'espressione JSONPath utilizzata per determinare il valore di output.
- Tipo: (facoltativo) il tipo di dati del valore restituito dal campo del selettore. I valori di tipo validi sono `String`, `Integer`, `Boolean`, `StringList`, `StringMap`, `MapList`. Il valore predefinito è `String`.

Se il valore di un output non corrisponde al tipo di dati specificato, Automation prova a convertire il tipo di dati. Ad esempio, se il valore restituito è un `Integer`, ma il `Type` specificato è `String`, allora il valore dell'output finale è un valore `String`. Sono supportati i seguenti tipi di conversione:

- I valori String possono essere convertiti in StringList, Integer e Boolean.
- I valori Integer possono essere convertiti in String, e StringList.
- I valori Boolean possono essere convertiti in String, e StringList.
- I valori StringList, IntegerList o BooleanList contenenti un elemento possono essere convertiti in StringInteger o Boolean.

Quando si utilizzano parametri o output con operazioni di automazione, il tipo di dati non può essere modificato dinamicamente all'interno dell'input di un'operazione.

Di seguito è riportato un runbook di esempio che illustra come definire gli output delle operazioni e come utilizzare tale valore come input per un'operazione successiva. I runbook eseguono le operazioni seguenti:

- Utilizza l'aws:executeAwsApi azione per richiamare l'operazione DescribeImages API Amazon EC2 per ottenere il nome di uno specifico Windows Server 2016. AMI Restituisce l'ID immagine come ImageId.
- Utilizza l'aws:executeAwsApi azione per richiamare l'operazione RunInstances API Amazon EC2 per avviare un'istanza che utilizza il ImageId passaggio precedente. Restituisce l'ID di istanza come InstanceId.
- Utilizza l' aws:waitForAwsResourceProperty azione per interrogare l'operazione dell' DescribeInstanceStatus API Amazon EC2 e attendere che l'istanza raggiunga lo stato. running Il timeout dell'operazione è pari a 60 secondi. Si verifica il timeout della fase se l'istanza non raggiunge lo stato running dopo 60 secondi dall'avvio del polling.
- Utilizza l'operazione aws:assertAwsResourceProperty per chiamare l'operazione API DescribeInstanceStatus di Amazon EC2 per affermare che l'istanza si trova nello stato running. La fase ha esito negativo se lo stato dell'istanza non è running.

```

description: Sample runbook using AWS API operations
schemaVersion: '0.3'
assumeRole: "{{ AutomationAssumeRole }}"
parameters:
 AutomationAssumeRole:
 type: String
 description: "(Optional) The ARN of the role that allows Automation to perform the
actions on your behalf."
```

```
 default: ''
 ImageName:
 type: String
 description: "(Optional) Image Name to launch EC2 instance with."
 default: "Windows_Server-2022-English-Full-Base*"
mainSteps:
- name: getImageId
 action: aws:executeAwsApi
 inputs:
 Service: ec2
 Api: DescribeImages
 Filters:
 - Name: "name"
 Values:
 - "{{ ImageName }}"
 outputs:
 - Name: ImageId
 Selector: "$.Images[0].ImageId"
 Type: "String"
- name: launchOneInstance
 action: aws:executeAwsApi
 inputs:
 Service: ec2
 Api: RunInstances
 ImageId: "{{ getImageId.ImageId }}"
 MaxCount: 1
 MinCount: 1
 outputs:
 - Name: InstanceId
 Selector: "$.Instances[0].InstanceId"
 Type: "String"
- name: waitUntilInstanceStateRunning
 action: aws:waitForAwsResourceProperty
 timeoutSeconds: 60
 inputs:
 Service: ec2
 Api: DescribeInstanceStatus
 InstanceIds:
 - "{{ launchOneInstance.InstanceId }}"
 PropertySelector: "$.InstanceStatuses[0].InstanceState.Name"
 DesiredValues:
 - running
- name: assertInstanceStateRunning
 action: aws:assertAwsResourceProperty
```



```

inputs:
 Service: ec2
 Api: DescribeInstanceStatus
 InstanceIds:
 - "{{ launchOneInstance.InstanceId }}"
 PropertySelector: "$.InstanceStatuses[0].InstanceState.Name"
 DesiredValues:
 - running
outputs:
 - "launchOneInstance.InstanceId"
 ...

```

Ciascuna delle azioni di automazione descritte in precedenza consente di chiamare un'operazione API specifica specificando lo spazio dei nomi del servizio, il nome dell'operazione API, i parametri di input e i parametri di output. Gli input vengono definiti dall'operazione API selezionata. Puoi visualizzare le operazioni API (definite anche metodi) scegliendo un servizio nel pannello di navigazione a sinistra nella pagina [Services Reference \(Informazioni di riferimento relative ai servizi\)](#). Scegliere un metodo nella sezione Client del servizio che si desidera chiamare. Ad esempio, tutte le operazioni API (metodi) per Amazon Relational Database Service (Amazon RDS) sono elencate nella seguente pagina: [Amazon RDS methods \(Metodi di Amazon RDS\)](#).

Puoi visualizzare lo schema per ciascuna operazione di automazione nelle seguenti posizioni:

- [aws:assert – Assert AwsResourceProperty AWS stato della risorsa o stato dell'evento](#)
- [aws:execute AwsApi — Chiama ed esegui AWS operazioni API](#)
- [aws:wait ForAwsResourceProperty – Attendi un AWS proprietà della risorsa](#)

Gli schemi includono le descrizioni dei campi obbligatori per l'utilizzo di ciascuna operazione.

### Utilizzo dei campi Selector/PropertySelector

Per ogni operazione di automazione è necessario specificare un output Selector (per `aws:executeAwsApi`) o un PropertySelector (per `aws:assertAwsResourceProperty` e `aws:waitForAwsResourceProperty`). Questi campi vengono utilizzati per elaborare la risposta JSON da un'operazione AWS API. Questi campi utilizzano la sintassi JSONPath.

Ecco un esempio che illustra questo concetto per l'operazione `aws:executeAwsApi`.

```

mainSteps:

```

```

- name: getImageId
 action: aws:executeAwsApi
 inputs:
 Service: ec2
 Api: DescribeImages
 Filters:
 - Name: "name"
 Values:
 - "{{ ImageName }}"
 outputs:
 - Name: ImageId
 Selector: "$.Images[0].ImageId"
 Type: "String"
 ...

```

Nella fase `aws:executeAwsApi` dell'elemento `getImageId`, l'automazione richiama l'operazione API `DescribeImages` e riceve una risposta da `ec2`. L'automazione applica quindi `Selector - "$.Images[0].ImageId"` alla risposta API e assegna il valore selezionato alla variabile di output `ImageId`. Altre fasi della stessa automazione possono utilizzare il valore di `ImageId` specificando `"{{ getImageId.ImageId }}"`.

Ecco un esempio che illustra questo concetto per l'operazione `aws:waitForAwsResourceProperty`:

```

- name: waitUntilInstanceStateRunning
 action: aws:waitForAwsResourceProperty
 # timeout is strongly encouraged for action - aws:waitForAwsResourceProperty
 timeoutSeconds: 60
 inputs:
 Service: ec2
 Api: DescribeInstanceStatus
 InstanceIds:
 - "{{ launchOneInstance.InstanceId }}"
 PropertySelector: "$.InstanceStatuses[0].InstanceState.Name"
 DesiredValues:
 - running
 ...

```

Nella fase `aws:waitForAwsResourceProperty` dell'elemento `waitUntilInstanceStateRunning`, l'automazione richiama l'operazione API `DescribeInstanceStatus` e riceve una risposta da `ec2`. L'automazione applica quindi

PropertySelector - "\$.InstanceStatuses[0].InstanceState.Name" alla risposta e verifica se il valore restituito specificato corrisponde a un valore nell'elenco DesiredValues (in questo caso running). La fase ripete il processo finché la risposta non restituisce lo stato di istanza running.

### Utilizzo della variabile JSONPath nei runbook

Un'espressione JSONPath è una stringa che inizia con «\$». utilizzato per selezionare uno o più componenti all'interno di un elemento JSON. L'elenco seguente include informazioni sugli operatori JSONPath supportati dal servizio di automazione di Systems Manager:

- Dot-notated figlio (.) : utilizzare con un oggetto JSON. Questo operatore seleziona il valore di una chiave specifica.
- Deep-scan (..) : utilizzare con un elemento JSON. Questo operatore analizza il livello dell'elemento JSON per livello e seleziona un elenco di valori con la chiave specificata. Si noti che il tipo restituito di questo operatore è sempre un array JSON. Nel contesto di un tipo di output di un'azione di automazione, l'operatore può essere uno StringList o MapList.
- Array-Index ([]): da utilizzare con un array JSON. Questo operatore recupera il valore di un indice specifico.
- Filtro ([? (**expression**)]): da utilizzare con un array JSON. Questo operatore filtra i valori dell'array JSON che corrispondono ai criteri definiti nell'espressione del filtro. Le espressioni di filtro possono utilizzare solo i seguenti operatori: ==, !=, >, <, >= o <=. La combinazione di più espressioni di filtro con AND (&&) o OR (||) non è supportata. Si noti che il tipo restituito di questo operatore è sempre un array JSON.

Per comprendere meglio gli operatori JSONPath, analizzare la seguente risposta JSON dell'operazione API ec2 DescribeInstances. Dopo questa risposta sono disponibili alcuni esempi che illustrano i vari risultati derivanti dall'applicazione di diverse espressioni JSONPath alla risposta dell'operazione API DescribeInstances.

```
{
 "NextToken": "abcdefg",
 "Reservations": [
 {
 "OwnerId": "123456789012",
 "ReservationId": "r-abcd12345678910",
 "Instances": [
 {
```

```

 "ImageId": "ami-12345678",
 "BlockDeviceMappings": [
 {
 "Ebs": {
 "DeleteOnTermination": true,
 "Status": "attached",
 "VolumeId": "vol-000000000000000"
 },
 "DeviceName": "/dev/xvda"
 }
],
 "State": {
 "Code": 16,
 "Name": "running"
 }
 },
 "Groups": []
},
{
 "OwnerId": "123456789012",
 "ReservationId": "r-12345678910abcd",
 "Instances": [
 {
 "ImageId": "ami-12345678",
 "BlockDeviceMappings": [
 {
 "Ebs": {
 "DeleteOnTermination": true,
 "Status": "attached",
 "VolumeId": "vol-111111111111111"
 },
 "DeviceName": "/dev/xvda"
 }
],
 "State": {
 "Code": 80,
 "Name": "stopped"
 }
 }
],
 "Groups": []
}
]

```

```
}
```

### Esempio JSONPath 1: recupero di una stringa specifica da una risposta JSON

JSONPath:

```
$.Reservations[0].Instances[0].ImageId
```

Returns:

```
"ami-12345678"
```

Type: String

### Esempio JSONPath 2: recupero di un valore booleano specifico da una risposta JSON

JSONPath:

```
$.Reservations[0].Instances[0].BlockDeviceMappings[0].Ebs.DeleteOnTermination
```

Returns:

```
true
```

Type: Boolean

### Esempio JSONPath 3: recupero di un valore intero specifico da una risposta JSON

JSONPath:

```
$.Reservations[0].Instances[0].State.Code
```

Returns:

```
16
```

Type: Integer

### JSONPath Esempio 4: scansiona in profondità una risposta JSON, quindi ottieni tutti i valori per as Volumeld StringList

JSONPath:

```
$.Reservations..BlockDeviceMappings..VolumeId
```

Returns:

```
[
 "vol-00000000000000",
 "vol-11111111111111"
```

```
]
```

Type: `StringList`

### JSONPath Esempio 5: ottieni un oggetto specifico come `BlockDeviceMappings` `StringMap`

JSONPath:

```
$.Reservations[0].Instances[0].BlockDeviceMappings[0]
```

Returns:

```
{
 "Ebs" : {
 "DeleteOnTermination" : true,
 "Status" : "attached",
 "VolumeId" : "vol-0000000000000000"
 },
 "DeviceName" : "/dev/xvda"
}
```

Type: `StringMap`

### JSONPath Esempio 6: scansiona in profondità una risposta JSON, quindi ottieni tutti gli oggetti `State` come `MapList`

JSONPath:

```
$.Reservations..Instances..State
```

Returns:

```
[
 {
 "Code" : 16,
 "Name" : "running"
 },
 {
 "Code" : 80,
 "Name" : "stopped"
 }
]
```

Type: `MapList`

### Esempio 7 di JSONPath: filtro per le istanze nello stato **running**

```
JSONPath:
$.Reservations..Instances[?(@.State.Name == 'running')]
```

```
Returns:
[
 {
 "ImageId": "ami-12345678",
 "BlockDeviceMappings": [
 {
 "Ebs": {
 "DeleteOnTermination": true,
 "Status": "attached",
 "VolumeId": "vol-0000000000000000"
 },
 "DeviceName": "/dev/xvda"
 }
],
 "State": {
 "Code": 16,
 "Name": "running"
 }
 }
]
```

Type: MapList

Esempio 8 di JSONPath: restituisce **ImageId** per le istanze che non si trovano nello stato **running**

```
JSONPath:
$.Reservations..Instances[?(@.State.Name != 'running')].ImageId
```

```
Returns:
[
 "ami-12345678"
]
```

Type: StringList | String

## Creazione di integrazioni webhook per Automazione

Creare un'integrazione ti permette di inviare messaggi utilizzando webhook durante un'automazione. Le integrazioni possono essere richiamate durante un'automazione utilizzando l'operazione

`aws:invokeWebhook` nel tuo runbook. Se non hai ancora creato un webhook, consulta [Creazione di webhook per integrazioni](#). Per ulteriori informazioni sulle operazioni di `aws:invokeWebhook`, consulta [aws:invokeWebhook: richiamo dell'integrazione di un webhook di Automation](#).

Come illustrato nelle procedure seguenti, puoi creare un'integrazione utilizzando la console di Systems Manager Automation o lo strumento a riga di comando desiderato.

### Creazione di integrazioni (console)

#### Creazione di un'integrazione per Automazione (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Automazione.
3. Seleziona la scheda Integrazioni.
4. Seleziona Aggiungi integrazione e scegli Webhook.
5. Inserisci i valori obbligatori e tutti i valori facoltativi che desideri includere per l'integrazione.
6. Scegli Aggiungi per creare l'integrazione.

#### Creazione di integrazioni (riga di comando)

Per creare un'integrazione utilizzando gli strumenti a riga di comando, devi creare il parametro `SecureString` obbligatorio per un'integrazione. L'automazione utilizza uno spazio dei nomi riservato `Parameter Store` per archiviare le informazioni sull'integrazione. Se crei un'integrazione utilizzando il Console di gestione AWS, Automation gestisce questo processo per te. Dopo namespace, devi specificare il tipo di integrazione che desideri creare e quindi il nome dell'integrazione. Attualmente, Automation supporta integrazioni di tipo webhook.

I campi supportati per le integrazioni di tipo webhook sono i seguenti:

- Description
- headers
- payload
- URL

### Prima di iniziare



Se non l'hai già fatto, installa e configura AWS Command Line Interface (AWS CLI) o AWS Strumenti per PowerShell. Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

Per creare un'integrazione per Automazione (riga di comando)

- Esegui i comandi seguenti per creare il parametro SecureString obbligatorio per un'integrazione. Sostituisci ogni *example resource placeholder* con le tue informazioni. Il namespace di /d9d01087-4a3f-49e0-b0b4-d568d7826553/ssm/integrations/webhook/ è riservato in Parameter Store per le integrazioni. Il nome del tuo parametro deve utilizzare questo namespace seguito dal nome dell'integrazione. Ad esempio, /d9d01087-4a3f-49e0-b0b4-d568d7826553/ssm/integrations/webhook/*myWebhookIntegration*.

## Linux & macOS

```
aws ssm put-parameter \
 --name "/d9d01087-4a3f-49e0-b0b4-d568d7826553/ssm/integrations/
webhook/myWebhookIntegration" \
 --type "SecureString" \
 --data-type "aws:ssm:integration" \
 --value '{"description": "My first webhook integration for Automation.",
"url": "myWebHookURL"}'
```

## Windows

```
aws ssm put-parameter ^
 --name "/d9d01087-4a3f-49e0-b0b4-d568d7826553/ssm/integrations/
webhook/myWebhookIntegration" ^
 --type "SecureString" ^
 --data-type "aws:ssm:integration" ^
 --value "{\"description\": \"My first webhook integration for Automation.\",
\"url\": \"myWebHookURL\"}"
```

## PowerShell

```
Write-SSMParameter `
 -Name "/d9d01087-4a3f-49e0-b0b4-d568d7826553/ssm/integrations/
webhook/myWebhookIntegration" `
 -Type "SecureString"
 -DataType "aws:ssm:integration"
```

```
-Value '{"description": "My first webhook integration for Automation.",
"url": "myWebHookURL"}'
```

## Creazione di webhook per integrazioni

Quando crei webhook con il provider, nota quanto segue:

- Il protocollo deve essere HTTPS.
- Sono supportate le intestazioni delle richieste personalizzate.
- È possibile specificare un corpo della richiesta predefinito.
- Il corpo della richiesta predefinito può essere ignorato quando viene richiamata un'integrazione utilizzando l'operazione `aws:invokeWebhook`.

## Gestione dei timeout nei runbook

La proprietà `timeoutSeconds` è condivisa da tutte le operazioni di automazione. Puoi utilizzare questa proprietà per specificare il valore di timeout di esecuzione per un'operazione. Inoltre, puoi modificare il modo in cui un timeout dell'operazione influisce sull'automazione e sullo stato di esecuzione generale. Puoi eseguire questa operazione definendo anche le proprietà condivise `onFailure` e `isCritical` per un'operazione.

Ad esempio, a seconda del caso d'uso, è possibile che l'automazione continui con un'operazione diversa e non influisca sullo stato generale dell'automazione se si verifica il timeout di un'operazione. In questo esempio, specifichi il tempo di attesa prima del timeout dell'operazione utilizzando la proprietà `timeoutSeconds`. Quindi specifichi l'operazione, o la fase, che l'automazione deve eseguire in caso di timeout. Specifica un valore utilizzando il formato `step: step name` per la proprietà `onFailure` anziché il valore predefinito `Abort`. Per impostazione predefinita, se si verifica il timeout di un'operazione, lo stato di esecuzione di automazione è `Timed Out`. Per evitare che un timeout influisca sullo stato di esecuzione di automazione, specifica `false` per la proprietà `isCritical`.

Nell'esempio seguente viene illustrato come definire le proprietà condivise per un'operazione descritta in questo scenario.

## YAML

```
- name: verifyImageAvailability
 action: 'aws:waitForAwsResourceProperty'
```

```
timeoutSeconds: 600
isCritical: false
onFailure: 'step:getCurrentImageState'
inputs:
 Service: ec2
 Api: DescribeImages
 ImageIds:
 - '{{ createImage.newImageId }}'
 PropertySelector: '$.Images[0].State'
 DesiredValues:
 - available
nextStep: copyImage
```

## JSON

```
{
 "name": "verifyImageAvailability",
 "action": "aws:waitForAwsResourceProperty",
 "timeoutSeconds": 600,
 "isCritical": false,
 "onFailure": "step:getCurrentImageState",
 "inputs": {
 "Service": "ec2",
 "Api": "DescribeImages",
 "ImageIds": [
 "{{ createImage.newImageId }}"
],
 "PropertySelector": "$.Images[0].State",
 "DesiredValues": [
 "available"
]
 },
 "nextStep": "copyImage"
}
```

Per ulteriori informazioni sulle proprietà condivise da tutte le operazioni di automazione, consulta [Proprietà condivise da tutte le operazioni](#).

## Riferimento al runbook dell'Automazione Systems Manager

Per aiutarti a iniziare rapidamente, AWS Systems Manager fornisce runbook predefiniti. Questi runbook sono gestiti da Amazon Web Services e Supporto AWS. [AWS Config II Runbook Reference](#)

descrive ciascuno dei runbook predefiniti forniti da Systems Manager,, e. Supporto AWS Config Per ulteriori informazioni, consulta [Documentazione di riferimento al runbook Automazione Systems Manager](#).

## Esercitazioni

I seguenti tutorial ti aiutano a utilizzare l' AWS Systems Manager automazione per affrontare i casi d'uso più comuni. Questi tutorial illustrano come utilizzare i runbook personali, quelli predefiniti forniti da Automazione e altri strumenti di Systems Manager con altri Servizi AWS.

Questa sezione contiene gli argomenti seguenti.

- [Aggiorna un Linux AMI](#)
- [Aggiornamento di un' Windows Server AMI](#)
- [Utilizzo Supporto AWS runbook self-service](#)
- [Ripristino di password e chiavi SSH sulle istanze EC2](#)

### Aggiornamento in corso AMI

I tutorial seguenti illustrano come aggiornare le Amazon Machine Image (AMIs) per includere le patch più recenti.

#### Aggiorna un Linux AMI

Questa procedura guidata di Automazione Systems Manager illustra come utilizzare la console o la AWS CLI e il runbook `AWS-UpdateLinuxAmi` per aggiornare un'AMI Linux con le patch più recenti dei pacchetti specificati. L'automazione è uno strumento di AWS Systems Manager. Il runbook `AWS-UpdateLinuxAmi` automatizza l'installazione anche di altri pacchetti e configurazioni specifici del sito. È possibile aggiornare un'ampia gamma di distribuzioni Linux utilizzando questa procedura guidata, tra cui Ubuntu Server, Red Hat Enterprise Linux (RHEL) oppure Amazon Linux AMIs. Per un elenco completo delle versioni Linux supportate, consulta [Patch Manager prerequisiti](#).

Il `AWS-UpdateLinuxAmi` runbook consente di automatizzare le attività di manutenzione delle immagini senza dover creare il runbook in JSON o YAML. È possibile utilizzare il runbook `AWS-UpdateLinuxAmi` per eseguire i tipi di processi seguenti.

- Aggiornamento di tutti i pacchetti di distribuzione e del software Amazon su Amazon Linux, Red Hat Enterprise Linux o Ubuntu Server Amazon Machine Image (AMI). Questo è il comportamento predefinito del runbook.

- Effettua l'installazione AWS Systems Manager SSM Agent su un'immagine esistente per abilitare gli strumenti di Systems Manager, ad esempio l'esecuzione di comandi remoti tramite AWS Systems Manager Run Command o la raccolta dell'inventario del software tramite Inventory.
- Installazione di pacchetti software aggiuntivi.

## Prima di iniziare

Prima di iniziare a lavorare con i runbook, configura i ruoli e, facoltativamente, EventBridge per l'automazione. Per ulteriori informazioni, consulta [Configurazione del servizio di automazione](#). Questa procedura dettagliata richiede inoltre di specificare il nome di un profilo di istanza AWS Identity and Access Management (IAM). Per ulteriori informazioni sulla creazione di un profilo dell'istanza IAM, consulta la pagina [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#).

Il runbook `AWS-UpdateLinuxAmi` accetta i parametri di input seguenti.

| Parametro              | Tipo    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SourceAmiId            | Stringa | (Obbligatorio) L'ID origine di AMI.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IamInstanceProfileName | Stringa | (Obbligatorio) Il nome del ruolo del profilo dell'istanza IAM creato in <a href="#">Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager</a> . Il ruolo del profilo dell'istanza concede le autorizzazioni al servizio di automazione per eseguire operazioni sulle istanze, ad esempio l'esecuzione di comandi o l'avvio e l'arresto dei servizi. Il runbook utilizza solo il nome del ruolo del profilo dell'istanza. Se si specifica l'Amazon Resource |

| Parametro            | Tipo    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      |         | Name (ARN), l'automazione ha esito negativo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| AutomationAssumeRole | Stringa | (Obbligatorio) Nome del ruolo di servizio IAM creato in <a href="#">Configurazione del servizio di automazione</a> . Il ruolo di servizio (definito anche ruolo presunto) concede l'autorizzazione al servizio di automazione di assumere il ruolo IAM e di eseguire operazioni a nome dell'utente. Ad esempio, il ruolo di servizio permette al servizio di automazione di creare una nuova AMI quando viene eseguita l'operazione <code>aws:createImage</code> in un runbook. Per questo parametro, è necessario specificare l'ARN completo. |
| TargetAmiName        | Stringa | (Facoltativo) Nome della nuova AMI dopo la creazione. Il nome predefinito è una stringa generata dal sistema contenente l'ID dell'AMI di origine e la data/ora di creazione.                                                                                                                                                                                                                                                                                                                                                                   |

| Parametro        | Tipo    | Description                                                                                                                                                                   |
|------------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| InstanceType     | Stringa | (Facoltativo) Tipo di istanza da avviare come host del workspace. I tipi di istanza variano in base alla regione. Il tipo predefinito è t2.micro.                             |
| PreUpdateScript  | Stringa | (Facoltativo) URL di uno script da eseguire prima dell'applicazione degli aggiornamenti. L'impostazione predefinita ("none") non prevede l'esecuzione di uno script.          |
| PostUpdateScript | Stringa | (Facoltativo) URL di uno script da eseguire dopo l'applicazione degli aggiornamenti ai pacchetti. L'impostazione predefinita ("none") non prevede l'esecuzione di uno script. |
| IncludePackages  | Stringa | (Facoltativo) Vengono aggiornati solo i pacchetti specificati. Per impostazione predefinita ("all"), vengono applicati tutti gli aggiornamenti disponibili.                   |
| ExcludePackages  | Stringa | (Facoltativo) Nomi dei pacchetti da non aggiornare, in tutte le condizioni. Per impostazione predefinita ("none"), non viene escluso alcun pacchetto.                         |

## Fasi di automazione

Il runbook `AWS-UpdateLinuxAmi` include le seguenti operazioni di automazione, per impostazione predefinita.

### Fase 1: `launchInstance` (operazione **`aws:runInstances`**)

Questa fase avvia un'istanza utilizzando i dati utente di Amazon Elastic Compute Cloud (Amazon EC2) e un ruolo del profilo dell'istanza IAM. I dati utente installano l'SSM Agent appropriato, in base al sistema operativo. L'installazione SSM Agent consente di utilizzare strumenti di Systems Manager come Run CommandState Manager, e Inventory.

### Fase 2: `updateOSSoftware` (operazione **`aws:runCommand`**)

Questa fase esegue i comandi seguenti sull'istanza avviata:

- Scarica uno script di aggiornamento da Amazon S3.
- Esegue uno script facoltativo prima dell'aggiornamento.
- Aggiorna i pacchetti di distribuzione e il software di Amazon.
- Esegue uno script facoltativo dopo l'aggiornamento.

Il log di esecuzione viene memorizzato nella cartella `/tmp` in modo che l'utente possa visualizzarlo in un secondo momento.

Se si desidera aggiornare uno specifico set di pacchetti, è possibile specificare l'elenco di pacchetti utilizzando il parametro `IncludePackages`. Quando tale elenco viene specificato, il sistema tenta di aggiornare solo i pacchetti specificati e le relative dipendenze. Non verrà eseguito alcun altro aggiornamento. Per impostazione predefinita, quando non vengono specificati pacchetti da includere, il programma aggiorna tutti i pacchetti disponibili.

Se si desidera escludere dall'aggiornamento uno specifico set di pacchetti, è possibile specificare l'elenco di pacchetti utilizzando il parametro `ExcludePackages`. Quando tale elenco viene specificato, questi pacchetti conservano la propria versione corrente, indipendente dalle altre opzioni specificate. Per impostazione predefinita, quando non sono vengono specificati pacchetti da escludere, non verrà escluso alcun pacchetto.

### Fase 3: `stopInstance` (operazione **`aws:changeInstanceState`**)

Questa fase arresta l'istanza aggiornata.



#### Fase 4: createImage (operazione **aws:createImage**)

Questa fase crea una nuova AMI con un nome dettagliato che lo lega all'ID di origine e all'ora di creazione. Ad esempio: "AMIGenerato da EC2 Automation su {{global:DATE\_TIME}} from {{SourceAmiID}}» dove DATE\_TIME e sourceID rappresentano le variabili di automazione.

#### Fase 5: terminateInstance (operazione **aws:changeInstanceState**)

Questa fase esegue la pulizia dell'automazione mediante l'arresto dell'istanza in esecuzione.

#### Output

L'automazione restituisce il nuovo ID dell'AMI come output.

#### Note

Per impostazione predefinita, quando Automation esegue il AWS-UpdateLinuxAmi runbook, il sistema crea un'istanza temporanea nel VPC predefinito (172.30.0. 0/16). Se hai eliminato il VPC predefinito, ricevi il seguente errore:

VPC not defined 400

Per risolvere questo problema, è necessario creare una copia del runbook AWS -

UpdateLinuxAmi e specificare un ID di sottorete. Per ulteriori informazioni, consulta [VPC non definito 400](#).

Per creare un patch AMI utilizzando Automation (AWS Systems Manager)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Automazione.
3. Scegli Esegui automazione.
4. Nell'elenco Automation document (Documento di automazione) scegliere **AWS-UpdateLinuxAmi**.
5. Nella sezione Dettagli del documento, verifica che l'opzione Versione del documento sia impostata su Versione predefinita al runtime.
6. Scegliere Next (Successivo).
7. Nella sezione Execution Mode (Modalità esecuzione), scegliere Simple Execution (Esecuzione semplice).

8. Nella sezione Input parameters (Inserisci parametri) inserire le informazioni raccolte nella sezione Before you begin (Prima di iniziare).
9. Scegliere Execute (Esegui). La console visualizza lo stato dell'esecuzione del servizio di automazione.

Al termine dell'automazione, avviare un'istanza di test dall'AMI aggiornata per verificare le modifiche.

#### Note

Se una fase qualsiasi dell'automazione ha esito negativo, le informazioni sul malfunzionamento vengono elencate nella pagina Automation Executions (Esecuzioni di automazioni). L'automazione è stata progettata per terminare l'istanza temporanea dopo il corretto completamento di tutti i processi. Se una fase ha esito negativo, il sistema potrebbe non terminare l'istanza. Pertanto, se una fase ha esito negativo, terminare manualmente l'istanza temporanea.

## Aggiorna un Linux AMI (AWS CLI)

Questa procedura dettagliata di AWS Systems Manager automazione mostra come utilizzare il AWS-UpdateLinuxAmi runbook AWS Command Line Interface (AWS CLI) e Systems Manager per applicare automaticamente una patch a Linux Amazon Machine Image (AMI) con le ultime versioni dei pacchetti specificati. L'automazione è uno strumento di AWS Systems Manager. Il runbook AWS-UpdateLinuxAmi automatizza l'installazione anche di altri pacchetti e configurazioni specifici del sito. È possibile aggiornare un'ampia gamma di distribuzioni Linux utilizzando questa procedura guidata, tra cui Ubuntu Server, Red Hat Enterprise Linux (RHEL) oppure Amazon Linux AMIs. Per un elenco completo delle versioni Linux supportate, consulta [Patch Manager prerequisiti](#).

Il AWS-UpdateLinuxAmi runbook consente di automatizzare le attività di manutenzione delle immagini senza dover creare il runbook in JSON o YAML. È possibile utilizzare il runbook AWS-UpdateLinuxAmi per eseguire i tipi di processi seguenti.

- Aggiornamento di tutti i pacchetti di distribuzione e del software Amazon su Amazon Linux, RHEL o Ubuntu Server Amazon Machine Image (AMI). Questo è il comportamento predefinito del runbook.
- Effettua l'installazione AWS Systems Manager SSM Agent su un'immagine esistente per abilitare le funzionalità di Systems Manager, come l'esecuzione di comandi remoti utilizzando o la raccolta dell'inventario del software utilizzando Inventory. AWS Systems Manager Run Command

- Installazione di pacchetti software aggiuntivi.

## Prima di iniziare

Prima di iniziare a lavorare con i runbook, configura i ruoli e, facoltativamente, EventBridge per l'automazione. Per ulteriori informazioni, consulta [Configurazione del servizio di automazione](#). Questa procedura dettagliata richiede inoltre di specificare il nome di un profilo di istanza AWS Identity and Access Management (IAM). Per ulteriori informazioni sulla creazione di un profilo dell'istanza IAM, consulta la pagina [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#).

Il runbook `AWS-UpdateLinuxAmi` accetta i parametri di input seguenti.

| Parametro              | Tipo    | Description                                                                                                                                                                                                                                                                                                                                         |
|------------------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SourceAmiId            | Stringa | (Obbligatorio) L'ID origine di AMI. Puoi fare riferimen to automaticamente all'ID più recente di Amazon EC2 AMI per Linux utilizzan do un parametro AWS Systems Manager Parameter Store pubblico. Per ulteriori informazioni, consulta <a href="#">Ricerca dei più recenti ID AMI di Amazon Linux tramite AWS Systems Manager Parameter Store</a> . |
| IamInstanceProfileName | Stringa | (Obbligatorio) Il nome del ruolo del profilo dell'istanza IAM creato in <a href="#">Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager</a> . Il ruolo del profilo dell'istanza concede le autorizzazioni al servizio di automazione per eseguire operazioni sulle istanze,                                              |

| Parametro            | Tipo    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      |         | ad esempio l'esecuzione di comandi o l'avvio e l'arresto dei servizi. Il runbook utilizza solo il nome del ruolo del profilo dell'istanza.                                                                                                                                                                                                                                                                                                                                                                                                     |
| AutomationAssumeRole | Stringa | (Obbligatorio) Nome del ruolo di servizio IAM creato in <a href="#">Configurazione del servizio di automazione</a> . Il ruolo di servizio (definito anche ruolo presunto) concede l'autorizzazione al servizio di automazione di assumere il ruolo IAM e di eseguire operazioni a nome dell'utente. Ad esempio, il ruolo di servizio permette al servizio di automazione di creare una nuova AMI quando viene eseguita l'operazione <code>aws:createImage</code> in un runbook. Per questo parametro, è necessario specificare l'ARN completo. |
| TargetAmiName        | Stringa | (Facoltativo) Nome della nuova AMI dopo la creazione. Il nome predefinito è una stringa generata dal sistema contenente l'ID dell'AMI di origine e la data/ora di creazione.                                                                                                                                                                                                                                                                                                                                                                   |

| Parametro        | Tipo    | Description                                                                                                                                                                   |
|------------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| InstanceType     | Stringa | (Facoltativo) Tipo di istanza da avviare come host del workspace. I tipi di istanza variano in base alla regione. Il tipo predefinito è t2.micro.                             |
| PreUpdateScript  | Stringa | (Facoltativo) URL di uno script da eseguire prima dell'applicazione degli aggiornamenti. L'impostazione predefinita ("none") non prevede l'esecuzione di uno script.          |
| PostUpdateScript | Stringa | (Facoltativo) URL di uno script da eseguire dopo l'applicazione degli aggiornamenti ai pacchetti. L'impostazione predefinita ("none") non prevede l'esecuzione di uno script. |
| IncludePackages  | Stringa | (Facoltativo) Vengono aggiornati solo i pacchetti specificati. Per impostazione predefinita ("all"), vengono applicati tutti gli aggiornamenti disponibili.                   |
| ExcludePackages  | Stringa | (Facoltativo) Nomi dei pacchetti da non aggiornare, in tutte le condizioni. Per impostazione predefinita ("none"), non viene escluso alcun pacchetto.                         |

## Fasi di automazione

Per impostazione predefinita, il runbook AWS-UpdateLinuxAmi include le seguenti fasi.

### Fase 1: launchInstance (operazione **aws:runInstances**)

Questa fase avvia un'istanza utilizzando i dati utente di Amazon Elastic Compute Cloud (Amazon EC2) e un ruolo del profilo dell'istanza IAM. I dati utente installano l'agente SSM appropriato, in base al sistema operativo. L'installazione SSM Agent consente di utilizzare strumenti di Systems Manager come Run CommandState Manager, e Inventory.

### Fase 2: updateOSSoftware (operazione **aws:runCommand**)

Questa fase esegue i comandi seguenti sull'istanza avviata:

- Scarica uno script di aggiornamento da Amazon Simple Storage Service (Amazon S3).
- Esegue uno script facoltativo prima dell'aggiornamento.
- Aggiorna i pacchetti di distribuzione e il software di Amazon.
- Esegue uno script facoltativo dopo l'aggiornamento.

Il log di esecuzione viene memorizzato nella cartella /tmp in modo che l'utente possa visualizzarlo in un secondo momento.

Se si desidera aggiornare uno specifico set di pacchetti, è possibile specificare l'elenco di pacchetti utilizzando il parametro `IncludePackages`. Quando tale elenco viene specificato, il sistema tenta di aggiornare solo i pacchetti specificati e le relative dipendenze. Non verrà eseguito alcun altro aggiornamento. Per impostazione predefinita, quando non vengono specificati pacchetti da includere, il programma aggiorna tutti i pacchetti disponibili.

Se si desidera escludere dall'aggiornamento uno specifico set di pacchetti, è possibile specificare l'elenco di pacchetti utilizzando il parametro `ExcludePackages`. Quando tale elenco viene specificato, questi pacchetti conservano la propria versione corrente, indipendente dalle altre opzioni specificate. Per impostazione predefinita, quando non sono vengono specificati pacchetti da escludere, non verrà escluso alcun pacchetto.

### Fase 3: stopInstance (operazione **aws:changeInstanceState**)

Questa fase arresta l'istanza aggiornata.

## Fase 4: createImage (operazione **aws:createImage**)

Questa fase crea una nuova AMI con un nome dettagliato che lo lega all'ID di origine e all'ora di creazione. Ad esempio: «AMI generata da EC2 Automation on {{global:DATE\_TIME}} from {{SourceAmiId}}» dove DATE\_TIME e sourceId rappresentano le variabili di automazione.

## Fase 5: terminateInstance (operazione **aws:changeInstanceState**)

Questa fase esegue la pulizia dell'automazione mediante l'arresto dell'istanza in esecuzione.

### Output

L'automazione restituisce il nuovo ID dell'AMI come output.

#### Note

Per impostazione predefinita, quando Automation esegue il AWS-UpdateLinuxAmi runbook, il sistema crea un'istanza temporanea nel VPC predefinito (172.30.0. 0/16). Se hai eliminato il VPC predefinito, ricevi il seguente errore:

VPC not defined 400

Per risolvere questo problema, è necessario creare una copia del runbook AWS-UpdateLinuxAmi e specificare un ID di sottorete. Per ulteriori informazioni, consulta [VPC non definito 400](#).

Per creare un patch AMI utilizzando l'automazione

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Eseguire il comando seguente per eseguire il runbook AWS-UpdateLinuxAmi. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
aws ssm start-automation-execution \
 --document-name "AWS-UpdateLinuxAmi" \
 --parameters \
 SourceAmiId=AMI ID, \
 IamInstanceProfileName=IAM instance profile, \
 ...
```

```
AutomationAssumeRole='arn:aws:iam::
{{global:ACCOUNT_ID}}:role/AutomationServiceRole'
```

Il comando restituisce un ID di esecuzione. Copia questo ID negli appunti. Usa questo ID per visualizzare lo stato dell'automazione.

```
{
 "AutomationExecutionId": "automation execution ID"
}
```

3. Per visualizzare l'automazione utilizzando il AWS CLI, esegui il comando seguente:

```
aws ssm describe-automation-executions
```

4. Eseguire il comando seguente per visualizzare i dettagli relativi al progresso dell'automazione. Sostituisci *automation execution ID* con le tue informazioni.

```
aws ssm get-automation-execution --automation-execution-id automation execution ID
```

Il completamento del processo di aggiornamento può richiedere 30 minuti o un intervallo maggiore.

 Note

È inoltre possibile monitorare lo stato dell'automazione nella console. Nell'elenco, scegliere l'automazione appena eseguita e quindi scegliere la scheda Steps (Fasi). In questa scheda è riportato lo stato delle operazioni dell'automazione.

Al termine dell'automazione, avviare un'istanza di test dall'AMI aggiornata per verificare le modifiche.

 Note

Se una fase qualsiasi dell'automazione ha esito negativo, le informazioni sul malfunzionamento vengono elencate nella pagina Automation Executions (Esecuzioni di automazioni). L'automazione è stata progettata per terminare l'istanza temporanea dopo il corretto completamento di tutti i processi. Se una fase ha esito negativo, il sistema potrebbe



non terminare l'istanza. Pertanto, se una fase ha esito negativo, terminare manualmente l'istanza temporanea.

## Aggiornamento di un' Windows Server AMI

Il `AWS-UpdateWindowsAmi` runbook ti consente di automatizzare le attività di manutenzione delle immagini su Amazon Windows Amazon Machine Image (AMI) senza dover creare il runbook in JSON o YAML. Questo runbook è supportato per Windows Server 2008 R2 o versioni successive. È possibile utilizzare il runbook `AWS-UpdateWindowsAmi` per eseguire i tipi di processi seguenti.

- Installazione di tutti gli aggiornamenti di Windows e aggiornamento del software Amazon (comportamento predefinito).
- Installazione di aggiornamenti di Windows specifici e aggiornamento del software Amazon.
- Personalizzazione di un'AMI tramite script.

### Prima di iniziare

Prima di iniziare a lavorare con i runbook, [configurare i ruoli per il servizio di automazione](#) per aggiungere una policy `iam:PassRole` che fa riferimento all'ARN del profilo dell'istanza a cui si desidera concedere l'accesso. Facoltativamente, configura Amazon for Automation. EventBridge Per ulteriori informazioni, consulta [Configurazione del servizio di automazione](#). Questa procedura dettagliata richiede anche di specificare il nome di un profilo di istanza AWS Identity and Access Management (IAM). Per ulteriori informazioni sulla creazione di un profilo dell'istanza IAM, consulta la pagina [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#).

#### Note

Gli aggiornamenti di AWS Systems Manager SSM Agent sono in genere distribuiti in regioni diverse in momenti diversi. Quando si personalizza o si aggiorna un'AMI, è possibile usare solo le AMI di origine pubblicate per la regione in uso. Ciò assicurerà che tu stia lavorando con la SSM Agent versione più recente per quella regione ed eviterà problemi di compatibilità.

Il runbook `AWS-UpdateWindowsAmi` accetta i parametri di input seguenti.

| Parametro              | Tipo    | Description                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SourceAmild            | Stringa | (Obbligatorio) L'ID origine di AMI. È possibile fare automaticamente riferimento alla versione più recente di ID dell'AMI di Windows Server utilizzando un parametro pubblico di Parameter Store di Systems Manager. Per ulteriori informazioni, consulta <a href="#">Query di ricerca dei più recenti ID di AMI di Windows tramite AWS Systems ManagerParameter Store</a> .                     |
| SubnetId               | Stringa | (Facoltativo) La sottorete in cui si desidera avviare l'istanza temporanea. Se è stato eliminato il VPC predefinito, è necessario specificare un valore per questo parametro.                                                                                                                                                                                                                    |
| IamInstanceProfileName | Stringa | (Obbligatorio) Il nome del ruolo del profilo dell'istanza IAM creato in <a href="#">Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager</a> . Il ruolo del profilo dell'istanza concede le autorizzazioni al servizio di automazione per eseguire operazioni sulle istanze, ad esempio l'esecuzione di comandi o l'avvio e l'arresto dei servizi. Il runbook utilizza |

| Parametro            | Tipo    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      |         | solo il nome del ruolo del profilo dell'istanza.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| AutomationAssumeRole | Stringa | (Obbligatorio) Nome del ruolo di servizio IAM creato in <a href="#">Configurazione del servizio di automazione</a> . Il ruolo di servizio (definito anche ruolo presunto) concede l'autorizzazione al servizio di automazione di assumere il ruolo IAM e di eseguire operazioni a nome dell'utente. Ad esempio, il ruolo di servizio permette al servizio di automazione di creare una nuova AMI quando viene eseguita l'operazione <code>aws:createImage</code> in un runbook. Per questo parametro, è necessario specificare l'ARN completo. |
| TargetAmiName        | Stringa | (Facoltativo) Nome della nuova AMI dopo la creazione. Il nome predefinito è una stringa generata dal sistema contenente l'ID dell'AMI di origine e la data/ora di creazione.                                                                                                                                                                                                                                                                                                                                                                   |

| Parametro        | Tipo    | Description                                                                                                                                                                                              |
|------------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| InstanceType     | Stringa | (Facoltativo) Tipo di istanza da avviare come host del workspace. I tipi di istanza variano in base alla regione. Il tipo predefinito è t2.medium.                                                       |
| PreUpdateScript  | Stringa | (Facoltativo) Script da eseguire prima di aggiornare l'AMI. Inserisci uno script come parametro nel runbook oppure al runtime.                                                                           |
| PostUpdateScript | Stringa | (Facoltativo) Script da eseguire dopo l'aggiornamento dell'AMI. Inserisci uno script come parametro nel runbook oppure al runtime.                                                                       |
| IncludeKbs       | Stringa | (Facoltativo) Specificare uno o più ID articolo Microsoft Knowledge Base (KB) da includere. È possibile installare e più ID utilizzando valori separati da virgole. Formati validi: KB9876543 o 9876543. |
| ExcludeKbs       | Stringa | (Facoltativo) Specificare uno o più ID articolo Microsoft Knowledge Base (KB) da escludere. È possibile escludere più ID utilizzando valori separati da virgole. Formati validi: KB9876543 o 9876543.    |

| Parametro      | Tipo    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Categories     | Stringa | (Facoltativo) Specificare una o più categorie di aggiornamento. È possibile filtrare le categorie utilizzando valori separati da virgole. Opzioni: Critical Update, Security Update, Definition Update, Update Rollup, Service Pack, Tool, Update o Driver. I formati validi includono una singola voce, ad esempio: Critical Update. In alternativa, è possibile specificare un elenco di valori separati da virgole: Critical Update, Security Update, Definition Update. |
| SeverityLevels | Stringa | (Facoltativo) Specificare uno o più livelli di gravità MSRC associati a un aggiornamento. È possibile filtrare i livelli di gravità utilizzando valori separati da virgole. Opzioni: Critical, Important, Low, Moderate o Unspecified. I formati validi includono una singola voce, ad esempio: Critical. In alternativa, è possibile specificare un elenco di valori separati da virgole: Critical, Important, Low.                                                        |

## Fasi di automazione

Per impostazione predefinita, il runbook AWS-UpdateWindowsAmi include le seguenti fasi.

## Fase 1: launchInstance (operazione **aws:runInstances**)

Questa fase avvia un'istanza con un ruolo del profilo dell'istanza IAM dal parametro `SourceAmiID` specificato.

## Fase 2: esecuzione PreUpdateScript (**aws:runCommand**)

Questo passaggio consente di specificare uno script come stringa da eseguire prima dell'installazione degli aggiornamenti.

## Fase 3: updateEC2Config (operazione **aws:runCommand**)

Questo passaggio utilizza il `AWS-InstallPowerShellModule` runbook per scaricare un PowerShell modulo AWS pubblico. Systems Manager verifica l'integrità del modulo utilizzando un SHA-256 hash. Systems Manager verifica quindi il sistema operativo per determinare se aggiornare `EC2Config` o `EC2Launch`. `EC2Config` viene eseguito su Windows Server 2008 R2 fino a Windows Server 2012 R2. `EC2Launch` viene eseguito su Windows Server 2016.

## Fase 4: updateSSMAgent (operazione **aws:runCommand**)

Questa fase aggiorna SSM Agent utilizzando il runbook `AWS-UpdateSSMAgent`.

## Fase 5: updateAWSPVDriver (operazione **aws:runCommand**)

Questo passaggio aggiorna i driver AWS PV utilizzando il runbook. `AWS-ConfigureAWSPackage`

## Fase 6: aggiornamento AwsEnaNetworkDriver (**aws:runCommand**)

Questo passaggio aggiorna i driver AWS ENA Network utilizzando il `AWS-ConfigureAWSPackage` runbook.

## Fase 7: installazione WindowsUpdates (**aws:runCommand**)

Questa fase installa gli aggiornamenti di Windows utilizzando il runbook `AWS-InstallWindowsUpdates`. Per impostazione predefinita, Systems Manager cerca e installa tutti gli aggiornamenti mancanti. È possibile modificare il comportamento predefinito specificando uno dei parametri seguenti: `IncludeKbs`, `ExcludeKbs`, `Categories` o `SeverityLevels`.

## Fase 8: esecuzione PostUpdateScript (**aws:runCommand**)

Questo passaggio consente di specificare uno script come stringa da eseguire dopo l'installazione degli aggiornamenti.

## Fase 9: esecuzione SysprepGeneralize (**aws:runCommand**)

Questo passaggio utilizza il `AWS-InstallPowerShellModule` runbook per scaricare un PowerShell modulo AWS pubblico. Systems Manager verifica l'integrità del modulo utilizzando un SHA-256 hash. Systems Manager esegue quindi sysprep utilizzando metodi AWS supportati per EC2Launch (Windows Server 2016) o EC2Config (da Windows Server 2008 R2 a 2012 R2).

## Fase 10: stopInstance (operazione **aws:changeInstanceState**)

Questa fase arresta l'istanza aggiornata.

## Fase 11: createImage (operazione **aws:createImage**)

Questa fase crea una nuova AMI con un nome dettagliato che lo lega all'ID di origine e all'ora di creazione. Ad esempio: «AMI generata da EC2 Automation on {{global:DATE\_TIME}} from {{{}}}\" dove `DATE_TIME` e `sourceID` rappresentano le variabili di automazione. `SourceAmiId`

## Fase 12: (azione) TerminateInstance **aws:changeInstanceState**

Questa fase esegue la pulizia dell'automazione mediante l'arresto dell'istanza in esecuzione.

## Output

Questa sezione consente di designare gli output di vari passaggi o valori di qualsiasi parametro come output di automazione. Per impostazione predefinita, l'output è l'ID dell'AMI aggiornata di Windows creata dall'automazione.

### Note

Per impostazione predefinita, quando Automation esegue il `AWS-UpdateWindowsAmi` runbook e crea un'istanza temporanea, il sistema utilizza il VPC predefinito (172.30.0. 0/16).

Se hai eliminato il VPC predefinito, ricevi il seguente errore:

VPC non definito 400

Per risolvere questo problema, è necessario creare una copia del runbook `AWS-UpdateWindowsAmi` e specificare un ID di sottorete. Per ulteriori informazioni, consulta [VPC non definito 400](#).

Per creare un Windows con patch AMI utilizzando Automation

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Eseguire il comando seguente per eseguire il runbook AWS-UpdateWindowsAmi. Sostituisci ogni *example resource placeholder* con le tue informazioni. Il comando di esempio seguente utilizza un'AMI recente di Amazon EC2 per ridurre il numero di patch da applicare. Se si esegue il comando più di una volta, è necessario specificare un valore univoco per targetAMIname. I nomi per l'AMI devono essere univoci.

```
aws ssm start-automation-execution \
 --document-name="AWS-UpdateWindowsAmi" \
 --parameters SourceAmiId='AMI ID',IamInstanceProfileName='IAM
 instance profile',AutomationAssumeRole='arn:aws:iam::
 {{global:ACCOUNT_ID}}:role/AutomationServiceRole'
```

Il comando restituisce un ID di esecuzione. Copia questo ID negli appunti. Usa questo ID per visualizzare lo stato dell'automazione.

```
{
 "AutomationExecutionId": "automation execution ID"
}
```

3. Per visualizzare l'automazione utilizzando il AWS CLI, esegui il comando seguente:

```
aws ssm describe-automation-executions
```

4. Eseguire il comando seguente per visualizzare i dettagli relativi al progresso dell'automazione.

```
aws ssm get-automation-execution
 --automation-execution-id automation execution ID
```

#### Note

A seconda del numero di patch applicate, il processo di applicazione delle patch di Windows eseguito in questa automazione di esempio può richiedere 30 minuti o più.



## Aggiorna un golden AMI utilizzando l'automazione, AWS Lambda e Parameter Store

L'esempio seguente utilizza il modello in cui un'organizzazione gestisce e periodicamente applica patch ad AMIs di proprietà anziché crearle da AMIs di Amazon Elastic Compute Cloud (Amazon EC2).

La procedura seguente mostra come applicare automaticamente le patch del sistema operativo (SO) a un'AMI già considerata come la più aggiornata o all'AMI più recente. Nell'esempio, il valore predefinito del parametro `SourceAmiId` è definito da un AWS Systems Manager Parameter Store parametro chiamato `latestAmi`. Il valore di `latestAmi` viene aggiornato da una AWS Lambda funzione richiamata alla fine dell'automazione. Grazie a questo processo di automazione, il tempo e gli sforzi impiegati per l'applicazione delle patch AMIs sono ridotti al minimo perché le patch vengono sempre applicate alle più aggiornate. AMI Parameter Store e l'automazione sono strumenti di AWS Systems Manager.

Prima di iniziare

Configura i ruoli di automazione e, facoltativamente, Amazon EventBridge for Automation. Per ulteriori informazioni, consulta [Configurazione del servizio di automazione](#).

Indice

- [Attività 1: creare un parametro in Systems Manager Parameter Store](#)
- [Attività 2: creare un ruolo IAM per AWS Lambda](#)
- [Attività 3: Creare un AWS Lambda funzione](#)
- [Processo 4: creazione di un runbook e applicazione di patch all'AMI](#)

Attività 1: creare un parametro in Systems Manager Parameter Store

In Parameter Store creare un parametro di stringa che utilizza le seguenti informazioni:

- Nome (Nome): `latestAmi`.
- Valore: Un ID AMI. Ad esempio: `ami-188d6e0e`.

Per informazioni su come creare un parametro di stringa di Parameter Store, consulta [Creazione in corso Parameter Store parametri in Systems Manager](#).

## Attività 2: creare un ruolo IAM per AWS Lambda

Utilizza la seguente procedura per creare un ruolo del servizio IAM per AWS Lambda. Queste policy forniscono l'autorizzazione a Lambda per aggiornare il valore del parametro `latestAmi` utilizzando una funzione Lambda e Systems Manager.

Per creare un ruolo di servizio IAM per Lambda

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, scegliere Policies (Policy) e Create Policy (Crea policy).
3. Scegli la scheda JSON.
4. Sostituisci il contenuto predefinito con la seguente policy. Sostituisci ogni *example resource placeholder* con le tue informazioni.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "logs:CreateLogGroup",
 "Resource": "arn:aws:logs:us-east-1:111122223333:*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "logs:CreateLogStream",
 "logs:PutLogEvents"
],
 "Resource": [
 "arn:aws:logs:us-east-1:111122223333:log-group:/aws/lambda/function name:*"
]
 }
]
}
```

5. Scegli Successivo: Tag.

6. (Facoltativo) Aggiungere una o più coppie tag chiave-valore per organizzare, monitorare o controllare l'accesso per questa policy.
7. Scegli Prossimo: Rivedi.
8. Nella pagina Rivedi policy, per l'opzione Nome specifica un nome per la policy inline, ad esempio **amiLambda**.
9. Scegli Crea policy.
10. Ripetere le fasi 2 e 3.
11. Quindi incollare la policy seguente. Sostituisci ogni *example resource placeholder* con le tue informazioni.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ssm:PutParameter",
 "Resource": "arn:aws:ssm:us-east-1:111122223333:parameter/latestAmi"
 },
 {
 "Effect": "Allow",
 "Action": "ssm:DescribeParameters",
 "Resource": "*"
 }
]
}
```

12. Scegli Successivo: Tag.
13. (Facoltativo) Aggiungere una o più coppie tag chiave-valore per organizzare, monitorare o controllare l'accesso per questa policy.
14. Scegli Prossimo: Rivedi.
15. Nella pagina Rivedi policy, per l'opzione Nome specifica un nome per la policy inline, ad esempio **amiParameter**.
16. Scegli Crea policy.
17. Nel pannello di navigazione, scegli Ruoli e quindi Crea ruolo.

18. In Caso d'uso, scegli Lambda, quindi scegli Successivo.
19. Nella pagina Collega autorizzazioni, utilizza il campo Cerca per individuare le due policy create in precedenza.
20. Seleziona la casella di controllo accanto alle policy, quindi scegli Successivo: Tag.
21. Per Role name (Nome ruolo), inserire un nome per il nuovo ruolo, ad esempio **lambda-ssm-role** o un altro nome che preferisci.

 Note

Poiché varie entità possono fare riferimento al ruolo, non è possibile modificare il nome del ruolo dopo averlo creato.

22. (Facoltativo) Aggiungi una o più coppie di tag chiave-valore per organizzare, monitorare o controllare l'accesso per questo ruolo, quindi scegli Crea ruolo.

### Attività 3: Creare un AWS Lambda funzione

Utilizzare la procedura seguente per creare una funzione Lambda che aggiorna automaticamente il valore del parametro `latestAmi`.

#### Come creare una funzione Lambda

1. Accedi Console di gestione AWS e apri la AWS Lambda console all'indirizzo <https://console.aws.amazon.com/lambda/>.
2. Scegli Crea funzione.
3. Nella pagina Create function (Crea funzione), scegliere Author from scratch (Crea da zero).
4. Nel campo Function name (Nome funzione), immettere **Automation-UpdateSsmParam**.
5. Per Runtime, scegli Python 3.11.
6. Per Architettura, seleziona il tipo di processore del computer che Lambda deve utilizzare per eseguire la funzione, x86\_64 o arm64.
7. Nella sezione Autorizzazioni, espandi Modifica ruolo di esecuzione predefinito.
8. Scegli Utilizza un ruolo esistente, quindi scegli il ruolo di servizio creato per Lambda nell'attività 2.
9. Scegli Crea funzione.

10. Nella sezione Origine codice, nella scheda `lambda_function`, elimina il codice precompilato nel campo, quindi incolla il seguente codice di esempio.

```
from __future__ import print_function

import json
import boto3

print('Loading function')

#Updates an SSM parameter
#Expects parameterName, parameterValue
def lambda_handler(event, context):
 print("Received event: " + json.dumps(event, indent=2))

 # get SSM client
 client = boto3.client('ssm')

 #confirm parameter exists before updating it
 response = client.describe_parameters(
 Filters=[
 {
 'Key': 'Name',
 'Values': [event['parameterName']]
 },
]
)

 if not response['Parameters']:
 print('No such parameter')
 return 'SSM parameter not found.'

 #if parameter has a Description field, update it PLUS the Value
 if 'Description' in response['Parameters'][0]:
 description = response['Parameters'][0]['Description']

 response = client.put_parameter(
 Name=event['parameterName'],
 Value=event['parameterValue'],
 Description=description,
 Type='String',
 Overwrite=True
```

```
)

 #otherwise just update Value
 else:
 response = client.put_parameter(
 Name=event['parameterName'],
 Value=event['parameterValue'],
 Type='String',
 Overwrite=True
)

 responseString = 'Updated parameter %s with value %s.' %
(event['parameterName'], event['parameterValue'])

 return responseString
```

11. Scegli File, Salva.
12. Per testare la funzione Lambda, dal menu Test scegli Configura evento di test.
13. Nel campo Event name (Nome evento), inserire un nome per l'evento di test, ad esempio **MyTestEvent**.
14. Sostituire il testo esistente con il seguente esempio JSON. Sostituisci **AMI ID** con le tue informazioni per impostare il latestAmi valore del parametro.

```
{
 "parameterName": "latestAmi",
 "parameterValue": "AMI ID"
}
```

15. Selezionare Salva.
16. Scegliere Test per testare la funzione. Nella scheda Risultato dell'esecuzione, lo stato deve essere riportato come Completato, insieme ad altri dettagli sull'aggiornamento.

#### Processo 4: creazione di un runbook e applicazione di patch all'AMI

Utilizzare la procedura seguente per creare ed eseguire un runbook che applica patch all'AMI specificata per il parametro latestAmi. Al termine dell'automazione, il valore del parametro latestAmi viene aggiornato con l'ID dell'AMI con patch applicate. Le automazioni successive utilizzano l'AMI creata dall'esecuzione precedente.

## Per creare ed eseguire il runbook

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Documenti.
3. Per Crea documento, scegli Automazione.
4. In Nome, inserisci **UpdateMyLatestWindowsAmi**.
5. Scegliere la scheda Editor, quindi Edit (Modifica).
6. Scegli OK quando richiesto.
7. Nel campo Editor di documenti, sostituisci il contenuto predefinito con il seguente runbook di esempio YAML.

```

description: Systems Manager Automation Demo - Patch AMI and Update ASG
schemaVersion: '0.3'
assumeRole: '{{ AutomationAssumeRole }}'
parameters:
 AutomationAssumeRole:
 type: String
 description: '(Required) The ARN of the role that allows Automation to perform
the actions on your behalf. If no role is specified, Systems Manager Automation
uses your IAM permissions to execute this document.'
 default: ''
 SourceAMI:
 type: String
 description: The ID of the AMI you want to patch.
 default: '{{ ssm:latestAmi }}'
 SubnetId:
 type: String
 description: The ID of the subnet where the instance from the SourceAMI
parameter is launched.
 SecurityGroupIds:
 type: StringList
 description: The IDs of the security groups to associate with the instance
that's launched from the SourceAMI parameter.
 NewAMI:
 type: String
 description: The name of of newly patched AMI.
 default: 'patchedAMI-{{global:DATE_TIME}}'
 InstanceProfile:
```

```

 type: String
 description: The name of the IAM instance profile you want the source instance
to use.
 SnapshotId:
 type: String
 description: (Optional) The snapshot ID to use to retrieve a patch baseline
snapshot.
 default: ''
 RebootOption:
 type: String
 description: '(Optional) Reboot behavior after a patch Install operation. If
you choose NoReboot and patches are installed, the instance is marked as non-
compliant until a subsequent reboot and scan.'
 allowedValues:
 - NoReboot
 - RebootIfNeeded
 default: RebootIfNeeded
 Operation:
 type: String
 description: (Optional) The update or configuration to perform on the instance.
The system checks if patches specified in the patch baseline are installed on the
instance. The install operation installs patches missing from the baseline.
 allowedValues:
 - Install
 - Scan
 default: Install
 mainSteps:
 - name: startInstances
 action: 'aws:runInstances'
 timeoutSeconds: 1200
 maxAttempts: 1
 onFailure: Abort
 inputs:
 ImageId: '{{ SourceAMI }}'
 InstanceType: m5.large
 MinInstanceCount: 1
 MaxInstanceCount: 1
 IamInstanceProfileName: '{{ InstanceProfile }}'
 SubnetId: '{{ SubnetId }}'
 SecurityGroupIds: '{{ SecurityGroupIds }}'
 - name: verifyInstanceManaged
 action: 'aws:waitForAwsResourceProperty'
 timeoutSeconds: 600
 inputs:

```



```

 Service: ssm
 Api: DescribeInstanceInformation
 InstanceInformationFilterList:
 - key: InstanceIds
 valueSet:
 - '{{ startInstances.InstanceIds }}'
 PropertySelector: '$.InstanceInformationList[0].PingStatus'
 DesiredValues:
 - Online
 onFailure: 'step:terminateInstance'
- name: installPatches
 action: 'aws:runCommand'
 timeoutSeconds: 7200
 onFailure: Abort
 inputs:
 DocumentName: AWS-RunPatchBaseline
 Parameters:
 SnapshotId: '{{SnapshotId}}'
 RebootOption: '{{RebootOption}}'
 Operation: '{{Operation}}'
 InstanceIds:
 - '{{ startInstances.InstanceIds }}'
- name: stopInstance
 action: 'aws:changeInstanceState'
 maxAttempts: 1
 onFailure: Continue
 inputs:
 InstanceIds:
 - '{{ startInstances.InstanceIds }}'
 DesiredState: stopped
- name: createImage
 action: 'aws:createImage'
 maxAttempts: 1
 onFailure: Continue
 inputs:
 InstanceId: '{{ startInstances.InstanceIds }}'
 ImageName: '{{ NewAMI }}'
 NoReboot: false
 ImageDescription: Patched AMI created by Automation
- name: terminateInstance
 action: 'aws:changeInstanceState'
 maxAttempts: 1
 onFailure: Continue
 inputs:

```

```
 InstanceIds:
 - '{{ startInstances.InstanceIds }}'
 DesiredState: terminated
 - name: updateSsmParam
 action: aws:invokeLambdaFunction
 timeoutSeconds: 1200
 maxAttempts: 1
 onFailure: Abort
 inputs:
 FunctionName: Automation-UpdateSsmParam
 Payload: '{"parameterName":"latestAmi",
"parameterValue":"{{createImage.ImageId}}"}'
 outputs:
 - createImage.ImageId
```

8. Scegli Crea automazione.
9. Nel pannello di navigazione, scegli Automazione, quindi Esegui automazione.
10. Nella pagina Choose document (Scegli il documento), scegli la scheda Owned by me (Di mia proprietà).
11. Cerca il UpdateMyLatestWindowsAmi runbook e seleziona il pulsante nella UpdateMyLatestWindowsAmi scheda.
12. Scegli Avanti.
13. Scegliere Simple execution (Esecuzione semplice).
14. Specifica i valori per il parametro di input.
15. Scegliere Execute (Esegui).
16. Una volta completata l'esecuzione, scegliere Parameter Store nel pannello di navigazione e confermare che il nuovo valore del parametro latestAmi corrisponde al valore restituito dall'automazione. È inoltre possibile verificare se il nuovo ID dell'AMI corrisponde all'output del servizio di automazione nella sezione AMI della console di Amazon EC2.

## Aggiornamento in corso AMI utilizzando l'automazione e Jenkins

Se la tua organizzazione utilizza Jenkins software in una CI/CD pipeline, puoi aggiungere Automation come fase successiva alla compilazione per preinstallare le versioni delle applicazioni in (). Amazon Machine Images AMIs L'automazione è uno strumento di AWS Systems Manager. È inoltre possibile utilizzare la funzionalità di pianificazione di Jenkins per chiamare il servizio di automazione e creare un piano personalizzato per l'applicazione di patch del sistema operativo (SO).

L'esempio seguente mostra come invocare il servizio di automazione da un server Jenkins in esecuzione on-premises o in Amazon Elastic Compute Cloud (Amazon EC2). Per l'autenticazione, il Jenkins server utilizza AWS credenziali basate su una policy IAM creata nell'esempio e allegata al profilo dell'istanza.

#### Note

Assicurati di seguire le best practice di sicurezza Jenkins durante la configurazione dell'istanza.

Prima di iniziare

Prima di configurare il servizio di automazione con Jenkins, completa le seguenti attività:

- Completare l'esempio descritto nell'argomento [Aggiorna un golden AMI utilizzando l'automazione, AWS Lambda e Parameter Store](#). L'esempio seguente utilizza il UpdateMyLatestWindowsAmirunbook creato in quell'esempio.
- Configurare i ruoli IAM per il servizio di automazione. Systems Manager richiede un ruolo del profilo dell'istanza e un ARN del ruolo di servizio per elaborare le automazioni. Per ulteriori informazioni, consulta [Configurazione del servizio di automazione](#).

Per creare una policy IAM per Jenkins server

1. Accedi a Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, scegliere Policies (Policy) e Create Policy (Crea policy).
3. Scegli la scheda JSON.
4. Sostituisci ogni *example resource placeholder* con le tue informazioni.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ssm:StartAutomationExecution",
```

```
 "Resource": [
 "arn:aws:ssm:us-east-1:111122223333:document/UpdateMyLatestWindowsAmi",
 "arn:aws:ssm:us-east-1:111122223333:automation-execution/*"
]
 }
}
```

5. Scegli Review policy (Rivedi policy).
6. Nella pagina Review policy (Rivedi policy), per l'opzione Name (Nome) specificare un nome per la policy inline, ad esempio **JenkinsPolicy**.
7. Scegli Crea policy.
8. Nel riquadro di navigazione, seleziona Ruoli.
9. Scegli il profilo dell'istanza collegato al server Jenkins.
10. Nella scheda Autorizzazioni, scegli Aggiungi autorizzazioni, quindi scegli Collega policy.
11. Nella sezione Altre policy di autorizzazione, inserisci il nome della policy creata nei passaggi precedenti. Ad esempio, JenkinsPolicy.
12. Seleziona la casella di controllo accanto alla policy, quindi scegli Collega policy.

Utilizza la seguente procedura per configurarla AWS CLI sul tuo Jenkins server.

Per configurare il Jenkins server per l'automazione

1. Collegati al server Jenkins sulla porta 8080 utilizzando il browser preferito per accedere all'interfaccia di gestione.
2. Inserire la password trovata in `/var/lib/jenkins/secrets/initialAdminPassword`. Per visualizzare la password, eseguire il comando seguente.

```
sudo cat /var/lib/jenkins/secrets/initialAdminPassword
```

3. Lo script di installazione di Jenkins indirizza alla pagina Personalizzazione di Jenkins. Selezionare Install suggested plugins (Installazione dei plug-in suggeriti).
4. Al termine dell'installazione, scegli Credenziali amministratore, seleziona Salva credenziali e successivamente Inizia a usare Jenkins.
5. Nel pannello di navigazione a sinistra, scegli Gestione di Jenkins e successivamente seleziona Gestione dei plug-in.

6. Scegliere la scheda Available (Disponibilità) e quindi inserire **Amazon EC2 plugin**.
7. Selezionare la casella di controllo relativa a **Amazon EC2 plugin** e quindi selezionare Install without restart (Installazione senza riavvio).
8. Al termine dell'installazione, selezionare Go back to the top page (Torna alla pagina iniziale).
9. Scegli GestisciJenkins, quindi seleziona Gestisci nodi e cloud.
10. Nella sezione Cloud, seleziona Aggiungi un nuovo cloud, quindi scegli Amazon EC2.
11. Inserisci le tue informazioni nei campi rimanenti. Assicurati di selezionare l'opzione Utilizza il profilo dell'istanza EC2 per ottenere le credenziali.

Utilizza la procedura seguente per configurare il progetto Jenkins in modo che invochi il servizio di automazione.

Per configurare il tuo Jenkins server per richiamare Automation

1. Apri la console Jenkins nel browser Web.
2. Scegliere il progetto che si desidera configurare con il servizio di automazione, quindi scegliere Configure (Configura).
3. Nella scheda Build (Compilazione) scegliere Add Build Step (Aggiungi fase di compilazione).
4. Scegliere Execute shell (Esegui shell) o Execute Windows batch command (Esegui comando batch Windows) (a seconda del sistema operativo in uso).
5. Nel campo Comando, esegui un AWS CLI comando come il seguente. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
aws ssm start-automation-execution \
 --document-name runbook name \
 --region Regione AWS of your source AMI \
 --parameters runbook parameters
```

Il comando di esempio seguente utilizza il UpdateMyLatestWindowsAmirunbook e il parametro Systems Manager latestAmi creati in [Aggiorna un golden AMI utilizzando l'automazione, AWS Lambda e Parameter Store](#).

```
aws ssm start-automation-execution \
 --document-name UpdateMyLatestWindowsAmi \
 --parameters \
 "sourceAMIId '{{ssm:latestAmi}}'"
```

```
--region region
```

In Jenkins, il comando è simile all'esempio illustrato nel seguente screenshot.



6. Nel progetto Jenkins, scegli Crea ora. Jenkins restituisce un output simile al seguente.

### Console Output

```
Started by user admin
Building in workspace /var/lib/jenkins/workspace/Build AMI
[Build AMI] $ /bin/sh -xe /tmp/hudson3259912997441414819.sh
+ aws --region us-east-1 ssm start-automation-execution --document-name UpdateMyLatestWindowsAmi --parameters 'sourceAMIId='\''{{ssm:latestAmi}}'\''
{
 "AutomationExecutionId": "7badf13a-ff8c-11e6-9503-9d48daa849f3"
}
Finished: SUCCESS
```

## Aggiornamento in corso AMI per gruppi Auto Scaling

Nell'esempio seguente aggiorna un gruppo Auto Scaling con una nuova AMI con patch applicate. Questo approccio garantisce che le nuove immagini vengano automaticamente rese disponibili nei vari ambienti di calcolo che usano gruppi Auto Scaling.

La fase finale dell'automazione in questo esempio utilizza una funzione Python per creare un nuovo modello di avvio che utilizza la nuova AMI con patch applicate. Quindi il gruppo Auto Scaling è aggiornato per utilizzare il nuovo modello di avvio. In questo tipo di scenario con dimensionamento automatico, gli utenti possono terminare le istanze esistenti nel gruppo Auto Scaling per forzare l'avvio di una nuova istanza che utilizza la nuova immagine. In alternativa, gli utenti possono attendere che siano gli eventi di scalabilità verticale o orizzontale ad avviare le istanze più recenti.

Prima di iniziare

Prima di iniziare a utilizzare questo esempio, completare le attività descritte di seguito.

- Configurare i ruoli IAM per il servizio di automazione. Systems Manager richiede un ruolo del profilo dell'istanza e un ARN del ruolo di servizio per elaborare le automazioni. Per ulteriori informazioni, consulta [Configurazione del servizio di automazione](#).

### Crea il PatchAMIAndUpdateASG runbook

Utilizzate la procedura seguente per creare il PatchAMIAndUpdateASG runbook che applica le patch AMI specificate per il parametro SourceAMI. Il runbook aggiorna anche un gruppo Auto Scaling utilizzando l'AMI con patch applicate più recente.

Per creare ed eseguire il runbook

1. Apri la console all'indirizzo. AWS Systems Manager <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Documenti.
3. Nel menu a discesa Create document (Crea un documento), scegliere Automation (Automazione).
4. Nel campo Name (Nome), inserire **PatchAMIAndUpdateASG**.
5. Scegliere la scheda Editor, quindi Edit (Modifica).
6. Scegliere OK quando richiesto ed eliminare il contenuto nel campo Document editor (Editor di documenti).
7. Nel campo Document editor (Editor di documenti) incollare il seguente contenuto del runbook di esempio YAML.

```

description: Systems Manager Automation Demo - Patch AMI and Update ASG
schemaVersion: '0.3'
assumeRole: '{{ AutomationAssumeRole }}'
parameters:
 AutomationAssumeRole:
 type: String
 description: '(Required) The ARN of the role that allows Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses your IAM permissions to execute this document.'
 default: ''
 SourceAMI:
 type: String
 description: '(Required) The ID of the AMI you want to patch.'
```

```
SubnetId:
 type: String
 description: '(Required) The ID of the subnet where the instance from the
SourceAMI parameter is launched.'
SecurityGroupIds:
 type: StringList
 description: '(Required) The IDs of the security groups to associate with the
instance launched from the SourceAMI parameter.'
NewAMI:
 type: String
 description: '(Optional) The name of of newly patched AMI.'
 default: 'patchedAMI-{{global:DATE_TIME}}'
TargetASG:
 type: String
 description: '(Required) The name of the Auto Scaling group you want to
update.'
InstanceProfile:
 type: String
 description: '(Required) The name of the IAM instance profile you want the
source instance to use.'
SnapshotId:
 type: String
 description: '(Optional) The snapshot ID to use to retrieve a patch baseline
snapshot.'
 default: ''
RebootOption:
 type: String
 description: '(Optional) Reboot behavior after a patch Install operation. If
you choose NoReboot and patches are installed, the instance is marked as non-
compliant until a subsequent reboot and scan.'
 allowedValues:
 - NoReboot
 - RebootIfNeeded
 default: RebootIfNeeded
Operation:
 type: String
 description: '(Optional) The update or configuration to perform on the instance.
The system checks if patches specified in the patch baseline are installed on the
instance. The install operation installs patches missing from the baseline.'
 allowedValues:
 - Install
 - Scan
 default: Install
mainSteps:
```



```
- name: startInstances
 action: 'aws:runInstances'
 timeoutSeconds: 1200
 maxAttempts: 1
 onFailure: Abort
 inputs:
 ImageId: '{{ SourceAMI }}'
 InstanceType: m5.large
 MinInstanceCount: 1
 MaxInstanceCount: 1
 IamInstanceProfileName: '{{ InstanceProfile }}'
 SubnetId: '{{ SubnetId }}'
 SecurityGroupIds: '{{ SecurityGroupIds }}'
- name: verifyInstanceManaged
 action: 'aws:waitForAwsResourceProperty'
 timeoutSeconds: 600
 inputs:
 Service: ssm
 Api: DescribeInstanceInformation
 InstanceInformationFilterList:
 - key: InstanceIds
 valueSet:
 - '{{ startInstances.InstanceIds }}'
 PropertySelector: '$.InstanceInformationList[0].PingStatus'
 DesiredValues:
 - Online
 onFailure: 'step:terminateInstance'
- name: installPatches
 action: 'aws:runCommand'
 timeoutSeconds: 7200
 onFailure: Abort
 inputs:
 DocumentName: AWS-RunPatchBaseline
 Parameters:
 SnapshotId: '{{ SnapshotId }}'
 RebootOption: '{{ RebootOption }}'
 Operation: '{{ Operation }}'
 InstanceIds:
 - '{{ startInstances.InstanceIds }}'
- name: stopInstance
 action: 'aws:changeInstanceState'
 maxAttempts: 1
 onFailure: Continue
 inputs:
```

```

 InstanceIds:
 - '{{ startInstances.InstanceIds }}'
 DesiredState: stopped
- name: createImage
 action: 'aws:createImage'
 maxAttempts: 1
 onFailure: Continue
 inputs:
 InstanceId: '{{ startInstances.InstanceIds }}'
 ImageName: '{{ NewAMI }}'
 NoReboot: false
 ImageDescription: Patched AMI created by Automation
- name: terminateInstance
 action: 'aws:changeInstanceState'
 maxAttempts: 1
 onFailure: Continue
 inputs:
 InstanceIds:
 - '{{ startInstances.InstanceIds }}'
 DesiredState: terminated
- name: updateASG
 action: 'aws:executeScript'
 timeoutSeconds: 300
 maxAttempts: 1
 onFailure: Abort
 inputs:
 Runtime: python3.11
 Handler: update_asg
 InputPayload:
 TargetASG: '{{TargetASG}}'
 NewAMI: '{{createImage.ImageId}}'
 Script: |-
 from __future__ import print_function
 import datetime
 import json
 import time
 import boto3

 # create auto scaling and ec2 client
 asg = boto3.client('autoscaling')
 ec2 = boto3.client('ec2')

 def update_asg(event, context):
 print("Received event: " + json.dumps(event, indent=2))

```

```

 target_asg = event['TargetASG']
 new_ami = event['NewAMI']

 # get object for the ASG we're going to update, filter by name of
target ASG
 asg_query =
asg.describe_auto_scaling_groups(AutoScalingGroupNames=[target_asg])
 if 'AutoScalingGroups' not in asg_query or not
asg_query['AutoScalingGroups']:
 return 'No ASG found matching the value you specified.'

 # gets details of an instance from the ASG that we'll use to model the
new launch template after
 source_instance_id = asg_query.get('AutoScalingGroups')[0]['Instances']
[0]['InstanceId']
 instance_properties = ec2.describe_instances(
 InstanceIds=[source_instance_id]
)
 source_instance = instance_properties['Reservations'][0]['Instances']
[0]

 # create list of security group IDs
 security_groups = []
 for group in source_instance['SecurityGroups']:
 security_groups.append(group['GroupId'])

 # create a list of dictionary objects for block device mappings
 mappings = []
 for block in source_instance['BlockDeviceMappings']:
 volume_query = ec2.describe_volumes(
 VolumeIds=[block['Ebs']['VolumeId']]
)
 volume_details = volume_query['Volumes']
 device_name = block['DeviceName']
 volume_size = volume_details[0]['Size']
 volume_type = volume_details[0]['VolumeType']
 device = {'DeviceName': device_name, 'Ebs': {'VolumeSize':
volume_size, 'VolumeType': volume_type}}
 mappings.append(device)

 # create new launch template using details returned from instance in
the ASG and specify the newly patched AMI
 time_stamp = time.time()

```

```

 time_stamp_string =
datetime.datetime.fromtimestamp(time_stamp).strftime('%m-%d-%Y_%H-%M-%S')
 new_template_name = f'{new_ami}_{time_stamp_string}'
 try:
 ec2.create_launch_template(
 LaunchTemplateName=new_template_name,
 LaunchTemplateData={
 'BlockDeviceMappings': mappings,
 'ImageId': new_ami,
 'InstanceType': source_instance['InstanceType'],
 'IamInstanceProfile': {
 'Arn': source_instance['IamInstanceProfile']['Arn']
 },
 'KeyName': source_instance['KeyName'],
 'SecurityGroupIds': security_groups
 }
)
 except Exception as e:
 return f'Exception caught: {str(e)}'
 else:
 # update ASG to use new launch template
 asg.update_auto_scaling_group(
 AutoScalingGroupName=target_asg,
 LaunchTemplate={
 'LaunchTemplateName': new_template_name
 }
)
 return f'Updated ASG {target_asg} with new launch template
 {new_template_name} which uses AMI {new_ami}.'
outputs:
- createImage.ImageId

```

8. Scegli Crea automazione.
9. Nel pannello di navigazione, scegli Automazione, quindi Esegui automazione.
10. Nella pagina Choose document (Scegli il documento), scegli la scheda Owned by me (Di mia proprietà).
11. Cerca il PatchAMIAndUpdateASG runbook e seleziona il pulsante nella PatchAMIAndUpdateASG scheda.
12. Scegli Next (Successivo).
13. Scegliere Simple execution (Esecuzione semplice).

14. Specifica i valori per il parametro di input. Assicurarsi che SubnetId e SecurityGroupIds da te specificati consentano l'accesso agli endpoint pubblici di Systems Manager o agli endpoint dell'interfaccia per Systems Manager.
15. Scegli Esegui.
16. Una volta completata l'automazione, nella console di Amazon EC2 scegli Dimensionamento automatico, quindi scegli Modelli di avvio. Controllare che il nuovo modello di avvio sia visualizzato e utilizzato dalla nuova AMI.
17. Scegli Dimensionamento automatico, quindi scegli Gruppi Auto Scaling. Accertati che il gruppo Auto Scaling utilizzi il nuovo modello di avvio.
18. Termina una o più istanze nel gruppo Auto Scaling. Le istanze di sostituzione verranno avviate utilizzando la nuova AMI.

## Utilizzo Supporto AWS runbook self-service

Questa sezione descrive come utilizzare alcune delle automazioni self-service create dal team. Supporto AWS Queste automazioni ti aiutano a gestire le tue risorse. AWS

### Support Automation Workflows

I Support Automation Workflows (SAW) sono runbook di automazione scritti e gestiti dal team. Supporto AWS Questi runbook ti aiutano a risolvere i problemi più comuni relativi alle tue AWS risorse, a monitorare e identificare in modo proattivo i problemi di rete, a raccogliere e analizzare i log e altro ancora.

I runbook SAW utilizzano il prefisso **AWSsupport**. Ad esempio, [AWSsupport-ActivateWindowsWithAmazonLicense](#).

Inoltre, i clienti con piani di supporto Business Support+ e superiori AWS hanno accesso anche ai runbook che utilizzano il prefisso. **AWSPremiumSupport** Ad esempio, [AWSPremiumSupport-TroubleshootEC2DiskUsage](#).

Per saperne di più Supporto AWS, consulta [Guida introduttiva con. Supporto AWS](#)

### Esecuzione dello strumento EC2Rescue su istanze non raggiungibili

EC2Rescue consente di diagnosticare e risolvere i problemi relativi alle istanze di Amazon Elastic Compute Cloud (Amazon EC2) per Linux e Windows Server. È possibile eseguire lo

strumento manualmente, come descritto nelle sezioni di [Uso di EC2Rescue per Linux Server](#) e di [Uso di EC2Rescue per Windows Server](#). In alternativa, è possibile eseguire lo strumento automaticamente utilizzando il servizio di automazione di Systems Manager e il runbook **AWSSupport-ExecuteEC2Rescue**. L'automazione è uno strumento di AWS Systems Manager. Il runbook **AWSSupport-ExecuteEC2Rescue** è stato progettato per eseguire una combinazione di operazioni di Systems Manager, operazioni CloudFormation e funzioni Lambda per automatizzare le fasi normalmente richieste per l'uso di EC2Rescue.

È possibile utilizzare il runbook **AWSSupport-ExecuteEC2Rescue** per risolvere e potenzialmente correggere i vari tipi di problemi a livello di sistema operativo (SO). Le istanze con volumi root crittografati non sono supportate. Per un elenco completo, consulta i seguenti argomenti:

Windows: consulta la sezione sull'operazione di recupero nell'argomento relativo all'[uso di EC2Rescue per Windows Server con la riga di comando](#).

Linux e macOS: alcuni moduli di EC2Rescue per Linux rilevano i problemi e cercano di risolverli. Per ulteriori informazioni, consulta la documentazione relativa a [aws-ec2rescue-linux](#) per ciascun modulo su GitHub.

Come funziona

Risoluzione dei problemi di un'istanza con il servizio di automazione e il runbook **AWSSupport-ExecuteEC2Rescue** funziona nel seguente modo:

- L'utente specifica l'ID dell'istanza non raggiungibile e avvia il runbook.
- Il sistema crea un VPC temporaneo e quindi esegue una serie di funzioni Lambda per configurare il VPC.
- Il sistema identifica una sottorete per il VPC temporaneo nella stessa zona di disponibilità dell'istanza originale.
- Il sistema avvia un'istanza temporanea di SSM-enabled supporto.
- Il sistema arresta l'istanza originale e crea un backup. Collega quindi il volume root originale all'istanza helper.
- Il sistema utilizza Run Command per eseguire EC2Rescue sull'istanza helper. EC2Rescue identifica e tenta di risolvere i problemi nel volume root originale collegato. Al termine, EC2Rescue collega di nuovo il volume root all'istanza originale.
- Il sistema riavvia l'istanza originale e termina l'istanza temporanea. Il sistema termina anche il VPC temporaneo e le funzioni Lambda create all'inizio dell'automazione.

## Prima di iniziare

Prima di eseguire la seguente automazione, esegui le seguenti operazioni:

- Copiare l'ID istanza dell'istanza non raggiungibile. Specificate questo ID nella procedura.
- Facoltativamente, recuperare l'ID di una sottorete nella stessa zona di disponibilità dell'istanza non raggiungibile. L'istanza EC2Rescue verrà creata in questa sottorete. Se non specifichi una sottorete, Automation crea un nuovo VPC temporaneo nel tuo Account AWS. Verifica che il tuo Account AWS sia disponibile almeno un VPC. Per impostazione predefinita, in una Regione è possibile creare cinque VPC. Se nella Regione sono già stati creati cinque VPC, l'automazione avrà esito negativo e non verrà apportata alcuna modifica all'istanza. Per ulteriori informazioni sulle quote di Amazon VPC, consulta l'argomento relativo a [VPC e sottoreti](#) nella Guida utente Amazon VPC.
- Facoltativamente, puoi creare e specificare un ruolo AWS Identity and Access Management (IAM) per l'automazione. Se non si specifica questo ruolo, il servizio di automazione viene eseguito nel contesto dell'utente che ha eseguito l'automazione.

Concessione delle autorizzazioni **AWSSupport-EC2Rescue** per eseguire operazioni sulle istanze

EC2Rescue deve disporre dell'autorizzazione per eseguire una serie di operazioni sulle istanze durante l'esecuzione del servizio di automazione. Queste azioni richiamano i AWS Lambda servizi IAM e Amazon EC2 per tentare in modo sicuro e protetto di risolvere i problemi con le tue istanze. Se disponi Administrator-level delle autorizzazioni nel tuo Account AWS and/or VPC, potresti essere in grado di eseguire l'automazione senza configurare le autorizzazioni, come descritto in questa sezione. Se non disponi Administrator-level delle autorizzazioni, tu o un amministratore dovete configurare le autorizzazioni utilizzando una delle seguenti opzioni.

- [Concessione delle autorizzazioni mediante policy IAM](#)
- [Concessione delle autorizzazioni utilizzando un CloudFormation modello](#)

### Concessione delle autorizzazioni mediante policy IAM

È possibile collegare la seguente policy IAM all'utente, al gruppo o al ruolo come policy inline. In alternativa, è possibile creare una nuova policy gestita IAM e collegarla all'utente, al gruppo o al ruolo. Per ulteriori informazioni sull'aggiunta di una policy inline all'utente, al gruppo o al ruolo, consulta la pagina [Utilizzo delle policy inline](#). Per ulteriori informazioni sulla creazione di una nuova policy gestita, consulta la sezione relativa all'[uso di policy gestite](#).

 Note

Se crei una nuova policy gestita da IAM, devi anche allegare la policy AmazonSSMAutomationRole gestita in modo che le tue istanze possano comunicare con l'API Systems Manager.

## Policy IAM per AWSSupport-EC2Rescue

*account ID* Sostituiscila con le tue informazioni.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Action": [
 "lambda:InvokeFunction",
 "lambda:DeleteFunction",
 "lambda:GetFunction"
],
 "Resource": "arn:aws:lambda:*:111122223333:function:AWSSupport-
EC2Rescue-*",
 "Effect": "Allow"
 },
 {
 "Action": [
 "s3:GetObject",
 "s3:GetObjectVersion"
],
 "Resource": [
 "arn:aws:s3:::awssupport-ssm.*/*.template",
 "arn:aws:s3:::awssupport-ssm.*/*.zip"
],
 "Effect": "Allow"
 },
 {
 "Action": [
 "iam:CreateRole",
 "iam:CreateInstanceProfile",
 "iam:GetRole",
```



```

 "iam:GetInstanceProfile",
 "iam:PutRolePolicy",
 "iam:DetachRolePolicy",
 "iam:AttachRolePolicy",
 "iam:PassRole",
 "iam:AddRoleToInstanceProfile",
 "iam:RemoveRoleFromInstanceProfile",
 "iam>DeleteRole",
 "iam>DeleteRolePolicy",
 "iam>DeleteInstanceProfile"
],
 "Resource": [
 "arn:aws:iam::111122223333:role/AWSSupport-EC2Rescue-*",
 "arn:aws:iam::111122223333:instance-profile/AWSSupport-EC2Rescue-
*"
],
 "Effect": "Allow"
},
{
 "Action": [
 "lambda:CreateFunction",
 "ec2:CreateVpc",
 "ec2:ModifyVpcAttribute",
 "ec2>DeleteVpc",
 "ec2:CreateInternetGateway",
 "ec2:AttachInternetGateway",
 "ec2:DetachInternetGateway",
 "ec2>DeleteInternetGateway",
 "ec2:CreateSubnet",
 "ec2>DeleteSubnet",
 "ec2:CreateRoute",
 "ec2>DeleteRoute",
 "ec2:CreateRouteTable",
 "ec2:AssociateRouteTable",
 "ec2:DisassociateRouteTable",
 "ec2>DeleteRouteTable",
 "ec2:CreateVpcEndpoint",
 "ec2>DeleteVpcEndpoints",
 "ec2:ModifyVpcEndpoint",
 "ec2:Describe*",
 "autoscaling:DescribeAutoScalingInstances"
],
 "Resource": "*",
 "Effect": "Allow"
}

```

```
}
]
}
```

## Concessione delle autorizzazioni utilizzando un CloudFormation modello

CloudFormation automatizza il processo di creazione di ruoli e policy IAM utilizzando un modello preconfigurato. Utilizza la procedura seguente per creare i ruoli e le policy IAM richiesti per il servizio di automazione di EC2Rescue utilizzando CloudFormation.

Per creare i ruoli e le policy IAM per EC2Rescue

1. Scaricare [AWSSupport-EC2RescueRole.zip](#) ed estrarre il file `AWSSupport-EC2RescueRole.json` in una directory sul computer locale.
2. Se il tuo Account AWS trovi in una partizione speciale, modifica il modello per cambiare i valori ARN con quelli della tua partizione.

Ad esempio, per le regioni della Cina, modificare i casi da `arn:aws` a `arn:aws-cn`.

3. Accedi Console di gestione AWS e apri la console all'indirizzo. CloudFormation <https://console.aws.amazon.com/cloudformation>
4. Scegliere Create stack (Crea stack), With new resources (standard) (Con nuove risorse (standard)).
5. Nella pagina Create stack (Crea stack) per Prerequisite - Prepare template (Prerequisito - Prepara modello), scegliere Template is ready (Il modello è pronto).
6. In Specify template (Specifica il modello), scegliere Upload a template file (Carica un file modello).
7. Scegliere Choose file (Scegli file), quindi individuare e selezionare il file `AWSSupport-EC2RescueRole.json` dalla directory in cui è stato estratto.
8. Scegliere Next (Successivo).
9. Nella pagina Specify stack details (Specifica i dettagli dello stack), per il campo Stack name (Nome stack) inserire un nome per identificare lo stack, quindi scegliere Next (Successivo).
10. (Facoltativo) Nell'area Tag, applica una o più name/value coppie di tag key allo stack.

I tag sono metadati facoltativi assegnati a una risorsa. I tag consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Ad esempio,

è possibile applicare un tag uno stack per identificare il tipo di attività che esegue, i tipi di destinazioni o altre risorse coinvolte e l'ambiente in cui viene eseguito.

11. Seleziona Next (Successivo).
12. Nella pagina di revisione, rivedi i dettagli dello stack, quindi scorri verso il basso e scegli l'opzione Riconosco che CloudFormation potrebbe creare risorse IAM.
13. Seleziona Crea stack.

CloudFormation mostra lo stato `CREATE_IN_PROGRESS` per alcuni minuti. Dopo la creazione dello stack, lo stato diventa `CREATE_COMPLETE`. È inoltre possibile scegliere l'icona di aggiornamento per verificare lo stato del processo di creazione.

14. Nell'elenco Stacks, scegliere il pulsante di opzione accanto allo stack appena creato e quindi scegliere la scheda Outputs.
15. Annotare il valore. È l'ARN di `AssumeRole`. Si specifica questo ARN quando si esegue l'automazione nella procedura successiva, [Esecuzione del servizio di automazione](#).

## Esecuzione del servizio di automazione

### Important

La seguente automazione arresta l'istanza non raggiungibile. L'arresto dell'istanza può causare la perdita di dati sui volumi dell'archivio dell'istanza collegati (se presenti). L'arresto dell'istanza può causare anche la modifica dell'indirizzo IP pubblico se non è associato alcun indirizzo IP elastico.

## Esecuzione del servizio di automazione **AWSsupport-ExecuteEC2Rescue**.

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Automazione.
3. Scegli Esegui automazione.
4. Nella sezione Automation document (Documento di automazione) scegliere Owned by Amazon (Di proprietà di Amazon) nell'elenco.
5. Nell'elenco dei runbook scegliere il pulsante nella scheda per **AWSsupport-ExecuteEC2Rescue**, quindi scegliere Next (Successivo).

6. Nella pagina **Execute automation document** (Esegui documento di automazione), scegliere **Simple execution** (Esecuzione semplice).
7. Nella sezione **Document details** (Dettagli documento) verificare che l'opzione **Document version** (Versione documento) sia impostata sulla versione predefinita con il numero più alto. Ad esempio, `$DEFAULT` o `3` (default).
8. Nella sezione **Input parameters** (Parametri di input), specificare i seguenti parametri:
  - a. Per `UnreachableInstanceId`, specifica l'ID dell'istanza irraggiungibile.
  - b. (Facoltativo) Per `EC2RescueInstanceType`, specificare un tipo di istanza per l'istanza `EC2Rescue`. Il tipo di istanza di default è `t2.medium`.
  - c. Infatti `AutomationAssumeRole`, se hai creato i ruoli per questa automazione utilizzando la CloudFormation procedura descritta in precedenza in questo argomento, scegli l'ARN dell'automazione `AssumeRole` che hai creato nella console. CloudFormation
  - d. (Facoltativo) Per `LogDestination`, specifica un bucket S3 se desideri raccogliere i log a livello di sistema operativo durante la risoluzione dei problemi dell'istanza. I log vengono automaticamente caricati nel bucket specificato.
  - e. Per `SubnetId`, specifica una sottorete in un VPC esistente nella stessa zona di disponibilità dell'istanza irraggiungibile. Per impostazione predefinita, Systems Manager crea un nuovo VPC, ma è possibile specificare una sottorete in un VPC esistente.

 **Note**

Se l'opzione per specificare un bucket o un ID di sottorete non è disponibile, verificare nel campo **Default** (Impostazione predefinita) che si stia utilizzando la versione più recente del runbook.

9. (Facoltativo) Nell'area **Tag**, applica una o più **name/value** coppie di chiavi tag per aiutare a identificare l'automazione, ad esempio. `Key=Purpose, Value=EC2Rescue`
10. Scegliere **Execute** (Esegui).

Il runbook crea un backup dell'AMI come parte dell'automazione. Tutte le altre risorse create dall'automazione vengono eliminate automaticamente, ma questa AMI rimane nell'account in uso. All'AMI viene assegnato un nome utilizzando la seguente convenzione:

AMI di backup AWSSupport-EC2Rescue: *UnreachableInstanceId*

È possibile individuare questa AMI nella console Amazon EC2 cercando l'ID di esecuzione dell'automazione.

## Ripristino di password e chiavi SSH sulle istanze EC2

È possibile utilizzare il runbook `AWSSupport-ResetAccess` per riabilitare automaticamente la generazione della password dell'amministratore locale sulle istanze Amazon Elastic Compute Cloud (Amazon EC2) per Windows Server e per generare una nuova chiave SSH sulle istanze EC2 per Linux. Il `AWSSupport-ResetAccess` runbook è progettato per eseguire una combinazione di AWS Systems Manager azioni, AWS CloudFormation azioni e AWS Lambda funzioni che automatizzano i passaggi normalmente necessari per reimpostare la password dell'amministratore locale.

Puoi usare Automation con il `AWSSupport-ResetAccess` runbook per risolvere i seguenti problemi:

### Windows

Hai perso la coppia di chiavi EC2: per risolvere questo problema, puoi utilizzare il `AWSSupport-ResetAccess` runbook per creare una password abilitata AMI dall'istanza corrente, avviare una nuova istanza dall'AMI e selezionare una coppia di chiavi di tua proprietà.

Perdita della password dell'amministratore locale: per risolvere questo problema, è possibile utilizzare il runbook `AWSSupport-ResetAccess` per generare una nuova password che può essere decrittografata mediante la coppia di chiavi EC2 corrente.

### Linux

Hai perso la coppia di chiavi EC2 o hai configurato l'accesso SSH all'istanza con una chiave persa: per risolvere questo problema, puoi utilizzare il `AWSSupport-ResetAccess` runbook per creare una nuova chiave SSH per l'istanza corrente, che ti consente di connetterti nuovamente all'istanza.

#### Note

Se l'istanza EC2 per Windows Server è configurata per Systems Manager, è anche possibile reimpostare la password dell'amministratore locale utilizzando `EC2Rescue` e AWS Systems Manager Run Command. Per ulteriori informazioni, consulta [Utilizzo di EC2Rescue per Windows Server con Systems Manager Run Command](#) nella Guida per l'utente di Amazon EC2.

## Informazioni correlate

[Connessione all'istanza Linux da Windows tramite PuTTY](#) nella Guida per l'utente di Amazon EC2

### Come funziona

Risoluzione dei problemi di un'istanza con il servizio di automazione e il runbook AWSsupport-ResetAccess funziona nel seguente modo:

- L'utente specifica l'ID dell'istanza ed esegue il runbook.
- Il sistema crea un VPC temporaneo e quindi esegue una serie di funzioni Lambda per configurare il VPC.
- Il sistema identifica una sottorete per il VPC temporaneo nella stessa zona di disponibilità dell'istanza originale.
- Il sistema avvia un'istanza temporanea di supporto. SSM-enabled
- Il sistema arresta l'istanza originale e crea un backup. Collega quindi il volume root originale all'istanza helper.
- Il sistema utilizza Run Command per eseguire EC2Rescue sull'istanza helper. In Windows, EC2Rescue abilita la generazione della password per l'amministratore locale utilizzando EC2Config o EC2Launch sul volume root originale collegato. In Linux, EC2Rescue genera e implementa una nuova chiave SSH e salva la chiave privata, crittografata, in Parameter Store. Al termine, EC2Rescue collega di nuovo il volume root all'istanza originale.
- Il sistema crea una nuova Amazon Machine Image (AMI) dell'istanza, ora che la generazione delle password è abilitata. È possibile usare questa AMI per creare una nuova istanza EC2 e associare una nuova coppia di chiavi, se necessario.
- Il sistema riavvia l'istanza originale e termina l'istanza temporanea. Il sistema termina anche il VPC temporaneo e le funzioni Lambda create all'inizio dell'automazione.
- Windows: l'istanza genera una nuova password che è possibile decodificare dalla console Amazon EC2 utilizzando la coppia di chiavi corrente assegnata all'istanza.

Linux: è possibile accedere all'istanza tramite SSH utilizzando la chiave SSH memorizzata in Systems Manager Parameter Store come `key. ec2r/openssh instance ID`

### Prima di iniziare

Prima di eseguire la seguente automazione, esegui le seguenti operazioni:

- Copiare l'ID istanza dell'istanza per la quale si desidera reimpostare la password dell'amministratore. Specificate questo ID nella procedura.
- Facoltativamente, recuperare l'ID di una sottorete nella stessa zona di disponibilità dell'istanza non raggiungibile. L'istanza EC2Rescue verrà creata in questa sottorete. Se non specifichi una sottorete, Automation crea un nuovo VPC temporaneo nel tuo Account AWS. Verifica che il tuo Account AWS sia disponibile almeno un VPC. Per impostazione predefinita, in una Regione è possibile creare cinque VPC. Se nella Regione sono già stati creati cinque VPC, l'automazione avrà esito negativo e non verrà apportata alcuna modifica all'istanza. Per ulteriori informazioni sulle quote di Amazon VPC, consulta l'argomento relativo a [VPC e sottoreti](#) nella Guida utente Amazon VPC.
- Facoltativamente, puoi creare e specificare un ruolo AWS Identity and Access Management (IAM) per l'automazione. Se non si specifica questo ruolo, il servizio di automazione viene eseguito nel contesto dell'utente che ha eseguito l'automazione.

Concessione AWSSupport-EC2Rescue delle autorizzazioni per eseguire azioni sulle istanze

EC2Rescue deve disporre dell'autorizzazione per eseguire una serie di operazioni sulle istanze durante l'esecuzione del servizio di automazione. Queste azioni richiamano i servizi AWS Lambda, IAM e Amazon EC2 per tentare in modo sicuro e protetto di risolvere i problemi con le tue istanze. Se disponi Administrator-level delle autorizzazioni nel tuo Account AWS and/or VPC, potresti essere in grado di eseguire l'automazione senza configurare le autorizzazioni, come descritto in questa sezione. Se non disponi Administrator-level delle autorizzazioni, tu o un amministratore dovete configurare le autorizzazioni utilizzando una delle seguenti opzioni.

- [Concessione delle autorizzazioni mediante policy IAM](#)
- [Concessione delle autorizzazioni utilizzando un CloudFormation modello](#)

Concessione delle autorizzazioni mediante policy IAM

È possibile collegare la seguente policy IAM all'utente, al gruppo o al ruolo come policy inline. In alternativa, è possibile creare una nuova policy gestita IAM e collegarla all'utente, al gruppo o al ruolo. Per ulteriori informazioni sull'aggiunta di una policy inline all'utente, al gruppo o al ruolo, consulta la pagina [Utilizzo delle policy inline](#). Per ulteriori informazioni sulla creazione di una nuova policy gestita, consulta la sezione relativa all'[uso di policy gestite](#).

 Note

Se crei una nuova policy gestita da IAM, devi anche allegare la policy `AmazonSSMAutomationRole` gestita in modo che le tue istanze possano comunicare con l'API Systems Manager.

Policy IAM per **AWSSupport-ResetAccess**

*account ID* Sostituiscila con le tue informazioni.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Action": [
 "lambda:InvokeFunction",
 "lambda:DeleteFunction",
 "lambda:GetFunction"
],
 "Resource": "arn:aws:lambda:*:111122223333:function:AWSSupport-
EC2Rescue-*",
 "Effect": "Allow"
 },
 {
 "Action": [
 "s3:GetObject",
 "s3:GetObjectVersion"
],
 "Resource": [
 "arn:aws:s3:::awssupport-ssm.*/*.template",
 "arn:aws:s3:::awssupport-ssm.*/*.zip"
],
 "Effect": "Allow"
 },
 {
 "Action": [
 "iam:CreateRole",
 "iam:CreateInstanceProfile",
 "iam:GetRole",
```



```

 "iam:GetInstanceProfile",
 "iam:PutRolePolicy",
 "iam:DetachRolePolicy",
 "iam:AttachRolePolicy",
 "iam:PassRole",
 "iam:AddRoleToInstanceProfile",
 "iam:RemoveRoleFromInstanceProfile",
 "iam>DeleteRole",
 "iam>DeleteRolePolicy",
 "iam>DeleteInstanceProfile"
],
 "Resource": [
 "arn:aws:iam::111122223333:role/AWSSupport-EC2Rescue-*",
 "arn:aws:iam::111122223333:instance-profile/AWSSupport-EC2Rescue-
*"
],
 "Effect": "Allow"
},
{
 "Action": [
 "lambda:CreateFunction",
 "ec2:CreateVpc",
 "ec2:ModifyVpcAttribute",
 "ec2>DeleteVpc",
 "ec2:CreateInternetGateway",
 "ec2:AttachInternetGateway",
 "ec2:DetachInternetGateway",
 "ec2>DeleteInternetGateway",
 "ec2:CreateSubnet",
 "ec2>DeleteSubnet",
 "ec2:CreateRoute",
 "ec2>DeleteRoute",
 "ec2:CreateRouteTable",
 "ec2:AssociateRouteTable",
 "ec2:DisassociateRouteTable",
 "ec2>DeleteRouteTable",
 "ec2:CreateVpcEndpoint",
 "ec2>DeleteVpcEndpoints",
 "ec2:ModifyVpcEndpoint",
 "ec2:Describe*"
],
 "Resource": "*",
 "Effect": "Allow"
}

```

```
]
}
```

## Concessione delle autorizzazioni utilizzando un CloudFormation modello

CloudFormation automatizza il processo di creazione di ruoli e policy IAM utilizzando un modello preconfigurato. Utilizza la procedura seguente per creare i ruoli e le policy IAM richiesti per il servizio di automazione di EC2Rescue utilizzando CloudFormation.

Per creare i ruoli e le policy IAM per EC2Rescue

1. Scaricare [AWSSupport-EC2RescueRole.zip](#) ed estrarre il file `AWSSupport-EC2RescueRole.json` in una directory sul computer locale.
2. Se ti Account AWS trovi in una partizione speciale, modifica il modello per cambiare i valori ARN con quelli della tua partizione.

Ad esempio, per le regioni della Cina, modificare i casi da `arn:aws` a `arn:aws-cn`.

3. Accedi Console di gestione AWS e apri la console all'indirizzo. CloudFormation <https://console.aws.amazon.com/cloudformation>
4. Scegliere Create stack (Crea stack), With new resources (standard) (Con nuove risorse (standard)).
5. Nella pagina Create stack (Crea stack) per Prerequisite - Prepare template (Prerequisito - Prepara modello), scegliere Template is ready (Il modello è pronto).
6. In Specify template (Specifica il modello), scegliere Upload a template file (Carica un file modello).
7. Scegliere Choose file (Scegli file), quindi individuare e selezionare il file `AWSSupport-EC2RescueRole.json` dalla directory in cui è stato estratto.
8. Scegliere Next (Successivo).
9. Nella pagina Specify stack details (Specifica i dettagli dello stack), per il campo Stack name (Nome stack) inserire un nome per identificare lo stack, quindi scegliere Next (Successivo).
10. (Facoltativo) Nell'area Tag, applica una o più name/value coppie di tag key allo stack.

I tag sono metadati facoltativi assegnati a una risorsa. I tag consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Ad esempio, è possibile applicare un tag uno stack per identificare il tipo di attività che esegue, i tipi di destinazioni o altre risorse coinvolte e l'ambiente in cui viene eseguito.

11. Seleziona Next (Successivo).
12. Nella pagina di revisione, rivedi i dettagli dello stack, quindi scorri verso il basso e scegli l'opzione Riconosco che CloudFormation potrebbe creare risorse IAM.
13. CloudFormation mostra lo stato CREATE\_IN\_PROGRESS per alcuni minuti. Dopo la creazione dello stack, lo stato diventa CREATE\_COMPLETE. È inoltre possibile scegliere l'icona di aggiornamento per verificare lo stato del processo di creazione.
14. Nell'elenco degli stack, scegliere l'opzione accanto allo stack appena creato e quindi scegliere la scheda Outputs (Output).
15. Copiare il valore visualizzato nel campo Value (Valore). È l'ARN di AssumeRole Specifica questo ARN quando esegui l'automazione.

## Esecuzione del servizio di automazione

La procedura seguente descrive come seguire runbook AWSSupport-ResetAccess tramite la console AWS Systems Manager .

### Important

L'esecuzione della seguente automazione arresta l'istanza. L'arresto dell'istanza può causare la perdita di dati sui volumi dell'archivio dell'istanza collegati (se presenti). L'arresto dell'istanza può causare anche la modifica dell'indirizzo IP pubblico se non è associato alcun indirizzo IP elastico. Per evitare queste modifiche di configurazione, utilizza Run Command per ripristinare l'accesso. Per ulteriori informazioni, consulta [Utilizzo di EC2Rescue per Windows Server con Systems Manager Run Command](#) nella Guida per l'utente di Amazon EC2.

## Per eseguire l'automazione AWSSupport-ResetAccess

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Automazione.
3. Scegli Esegui automazione.
4. Nella sezione Automation document (Documento di automazione) scegliere Owned by Amazon (Di proprietà di Amazon) nell'elenco.

5. Nell'elenco dei runbook scegliere il pulsante nella scheda per AWSSupport-ResetAccess, quindi scegliere Next (Successivo).
6. Nella pagina Execute automation document (Esegui documento di automazione), scegliere Simple execution (Esecuzione semplice).
7. Nella sezione Document details (Dettagli documento) verificare che l'opzione Document version (Versione documento) sia impostata sulla versione predefinita con il numero più alto. Ad esempio, \$DEFAULT o 3 (default).
8. Nella sezione Input parameters (Parametri di input), specificare i seguenti parametri:
  - a. Per InstanceId, specificare l'ID dell'istanza non raggiungibile.
  - b. Per SubnetId, specifica una sottorete in un VPC esistente nella stessa zona di disponibilità dell'istanza specificata. Per impostazione predefinita, Systems Manager crea un nuovo VPC, ma è possibile specificare una sottorete in un VPC esistente.

 Note

Se l'opzione per specificare un ID sottorete non è disponibile, verificare nel campo Default (Impostazione predefinita) che si stia utilizzando la versione più recente del runbook.

- c. Per EC2RescueInstanceType, specifica un tipo di istanza per l'istanza EC2Rescue. Il tipo di istanza di default è t2.medium.
  - d. Infatti AssumeRole, se hai creato ruoli per questa automazione utilizzando la CloudFormation procedura descritta in precedenza in questo argomento, specifica l'AssumeRole ARN che hai annotato nella console. CloudFormation
9. (Facoltativo) Nell'area Tag, applica una o più name/value coppie di chiavi tag per aiutare a identificare l'automazione, ad esempio Key=Purpose, Value=ResetAccess.
10. Scegliere Execute (Esegui).
11. Per monitorare lo stato di avanzamento dell'automazione, scegliere l'automazione in esecuzione e quindi scegliere la scheda Steps (Fasi). Al termine dell'automazione, scegliere la scheda Descriptions (Descrizioni), quindi View output (Visualizza output) per visualizzare i risultati. Per visualizzare l'output delle singole fasi, scegliere la scheda Steps (Fasi), quindi scegliere View Outputs (Visualizza output) accanto a una fase.

Il runbook crea un backup di AMI e un'AMI abilitata mediante password come parte dell'automazione. Tutte le altre risorse create dall'automazione vengono eliminate automaticamente, ma queste AMIs rimangono nell'account in uso. Alle AMIs viene assegnato un nome utilizzando le seguenti convenzioni:

- Backup AMI: `AWSSupport-EC2Rescue:InstanceID`
- Password-enabled AMI `AWSSupport-EC2Rescue: Password-enabled AMI di Instance ID`

È possibile individuare queste AMIs nella console cercando l'ID di esecuzione del servizio di automazione.

Per Linux, la nuova chiave SSH privata per l'istanza viene salvata e crittografata in Parameter Store. Il nome del parametro è `/ec2r/openssh/instance ID/key`.

Trasmissione dei dati ad Automazione tramite trasformatori di input

Questo tutorial sull' AWS Systems Manager automazione mostra come utilizzare la funzionalità di trasformazione di input di Amazon EventBridge per estrarre un'istanza `instance-id` di Amazon Elastic Compute Cloud (Amazon EC2) da un evento di modifica dello stato dell'istanza. L'automazione è uno strumento di AWS Systems Manager. Usiamo il trasformatore di input per passare i dati alla destinazione del runbook `AWS-CreateImage` come parametro di input `InstanceId`. La regola viene attivata quando un'istanza passa allo stato `stopped`.

Per ulteriori informazioni sull'utilizzo dei trasformatori di ingresso, consulta [Tutorial: Use Input Transformer to Customize What is Passed to the Event Target](#) nella Amazon User Guide. EventBridge

Prima di iniziare

Verifica di aver aggiunto le autorizzazioni e la politica di fiducia richieste per EventBridge il tuo ruolo di servizio Systems Manager Automation. Per ulteriori informazioni, consulta la [panoramica sulla gestione delle autorizzazioni di accesso alle EventBridge risorse](#) nella Amazon EventBridge User Guide.

Per utilizzare i trasformatori di input con il servizio di automazione

1. Apri la EventBridge console Amazon all'indirizzo. <https://console.aws.amazon.com/events/>
2. Nel pannello di navigazione, scegli Regole.
3. Scegli Crea regola.

4. Inserisci un nome e una descrizione per la regola.

Una regola non può avere lo stesso nome di un'altra regola nella stessa Regione e sullo stesso router di eventi.

5. Per Router di eventi, seleziona il router di eventi che desideri associare a questa regola. Se desideri che questa regola risponda agli eventi corrispondenti che provengono dai tuoi Account AWS, seleziona **predefinito**. Quando un Servizio AWS utente del tuo account emette un evento, viene sempre indirizzato al bus eventi predefinito del tuo account.
6. Per Tipo di regola, scegli **Regola con un modello di eventi**.
7. Scegli **Avanti**.
8. Per Origine degli eventi, scegli **AWS eventi** o **eventi EventBridge partner**.
9. Nella sezione **Modello di eventi**, scegli **Modulo di modello di eventi**.
10. Per Event source (Origine evento), scegli **AWS services (Servizi)**.
11. Per Servizio AWS, scegli **EC2**.
12. Per il tipo di evento, scegli **State-change Notifica dell'istanza EC2**.
13. Per Specifica del tipo di evento 1, seleziona **Stati specifici**, quindi scegli **arrestato**.
14. Per Specifica del tipo di evento 2, seleziona **Qualsiasi istanza** oppure seleziona **ID specifici dell'istanza** e immetti gli ID delle istanze da monitorare.
15. Scegli **Avanti**.
16. Per Tipi di destinazione, scegli **servizio AWS**.
17. Per Seleziona destinazione, scegli **Automazione di Systems Manager**.
18. Per Document (Documento), scegli **AWS-CreatImage**.
19. Nella sezione **Configure automation parameter(s) (Configurazione dei parametri di automazione)**, **Input Transformer (Trasformatore di input)**.
20. Per Input path (Percorso di input) inserisci **{"instance":"\$.detail.instance-id"}**.
21. Per Template (Modello) inserisci **{"InstanceId":[<instance>]}**.
22. Per Ruolo di esecuzione, scegli **Utilizza ruolo esistente** e quindi il ruolo di servizio di automazione.
23. Scegli **Avanti**.
24. (Facoltativo) Inserire uno o più tag per la regola. Per ulteriori informazioni, consulta [Tagging Your Amazon EventBridge Resources](#) nella Amazon EventBridge User Guide.
25. Scegli **Avanti**.

26. Rivedi i dettagli della regola e scegli Crea regola.

## Scopri gli stati restituiti da Systems Manager Automation

AWS Systems Manager L'automazione riporta informazioni dettagliate sullo stato dei vari stati attraversati da un'azione o da un passaggio di automazione quando si esegue un'automazione e per l'automazione complessiva. L'automazione è uno strumento di AWS Systems Manager. È possibile monitorare gli stati dell'automazione usando i metodi seguenti:

- Monitoraggio di Execution status (Stato dell'esecuzione) nella console del servizio di automazione di Systems Manager.
- Utilizzare gli strumenti a riga di comando preferiti. Per AWS Command Line Interface (AWS CLI), puoi utilizzare [describe-automation-step-executions o get-automation-execution](https://docs.aws.amazon.com/cli/latest/reference/ssm/get-automation-execution.html). <https://docs.aws.amazon.com/cli/latest/reference/ssm/get-automation-execution.html> Per, [Get-SSMAutomationStepExecution](#) puoi [Get-SSMAutomationExecution](#) usare o. AWS Tools for Windows PowerShell
- Configura Amazon EventBridge per rispondere alle modifiche dello stato delle azioni o dell'automazione.

Per ulteriori informazioni sulla gestione dei timeout in un'automazione, consulta [Gestione dei timeout nei runbook](#).

### Informazioni sugli stati di automazione

L'automazione riporta i dettagli sullo stato delle singole azioni di automazione oltre all'automazione complessiva.

Lo stato complessivo dell'automazione può essere diverso rispetto allo stato segnalato da una singola operazione o fase, come indicato nelle tabelle seguenti.

### Stato dettagliato delle operazioni

| Stato               | Informazioni                                                                                                                                                               |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pending (In attesa) | La fase non ha avviato l'esecuzione. Se l'automazione utilizza operazioni condizionali, le fasi rimangono in questo stato dopo che un'automazione è stata completata se la |

| Stato                        | Informazioni                                                                                                                                                                                                                                                                  |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | condizione non è stata soddisfatta per eseguire la fase. Le fasi rimangono anche in questo stato se l'automazione viene annullata prima dell'esecuzione della fase.                                                                                                           |
| InProgress                   | La fase è in esecuzione.                                                                                                                                                                                                                                                      |
| Waiting (In attesa)          | La fase è in attesa di input.                                                                                                                                                                                                                                                 |
| Completato                   | La fase ha esito positivo. Si tratta di uno stato terminale.                                                                                                                                                                                                                  |
| TimedOut                     | Una fase o un'approvazione non è stata completata prima del periodo di timeout specificato. Si tratta di uno stato terminale.                                                                                                                                                 |
| Cancelling (In annullamento) | La fase è attualmente interrotta dopo essere stata annullata da un richiedente.                                                                                                                                                                                               |
| Cancelled (Annullato)        | La fase è stata interrotta da un richiedente prima del completamento. Si tratta di uno stato terminale.                                                                                                                                                                       |
| Non riuscito                 | La fase non è stata completata correttamente. Si tratta di uno stato terminale.                                                                                                                                                                                               |
| Exited                       | Restituito solo dall'azione <code>aws:loop</code> . Il ciclo non è stato completato per intero. Un passaggio all'interno del ciclo è stato spostato in un passaggio esterno utilizzando le proprietà <code>nextStep</code> , <code>onCancel</code> o <code>onFailure</code> . |

### Stato dettagliato per un'automazione

| Stato               | Informazioni                                |
|---------------------|---------------------------------------------|
| Pending (In attesa) | L'automazione non ha iniziato a funzionare. |



| Stato                        | Informazioni                                                                                                                  |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| InProgress                   | L'automazione è in esecuzione.                                                                                                |
| Waiting (In attesa)          | L'automazione è in attesa di input.                                                                                           |
| Completato                   | L'automazione è stata completata con successo. Si tratta di uno stato terminale.                                              |
| TimedOut                     | Una fase o un'approvazione non è stata completata prima del periodo di timeout specificato. Si tratta di uno stato terminale. |
| Cancelling (In annullamento) | L'automazione si sta attualmente interrompendo dopo essere stata annullata da un richiedente.                                 |
| Annullato                    | L'automazione è stata interrotta da un richiedente prima del completamento. Si tratta di uno stato terminale.                 |
| Non riuscito                 | L'automazione non è stata completata correttamente. Si tratta di uno stato terminale.                                         |

## Risoluzione dei problemi di servizio di automazione di Systems Manager

Utilizza le seguenti informazioni per aiutarti a risolvere i problemi con AWS Systems Manager Automation. Questo argomento include attività di risoluzione dei problemi specifiche in base ai messaggi di errore restituiti dal servizio di automazione.

### Errori comuni del servizio di automazione

Questa sezione include informazioni sugli errori più comuni del servizio di automazione.

#### VPC non definito 400

Per impostazione predefinita, quando Automation esegue il `AWS-UpdateLinuxAmi` runbook o il `AWS-UpdateWindowsAmi` runbook, il sistema crea un'istanza temporanea nel VPC predefinito (172.30.0. 0/16). Se hai eliminato il VPC predefinito, ricevi il seguente errore:

## VPC not defined 400

Per risolvere questo problema, è necessario specificare un valore per il parametro `SubnetId` di input.

## Mancato avvio dell'esecuzione del servizio di automazione

Un'automazione può fallire con un errore di accesso negato o un errore di assunzione del ruolo non valido se i ruoli e le policy AWS Identity and Access Management (IAM) non sono stati configurati correttamente per l'automazione.

### Accesso negato

I seguenti esempi descrivono le situazioni in cui si è verificato il mancato avvio di un'automazione con un errore di accesso negato.

#### Accesso negato all'API Systems Manager

Messaggio di errore: `User: user arn isn't authorized to perform: ssm:StartAutomationExecution on resource: document arn (Service: AWSSimpleSystemsManagement; Status Code: 400; Error Code: AccessDeniedException; Request ID: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx)`

- Possibile causa 1: l'utente che ha cercato di avviare l'automazione non dispone dell'autorizzazione per chiamare l'API `StartAutomationExecution`. Per risolvere questo problema, collega la policy IAM all'utente utilizzato per avviare l'automazione.
- Possibile causa 2: l'utente che ha cercato di avviare l'automazione dispone dell'autorizzazione per chiamare l'API `StartAutomationExecution`, ma non dell'autorizzazione per chiamare l'API mediante il runbook specificato. Per risolvere questo problema, collega la policy IAM all'utente utilizzato per avviare l'automazione.

#### Accesso negato a causa di autorizzazioni mancanti PassRole

Messaggio di errore: `User: user arn isn't authorized to perform: iam:PassRole on resource: automation assume role arn (Service: AWSSimpleSystemsManagement; Status Code: 400; Error Code: AccessDeniedException; Request ID: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx)`

L'utente che tenta di avviare l'automazione non dispone dell'autorizzazione `PassRole` per il ruolo di assunzione. Per risolvere questo problema, associa la policy `iam:PassRole` al ruolo dell'utente.

che tenta di avviare l'automazione. Per ulteriori informazioni, consulta [Attività 2: Associa la PassRole policy iam: al tuo ruolo di automazione](#).

### Ruolo presunto non valido

Quando si esegue un servizio di automazione, un ruolo presunto viene fornito nel runbook oppure viene passato come valore di parametro per il runbook. Si possono verificare vari tipi di errore se il ruolo presunto non è specificato o configurato correttamente.

### Ruolo presunto non valido

Messaggio di errore: The format of the supplied assume role ARN isn't valid. Il formato del ruolo presunto non è valido. Per risolvere questo problema, verifica se un ruolo presunto valido è stato specificato nel runbook oppure come parametro di runtime durante l'avvio dell'automazione.

### Mancato utilizzo del ruolo presunto

Messaggio di errore: The defined assume role is unable to be assumed. (Service: AWSSimpleSystemsManagement; Status Code: 400; Error Code: InvalidAutomationExecutionParametersException; Request ID: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx)

- Possibile causa 1: il ruolo presunto non esiste. Per risolvere questo problema, crea il ruolo. Per ulteriori informazioni, consulta [the section called “Configurazione del servizio di automazione”](#). I dettagli specifici per la creazione di questo ruolo sono descritti nel seguente argomento, [Processo 1: creazione di un ruolo di servizio per il servizio di automazione](#).
- Possibile causa 2: il ruolo presunto non ha una relazione di trust con il servizio Systems Manager. Per risolvere questo problema, crea una relazione di trust. Per ulteriori informazioni, consulta [Non è possibile assumere un ruolo](#) nella Guida per l'utente IAM.

### Esecuzione avviata con stato non valido

### Action-specific guasti

I runbook contengono fasi e fasi eseguite in ordine. Ogni fase richiama una o più API di Servizio AWS. Le API determinano gli input, il comportamento e gli output della fase. Un errore che causa la mancata esecuzione di una fase puoi verificarsi in varie posizioni. I messaggi di errore indicano quando e dove si è verificato un errore.

Per visualizzare un messaggio di errore nella console Amazon Elastic Compute Cloud (Amazon EC2), scegli il collegamento Visualizza output associato alla fase non riuscita. Per visualizzare un messaggio di errore proveniente da AWS CLI, chiama `get-automation-execution` e cerca l'attributo `FailureMessage` in un errore `StepExecution`.

Negli esempi seguenti una fase associata all'operazione `aws:runInstance` è caratterizzata da un'esecuzione non riuscita. Ogni esempio fa riferimento a un tipo di errore diverso.

#### Immagine mancante

Messaggio di errore: Automation Step Execution fails when it's launching the instance(s). Get Exception from RunInstances API of ec2 Service. Exception Message from RunInstances API: [The image id '[ami id]' doesn't exist (Service: AmazonEC2; Status Code: 400; Error Code: InvalidAMIID.NotFound; Request ID: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx)]. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.

L'operazione `aws:runInstances` ha ricevuto input per un valore `ImageId` che non esiste. Per risolvere questo problema, aggiorna il runbook o i valori dei parametri con l'ID AMI corretto.

#### Policy del ruolo presunto con autorizzazioni insufficienti

Messaggio di errore: Automation Step Execution fails when it's launching the instance(s). Get Exception from RunInstances API of ec2 Service. Exception Message from RunInstances API: [You aren't authorized to perform this operation. Encoded authorization failure message: xxxxxxxx (Service: AmazonEC2; Status Code: 403; Error Code: UnauthorizedOperation; Request ID: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx)]. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.

Il ruolo presunto non dispone di autorizzazioni sufficienti per chiamare l'API `RunInstances` sulle istanze EC2. Per risolvere questo problema, allega una policy IAM al ruolo presunto con l'autorizzazione necessaria per chiamare l'API `RunInstances`. Per ulteriori informazioni, consulta [Crea ruoli di servizio per l'automazione tramite la console](#).

#### Stato imprevisto

Messaggio di errore: Step fails when it's verifying launched instance(s) are ready to be used. Instance i-xxxxxxx entered unexpected state: shutting-

down. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.

- Possibile causa 1: si è verificato un problema con l'istanza o il servizio Amazon EC2. Per risolvere questo problema, esegui l'accesso all'istanza o rivedi il log di sistema dell'istanza per individuare il motivo dell'arresto dell'istanza.
- Possibile causa 2: lo script di dati utente specificato per l'operazione `aws:runInstances` contiene un problema o la relativa sintassi è errata. Verifica la sintassi dello script di dati utente. Verifica anche che gli script di dati utente non arrestino l'istanza o non richi amino altri script che arrestano l'istanza.

### Action-Specific Riferimento sugli errori

Quando l'esecuzione di una fase ha esito negativo, il messaggio di errore potrebbe indicare il servizio chiamato quando si è verificato l'errore. La tabella seguente elenca i servizi richiamati da ciascuna operazione. La tabella fornisce anche i collegamenti alle informazioni su ciascun servizio.

| Azione                               | Servizi AWS richiamati o da questa azione | Ulteriori informazioni su questo servizio             | Risoluzione dei problemi                                          |
|--------------------------------------|-------------------------------------------|-------------------------------------------------------|-------------------------------------------------------------------|
| <code>aws:runInstances</code>        | Amazon EC2                                | <a href="#">Guida per l'utente di Amazon EC2</a>      | <a href="#">Risoluzione di problemi relativi alle istanze EC2</a> |
| <code>aws:changeInstanceState</code> | Amazon EC2                                | <a href="#">Guida per l'utente di Amazon EC2</a>      | <a href="#">Risoluzione di problemi relativi alle istanze EC2</a> |
| <code>aws:runCommand</code>          | Systems Manager                           | <a href="#">AWS Systems Manager Run Command</a>       | <a href="#">Risoluzione dei problemi di Systems Manager</a>       |
| <code>aws:createImage</code>         | Amazon EC2                                | <a href="#">Amazon Machine Images</a>                 |                                                                   |
| <code>aws:createStack</code>         | CloudFormation                            | <a href="#">AWS CloudFormation Guida per l'utente</a> | <a href="#">Risoluzione dei problemi CloudFormation</a>           |

| Azione                                | Servizi AWS richiamati da questa azione | Ulteriori informazioni su questo servizio             | Risoluzione dei problemi                                  |
|---------------------------------------|-----------------------------------------|-------------------------------------------------------|-----------------------------------------------------------|
| <code>aws:deleteStack</code>          | CloudFormation                          | <a href="#">AWS CloudFormation Guida per l'utente</a> | <a href="#">Risoluzione dei problemi CloudFormation</a>   |
| <code>aws:deleteImage</code>          | Amazon EC2                              | <a href="#">Amazon Machine Image</a>                  |                                                           |
| <code>aws:copyImage</code>            | Amazon EC2                              | <a href="#">Amazon Machine Images</a>                 |                                                           |
| <code>aws:createTag</code>            | Amazon EC2, Systems Manager             | <a href="#">Risorse e tag EC2</a>                     |                                                           |
| <code>aws:invokeLambdaFunction</code> | AWS Lambda                              | <a href="#">AWS Lambda Guida per gli sviluppatori</a> | <a href="#">Risoluzione di problemi relativi a Lambda</a> |

### Errore interno del servizio di automazione

Messaggio di errore: Internal Server Error. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.

Un problema con il servizio di automazione impedisce la corretta esecuzione del runbook specificato. Per risolvere il problema, contatta Supporto AWS. Devi fornire l'ID esecuzione e l'ID cliente, se disponibili.

### Esecuzione avviata, ma scaduta

Messaggio di errore: Step timed out while step is verifying launched instance(s) are ready to be used. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.

Si è verificato il timeout di una fase dell'operazione `aws:runInstances`. Questo errore si può verificare se l'esecuzione dell'operazione di una fase richiede un intervallo di tempo maggiore del valore specificato per `timeoutSeconds` nella fase. Per risolvere questo problema, specifica un

valore più alto per il parametro `timeoutSeconds` nell'operazione `aws:runInstances`. Se il problema persiste, individua il passaggio la cui esecuzione richiede più tempo del previsto

## AWS Systems Manager Modifica calendario

Con `Change Calendar`, è possibile impostare intervalli di data e ora in cui le azioni specificate (ad esempio, nei [runbook di Systems Manager Automation](#)) possono o non possono essere eseguite nel proprio Account AWS. In `Change Calendar`, questi intervalli sono chiamati eventi. Quando si crea una voce `Change Calendar`, si sta creando un [documento Systems Manager](#) del tipo `ChangeCalendar`. In `Change Calendar`, il documento memorizza i dati [iCalendar 2.0](#) in formato testo normale. Gli eventi aggiunti alla voce `Change Calendar` diventano parte del documento. Per iniziare a utilizzare `Change Calendar`, apri la [console di Systems Manager](#). Nel pannello di navigazione, scegli `Change Calendar`.

È possibile creare un calendario e i relativi eventi nella console di `Systems Manager`. È anche possibile importare un file `iCalendar` (.ics) esportato da un provider di calendari esterno supportato per aggiungere gli eventi al calendario. I provider supportati includono `Google Calendar`, `Microsoft Outlook` e `iCloud Calendar`.

Una voce `Change Calendar` può essere uno dei due tipi:

### **DEFAULT\_OPEN** o Apri per impostazione predefinita

Tutte le operazioni possono essere eseguite per impostazione predefinita, tranne durante gli eventi del calendario. Durante gli eventi, lo stato di un calendario `DEFAULT_OPEN` è `CLOSED` e l'esecuzione degli eventi è bloccata.

### **DEFAULT\_CLOSED** o Chiuso per impostazione predefinita

Tutte le operazioni sono bloccate per impostazione predefinita, tranne durante gli eventi del calendario. Durante gli eventi, lo stato di un calendario `DEFAULT_CLOSED` è `OPEN` e le operazioni possono essere eseguite.

Puoi scegliere di aggiungere automaticamente a un calendario tutti i flussi di lavoro di automazione pianificati, le finestre di manutenzione e le associazioni di `State Manager`. Puoi anche rimuovere uno di questi singoli tipi dalla visualizzazione del calendario.

## Chi dovrebbe usare Modifica calendario?

### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

- AWS clienti che eseguono i seguenti tipi di azioni:
  - Creazione o esecuzione dei runbook di Automazione.
  - Creazione di richieste di modifica in Change Manager.
  - Esecuzione di finestre di manutenzione.
  - Creazione di associazioni in State Manager.

Automazione Change Manager Maintenance Windows, e State Manager sono tutti strumenti AWS Systems Manager. Integrando queste funzionalità con Change Calendar, è possibile consentire o bloccare questi tre tipi di operazioni a seconda dello stato corrente del calendario delle modifiche associato a ciascuno di essi.

- Amministratori responsabili di mantenere coerenti, stabili e funzionali le configurazioni dei nodi gestiti di Systems Manager.

## Vantaggi di Modifica calendario

Di seguito sono riportati alcuni vantaggi di Change Calendar.

- Esaminare le modifiche prima che vengano applicate

Una Change Calendar voce può aiutare a garantire che le modifiche potenzialmente distruttive all'ambiente vengano esaminate prima di essere applicate.

- Applicare le modifiche solo nei tempi appropriati

Con le voci di Change Calendar è possibile mantenere stabile l'ambiente durante gli eventi. Ad esempio, è possibile creare una voce Change Calendar per bloccare le modifiche quando si prevede una richiesta elevata delle risorse, ad esempio durante una conferenza o una promozione di marketing pubblico. Una voce del calendario può anche bloccare le modifiche quando ci si



aspetta un supporto amministrativo limitato, ad esempio durante le vacanze o le festività. È possibile utilizzare una voce del calendario per consentire le modifiche, ad eccezione di determinati periodi del giorno o della settimana in cui è disponibile un supporto amministrativo limitato per risolvere i problemi relativi a operazioni o distribuzioni non riuscite.

- Ottenere lo stato attuale o imminente del calendario

In Systems Manager è possibile eseguire l'operazione API `GetCalendarState` per visualizzare lo stato corrente del calendario, lo stato in un momento specificato o la prossima volta che lo stato del calendario è pianificato per la modifica.

#### Note

L'`GetCalendarStateAPI` ha una quota di 10 richieste al secondo. Per informazioni sulle quote del documento SSM, consulta [Systems Manager Service Quotas](#) nella Riferimenti generali di Amazon Web Services.

- EventBridge supporto

Questo strumento Systems Manager è supportato come tipo di evento nelle EventBridge regole di Amazon. Per informazioni, consulta [Monitoraggio degli eventi di Systems Manager con Amazon EventBridge](#) e [Riferimento: modelli e tipi di EventBridge eventi Amazon per Systems Manager](#).

## Argomenti

- [Configurazione Modifica calendario](#)
- [Utilizzo di Change Calendar](#)
- [Aggiungendo Modifica calendario dipendenze dai runbook di Automation](#)
- [Risoluzione dei problemi Modifica calendario](#)

## Configurazione Modifica calendario

Completare quanto segue prima di utilizzare Change Calendar.

Installazione degli strumenti a riga di comando più recenti

Installare gli ultimi strumenti a riga di comando per ottenere informazioni sui calendari.

| Requisito                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AWS CLI                      | <p>(Facoltativo) Per utilizzare AWS Command Line Interface (AWS CLI) per ottenere informazioni sullo stato dei calendari, installa la versione più recente di AWS CLI sul tuo computer locale.</p> <p>Per ulteriori informazioni su come installare e o aggiornare CLI, consulta <a href="#">Installazione, aggiornamento e disinstallazione di AWS CLI</a> nella Guida per l'utente di AWS Command Line Interface .</p>        |
| AWS Strumenti per PowerShell | <p>(Facoltativo) Per utilizzare gli Strumenti per PowerShell ottenere informazioni sullo stato dei calendari, installa la versione più recente di Tools for PowerShell sul tuo computer locale.</p> <p>Per ulteriori informazioni su come installare o aggiornare gli Strumenti per PowerShell, vedere <a href="#">Installazione di AWS Strumenti per PowerShell</a> nella Guida per l'AWS Strumenti per PowerShell utente.</p> |

## Impostazione delle autorizzazioni

Se al tuo utente, gruppo o ruolo sono assegnate le autorizzazioni di amministratore, allora hai accesso completo a Change Calendar. Se non disponi delle autorizzazioni di amministratore, un amministratore dovrà concederti l'autorizzazione assegnando la policy gestita di AmazonSSMFullAccess o assegnando una policy che conceda le autorizzazioni necessarie all'utente, al gruppo o al ruolo.

Le seguenti autorizzazioni sono richieste per l'uso con Change Calendar.

## Voci di Change Calendar

Per creare, aggiornare o eliminare una voce di Change Calendar, incluse l'aggiunta e la rimozione di eventi dalla voce, una policy collegata all'utente, al gruppo o al ruolo deve consentire le seguenti operazioni:

- `ssm:CreateDocument`
- `ssm>DeleteDocument`
- `ssm:DescribeDocument`
- `ssm:DescribeDocumentPermission`
- `ssm:GetCalendar`
- `ssm:ListDocuments`
- `ssm:ModifyDocumentPermission`
- `ssm:PutCalendar`
- `ssm:UpdateDocument`
- `ssm:UpdateDocumentDefaultVersion`

## Stato del calendario

Per ottenere informazioni sullo stato corrente o imminente del calendario, una policy collegata all'utente, al gruppo o al ruolo deve consentire la seguente operazione:

- `ssm:GetCalendarState`

## Eventi operativi

Per visualizzare gli eventi operativi, come le finestre di manutenzione, le associazioni e le automazioni pianificate, la policy associata all'utente, al gruppo o al ruolo deve consentire le seguenti operazioni:

- `ssm:DescribeMaintenanceWindows`
- `ssm:DescribeMaintenanceWindowExecution`
- `ssm:DescribeAutomationExecutions`
- `ssm:ListAssociations`

 Note

Le voci del Change Calendar di proprietà di (ovvero create da) account diversi dal tuo sono in sola lettura, anche se condivise con il tuo account. Le finestre di manutenzione, le associazioni State Manager e le automazioni non sono condivise.

## Utilizzo di Change Calendar

È possibile utilizzare la AWS Systems Manager console per aggiungere, gestire o eliminare voci inChange Calendar, uno strumento in AWS Systems Manager. È inoltre possibile importare eventi da provider di calendari di terze parti supportate importando un file iCalendar (.ics) esportato dal calendario di origine. Inoltre, puoi utilizzare l'operazione GetCalendarState API o il comando `get-calendar-state` AWS Command Line Interface (AWS CLI) per ottenere informazioni sullo stato di Change Calendar in un momento specifico.

### Argomenti

- [Creazione di un calendario delle modifiche](#)
- [Creazione e gestione di eventi in Change Calendar](#)
- [Importazione e gestione di eventi da calendari di terze parti](#)
- [Aggiornamento di un calendario delle modifiche](#)
- [Condivisione di un calendario delle modifiche](#)
- [Eliminazione di un calendario delle modifiche](#)
- [Recupero dello stato di un calendario delle modifiche](#)

### Creazione di un calendario delle modifiche

Quando si crea una voce inChange Calendar, si crea un documento Systems Manager (documento SSM) che utilizza il `text` formato.

Per creare un calendario delle modifiche

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Change Calendar.
3. Seleziona Crea calendario.

oppure

Se la home page di Change Calendar si apre per prima, scegli Crea calendario delle modifiche.

4. Nella pagina Crea calendario in Dettagli del calendario, immetti un nome per la voce del calendario. I nomi delle voci del calendario possono contenere lettere, numeri, punti, trattini e caratteri di sottolineatura. Il nome dovrebbe essere sufficientemente specifico da identificare a colpo d'occhio lo scopo della voce del calendario. Un esempio è **support-off-hours**. Non è possibile aggiornare questo nome dopo aver creato la voce del calendario.
5. (Facoltativo) In Descrizione, immetti una descrizione per la voce del calendario.
6. (Facoltativo) Nella finestra Importa calendario, scegli Scegli file per selezionare un file iCalendar (.ics) esportato da un provider di calendari di terze parti. L'importazione del file aggiungerà i suoi eventi al calendario.

I provider supportati includono Google Calendar, Microsoft Outlook e iCloud Calendar.

Per ulteriori informazioni, consulta [Importazione di eventi da provider di calendario esterni](#).

7. In Tipo di calendario, scegli una delle seguenti opzioni:
  - Aperto per impostazione predefinita: il calendario è aperto (le operazioni di Automazione sono eseguibili fino all'avvio di un evento), quindi è chiuso per la durata di un evento associato.
  - Chiuso per impostazione predefinita: il calendario è chiuso (le operazioni di Automazione non sono eseguibili fino all'avvio di un evento), ma è aperto per la durata di un evento associato.
8. (Facoltativo) In Eventi di gestione delle modifiche, seleziona Aggiungi eventi di gestione delle modifiche al calendario. Questa selezione mostra tutte le finestre di manutenzione programmata, le associazioni di State Manager, i flussi di lavoro di automazione e le richieste di modifica di Change Manager nella visualizzazione del calendario mensile.

 Tip

Se in seguito desideri rimuovere definitivamente questi tipi di eventi dalla visualizzazione del calendario, modifica il calendario, deseleziona questa casella di controllo e scegli Salva.

9. Seleziona Crea calendario.

Dopo aver creato la voce del calendario, Systems Manager visualizza la voce del calendario nell'elenco Change Calendar. Le colonne mostrano la versione del calendario e il Account AWS

numero del proprietario del calendario. La voce del calendario non può impedire o consentire alcuna operazione finché non si aggiunge almeno un evento. Per ulteriori informazioni sulla creazione di un evento consulta [Creare un Modifica calendario evento](#). Per informazioni sull'importazione di eventi live, consulta [Importazione di eventi da provider di calendario esterni](#).

## Creazione e gestione di eventi in Change Calendar

Dopo aver creato un calendario in AWS Systems Manager Change Calendar, puoi creare, aggiornare ed eliminare gli eventi inclusi nel calendario aperto o chiuso. Change Calendar è uno strumento in AWS Systems Manager.

### Tip

In alternativa alla creazione di eventi direttamente nella console di Systems Manager, è possibile importare un file iCalendar (.ics) da un'applicazione di calendario di un provider esterno supportata. Per informazioni, consulta [Importazione e gestione di eventi da calendari di terze parti](#).

## Argomenti

- [Creare un Modifica calendario evento](#)
- [Aggiornamento di un evento Change Calendar](#)
- [Eliminazione di un Modifica calendario evento](#)

## Creare un Modifica calendario evento

Quando si aggiunge un evento a una voce in Change Calendar, si specifica un periodo di tempo in cui l'azione predefinita della voce del calendario viene sospesa. Ad esempio, se il tipo di voce del calendario è chiuso per impostazione predefinita, il calendario è aperto alle modifiche durante gli eventi. È inoltre possibile creare un evento consultivo, che ha solo un ruolo informativo nel calendario.

Attualmente, è possibile creare un evento Change Calendar solo utilizzando la console. Gli eventi vengono aggiunti al documento Change Calendar creato quando si crea una voce in Change Calendar.

## Per creare un Modifica calendario evento

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Change Calendar.
3. Nell'elenco di calendari, scegli il nome della voce del calendario a cui si desidera aggiungere un evento.
4. Nella pagina dei dettagli della voce del calendario, scegli Crea evento.
5. Nella pagina Crea evento pianificato in Dettagli evento, immetti un nome visualizzato per l'evento. I nomi dell'evento possono contenere lettere, numeri, punti, trattini e caratteri di sottolineatura. Il nome dovrebbe essere sufficientemente specifico da identificare lo scopo dell'evento. Un esempio è **nighttime-hours**.
6. In Descrizione, immetti una descrizione per l'evento. Ad esempio, **The support team isn't available during these hours**.
7. (Facoltativo) Se si desidera che questo evento funzioni solo come notifica visiva o promemoria, selezionare la casella di controllo Consulenza. Gli eventi di consulenza non svolgono alcun ruolo funzionale nel calendario. Servono solo a scopo informativo per coloro che visualizzano il calendario.
8. Per Data di inizio evento, immetti o scegli un giorno nel formato MM/DD/YYYY per avviare l'evento e immettere un'ora nel giorno specificato nel formato hh:mm:ss (ore, minuti e secondi) per avviare l'evento.
9. Per Data di fine evento, immetti o scegli un giorno nel formato MM/DD/YYYY per terminare l'evento e immettere un'ora nel giorno specificato nel formato hh:mm:ss (ore, minuti e secondi) per terminare l'evento.
10. Per Pianifica fuso orario, scegli un fuso orario che si applica agli orari di inizio e fine dell'evento. È possibile immettere parte del nome di una città o la differenza di fuso orario da Greenwich Mean Time (GMT) per trovare un fuso orario più velocemente. L'impostazione predefinita attuale è Universal Coordinated Time (UTC).
11. (Facoltativo) Per creare un evento che ricorra quotidianamente, settimanalmente o mensilmente, attivare Ricorrenza e quindi specificare la frequenza e la data di fine facoltativa per la ricorrenza.
12. Scegli Crea evento pianificato. Il nuovo evento viene aggiunto alla voce del calendario e viene visualizzato nella scheda Eventi della pagina dei dettagli della voce del calendario.

## Aggiornamento di un evento Change Calendar

Utilizza la procedura seguente per aggiornare un evento Change Calendar nella console AWS Systems Manager . Change Calendar è uno strumento di AWS Systems Manager.

### Aggiornamento di un evento Change Calendar

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Change Calendar.
3. Nell'elenco di calendari, scegliere il nome della voce del calendario per la quale si desidera modificare un evento.
4. Nella pagina dei dettagli della voce del calendario scegli Eventi.
5. Nella pagina del calendario, scegliere l'evento che si desidera modificare.

#### Tip

Utilizzare i pulsanti in alto a sinistra per spostarsi indietro o avanti di un anno o indietro o avanti di un mese. Modificare il fuso orario, se necessario, scegliendo il fuso orario corretto dall'elenco in alto a destra.

6. In Event details (Dettagli evento), scegliere Edit (Modifica).

Per modificare il nome e la descrizione dell'evento, aggiungere o sostituire i valori di testo correnti.

7. Per modificare il valore Event start date (Data di inizio evento), scegliere la data di inizio corrente e quindi scegliere una nuova data dal calendario. Per modificare l'ora di inizio, scegliere l'ora di inizio corrente e quindi scegliere una nuova ora dall'elenco.
8. Per modificare il valore Event end date (Data di fine evento), scegliere la data corrente e quindi scegliere una nuova data di fine dal calendario. Per modificare l'ora di fine, scegliere l'ora di fine corrente e quindi scegliere una nuova ora dall'elenco.
9. Per modificare il valore Schedule time zone (Pianifica fuso orario), scegliere un fuso orario da applicare agli orari di inizio e fine dell'evento. È possibile immettere parte del nome di una città o la differenza di fuso orario da Greenwich Mean Time (GMT) per trovare un fuso orario più velocemente. L'impostazione predefinita attuale è Universal Coordinated Time (UTC).
10. (Facoltativo) Se si desidera che questo evento funzioni solo come notifica visiva o promemoria, selezionare la casella di controllo Advisory (Consulenza). Gli eventi di consulenza non svolgono



alcun ruolo funzionale nel calendario. Servono solo a scopo informativo per coloro che visualizzano il calendario.

11. Scegli Save (Salva). Le modifiche vengono visualizzate nella scheda Events (Eventi) della pagina dei dettagli della voce del calendario. Scegliere l'evento aggiornato per visualizzare le modifiche.

## Eliminazione di un Modifica calendario evento

È possibile eliminare un evento alla volta Change Calendar utilizzando il Console di gestione AWS.

### Tip

Se hai selezionato Aggiungi eventi di gestione delle modifiche al calendario quando hai creato il calendario, puoi fare quanto segue:

- Per nascondere temporaneamente un tipo di evento di gestione delle modifiche dalla visualizzazione del calendario, scegli la X per il tipo nella parte superiore dell'anteprima mensile.
- Per rimuovere definitivamente questi tipi dalla visualizzazione del calendario, modifica il calendario, deseleziona la casella di controllo Aggiungi eventi di gestione delle modifiche al calendario e quindi scegli Salva. La rimozione dei tipi dalla visualizzazione del calendario non ne comporta l'eliminazione dal tuo account.

## Per eliminare un Modifica calendario evento

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Change Calendar.
3. Nell'elenco di calendari, scegliere il nome della voce del calendario da cui si desidera eliminare un evento.
4. Nella pagina dei dettagli della voce del calendario scegli Eventi.
5. Nella pagina del calendario, scegli l'evento che si desidera eliminare.

 Tip

Utilizza i pulsanti in alto a sinistra per spostare il calendario indietro o avanti di un anno o indietro o avanti di un mese. Modificare il fuso orario, se necessario, scegliendo il fuso orario corretto dall'elenco in alto a destra.

6. Nella pagina Dettagli dell'evento, scegli Elimina. Quando viene richiesto di confermare che si desidera eliminare l'evento, scegli Conferma.

## Importazione e gestione di eventi da calendari di terze parti

In alternativa alla creazione di eventi direttamente nella AWS Systems Manager console, puoi importare un file iCalendar (.ics) da un'applicazione di calendario di terze parti supportata. Il calendario può includere sia eventi importati che eventi creati in Change Calendar. È uno strumento di AWS Systems Manager.

### Prima di iniziare

Prima di provare a importare un file di calendario, esaminare i seguenti requisiti e vincoli:

#### Formato del file del calendario

Sono supportati solo i file iCalendar validi (.ics).

#### Provider di calendari supportati

Sono supportati solo i file .ics esportati dai provider esterni di calendari indicati di seguito:

- Google Calendari ([Istruzioni per l'esportazione](#))
- Microsoft Outlook ([Istruzioni per l'esportazione](#))
- Calendario iCloud ([Istruzioni per l'esportazione](#))

#### Dimensioni file

È possibile importare qualsiasi numero di file .ics. Tuttavia, la dimensione totale di tutti i file importati per ogni calendario non può superare i 64 KB.

 Tip

Per ridurre al minimo le dimensioni del `.ics`, assicurarsi di esportare solo i dettagli di base relativi alle voci del calendario. Se necessario, ridurre la durata del periodo di tempo che si desidera esportare.

## Time zone (Fuso orario)

Oltre al nome del calendario, a un provider del calendario e ad almeno un evento, il `.ics` dovrebbe indicare anche il fuso orario per il calendario. In caso contrario, o se si verifica un problema nell'identificazione del fuso orario, viene richiesto di specificarne uno dopo aver importato il file.

## Limitazione di eventi ricorrenti

Il file `.ics` esportato può includere eventi ricorrenti. Tuttavia, se una o più occorrenze di un evento ricorrente sono state eliminate nel calendario di origine, l'importazione ha esito negativo.

## Argomenti

- [Importazione di eventi da provider di calendario esterni](#)
- [Aggiornamento di tutti gli eventi da un provider esterno di calendario](#)
- [Eliminazione di tutti gli eventi importati da un calendario di terze parti](#)

## Importazione di eventi da provider di calendario esterni

Utilizza la procedura seguente per importare un file iCalendar (`.ics`) da un'applicazione di calendario di un provider esterno supportata. Gli eventi contenuti nel file vengono incorporati nelle regole per il calendario aperto o chiuso. Puoi importare il file in un nuovo calendario o in un calendario esistente.

Dopo aver importato il file `.ics`, è possibile rimuovere singoli eventi da esso utilizzando l'interfaccia Change Calendar. Per informazioni, consulta [Eliminazione di un Modifica calendario evento](#). È inoltre possibile eliminare tutti gli eventi dal calendario di origine eliminando il file `.ics`. Per informazioni, consulta [Eliminazione di tutti gli eventi importati da un calendario di terze parti](#).

## Per importare eventi da provider esterni di calendari

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.

2. Nel pannello di navigazione, scegli Change Calendar.
3. Per iniziare con un nuovo calendario, scegliere Crea calendario. In Importa calendario, scegli Scegli file. Per informazioni su altri passaggi per creare un nuovo calendario, consulta [Creazione di un calendario delle modifiche](#).

oppure

Per importare eventi di terze parti in un calendario esistente, scegliere il nome di un calendario esistente per aprirlo.

4. Scegli Operazioni, Modifica e quindi nell'area Importa calendario, scegli Scegli file.
5. Individua e seleziona il file `.ics` esportato sul computer locale.
6. Se richiesto, per Selezionare un fuso orario, seleziona il fuso orario da applicare al calendario.
7. Scegli Salva.

#### Aggiornamento di tutti gli eventi da un provider esterno di calendario

Se diversi eventi vengono aggiunti o rimossi dal calendario sorgente dopo aver importato il file iCalendar `.ics`, è possibile riflettere tali modifiche in Change Calendar. Innanzitutto, riesportare il calendario di origine e quindi importare il nuovo file in Change Calendar, che è uno strumento di AWS Systems Manager. Gli eventi nel calendario delle modifiche verranno aggiornati in modo da riflettere il contenuto del file più recente.

Per aggiornare tutti gli eventi da un provider esterno di calendari

1. Nel calendario del provider esterno, aggiungi o rimuovi gli eventi in base a come vuoi che vengano riflessi in Change Calendar e quindi riesporta il calendario in un nuovo file `.ics`.
2. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
3. Nel pannello di navigazione, scegli Change Calendar.
4. Dall'elenco dei calendari, scegliere il nome del calendario dall'elenco.
5. Nel menu Operazioni, scegliere Modifica.
6. Nella sezione Importa calendario, scegli Scegli file.
7. Vai al `.ics` file sostitutivo e selezionalo.
8. Scegli Save (Salva).

## Eliminazione di tutti gli eventi importati da un calendario di terze parti

Se non desideri più eventi importati da un provider di terze parti, puoi eliminare il file iCalendar .ics importato.

Per eliminare tutti gli eventi importati da un calendario di provider esterni

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Change Calendar.
3. Dall'elenco dei calendari, scegliere il nome del calendario dall'elenco.
4. Nel menu Operazioni, scegliere Modifica.
5. Nella sezione Importa calendario, in I miei calendari importati, scegli la X accanto al nome del calendario.
6. Scegli Save (Salva).

## Aggiornamento di un calendario delle modifiche

È possibile aggiornare la descrizione di un calendario delle modifiche, ma non il suo nome. Sebbene sia possibile modificare lo stato predefinito di una voce di calendario, tenere presente che questo inverte il comportamento delle operazioni di modifica durante gli eventi associati alla voce del calendario. Ad esempio, se si modifica lo stato di un calendario da Open by default (Aperto per impostazione predefinita) a Closed by default (Chiuso per impostazione predefinita), potrebbero essere apportate modifiche indesiderate durante i periodi di eventi quando gli utenti che hanno creato gli eventi associati non sono in attesa di modifiche.

Quando si aggiorna un calendario delle modifiche, si modifica il documento Change Calendar creato al momento della creazione della voce. Change Calendar è uno strumento di AWS Systems Manager.

Per aggiornare un calendario delle modifiche

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Change Calendar.
3. Nell'elenco di calendari, scegliere il nome del calendario che si desidera aggiornare.
4. Nella pagina dei dettagli del calendario, scegliere Actions, Edit (Operazioni, Modifica).

5. In Description (Descrizione), è possibile modificare il testo della descrizione. Non puoi modificare il nome di un calendario delle modifiche.
6. Per modificare lo stato del calendario, in Calendar type (Tipo di calendario), scegliere un valore diverso. Tenere presente che questo inverte il comportamento delle operazioni di modifica durante gli eventi associati alla voce del calendario. Prima di modificare il tipo di calendario, è necessario verificare con altri utenti Change Calendar che la modifica del tipo di calendario non consenta modifiche indesiderate durante gli eventi creati.
  - Open by default (Aperto per impostazione predefinita) – il calendario è aperto (le operazioni di automazione possono essere eseguite fino all'avvio di un evento), quindi chiuso per la durata di un evento associato.
  - Closed by default (Chiuso per impostazione predefinita) – il calendario è chiuso (le operazioni di automazione non possono essere eseguite fino all'avvio di un evento) ma aperto per la durata di un evento associato.
7. Scegli Save (Salva).

La voce del calendario non può impedire o consentire alcuna operazione finché non si aggiunge almeno un evento. Per informazioni su come aggiungere un evento, consulta [Creare un Modifica calendario evento](#).

## Condivisione di un calendario delle modifiche

È possibile condividere un calendario Change Calendar con altri Account AWS utilizzando la AWS Systems Manager console. Quando si condivide un calendario, il calendario è in sola lettura per gli utenti dell'account condiviso. Le finestre di manutenzione, le associazioni State Manager e le automazioni non sono condivise.

### Per condividere un calendario delle modifiche

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Change Calendar.
3. Nell'elenco di calendari, scegli il nome del calendario che si desidera condividere.
4. Nella pagina dei dettagli del calendario, scegli la scheda Condivisione.
5. Seleziona Operazioni, Condividi.

6. Nel calendario Condividi, per ID account, inserisci il numero ID di un numero valido Account AWS, quindi scegli Condividi.

Gli utenti dell'account condiviso possono leggere il calendario delle modifiche, ma non possono apportare modifiche.

### Eliminazione di un calendario delle modifiche

È possibile eliminare un calendario Change Calendar utilizzando la console Systems Manager o AWS Command Line Interface (AWS CLI). L'eliminazione di un calendario delle modifiche elimina tutti gli eventi associati.

Per eliminare un calendario delle modifiche

1. Aprire la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Change Calendar.
3. Nell'elenco di calendari, scegli il nome del calendario che si desidera eliminare.
4. Nella pagina dei dettagli del calendario scegli Operazioni, Elimina. Quando viene richiesto di confermare che si desidera eliminare il calendario, scegli Elimina.

### Recupero dello stato di un calendario delle modifiche

È possibile ottenere lo stato generale di un calendario o lo stato di un calendario in un momento specifico inChange Calendar. È inoltre possibile visualizzare la prossima volta in cui lo stato del calendario passerà da OPEN a CLOSED o viceversa.

#### Note

Per informazioni sull'integrazione Change Calendar con Amazon EventBridge per il monitoraggio automatico delle modifiche allo stato del calendario, consulta [the section called “Modifica calendario integrazione con Amazon EventBridge”](#). EventBridge l'integrazione fornisce notifiche basate sugli eventi durante la transizione degli stati del calendario, integrando l'approccio basato sul polling dell'azione API. GetCalendarState

È possibile eseguire questo processo solo utilizzando l'operazione API GetCalendarState. La procedura in questa sezione utilizza (). AWS Command Line Interface AWS CLI

Per ottenere lo stato di un calendario delle modifiche

- Eseguire il comando seguente per visualizzare lo stato di una o più voci di calendario in un momento specifico. Il parametro `--calendar-names` è obbligatorio, ma `--at-time` è facoltativo. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux & macOS

```
aws ssm get-calendar-state \
 --calendar-names "Calendar_name_or_document_ARN_1"
 "Calendar_name_or_document_ARN_2" \
 --at-time "ISO_8601_time_format"
```

Di seguito è riportato un esempio di :

```
aws ssm get-calendar-state \
 --calendar-names "arn:aws:ssm:us-east-2:123456789012:document/
MyChangeCalendarDocument" "arn:aws:ssm:us-east-2:123456789012:document/
SupportOffHours" \
 --at-time "2020-07-30T11:05:14-0700"
```

Windows

```
aws ssm get-calendar-state ^
 --calendar-names "Calendar_name_or_document_ARN_1"
 "Calendar_name_or_document_ARN_2" ^
 --at-time "ISO_8601_time_format"
```

Di seguito è riportato un esempio di :

```
aws ssm get-calendar-state ^
 --calendar-names "arn:aws:ssm:us-east-2:123456789012:document/
MyChangeCalendarDocument" "arn:aws:ssm:us-east-2:123456789012:document/
SupportOffHours" ^
 --at-time "2020-07-30T11:05:14-0700"
```

Il comando restituisce informazioni simili alle seguenti.

```
{
```



```
"State": "OPEN",
"AtTime": "2020-07-30T16:18:18Z",
"NextTransitionTime": "2020-07-31T00:00:00Z"
}
```

I risultati mostrano lo stato del calendario (se il calendario è di tipo DEFAULT\_OPEN o DEFAULT\_CLOSED) per le voci di calendario specificate che sono di proprietà o condivise con l'account --at-time, al momento specificato come valore e ora della transizione successiva. Se non si aggiunge il parametro --at-time, viene utilizzata l'ora corrente.

#### Note

Se si specifica più di un calendario in una richiesta, il comando restituisce lo stato di OPEN solo se tutti i calendari nella richiesta sono aperti. Se uno o più calendari nella richiesta sono chiusi, lo stato restituito è CLOSED.

## Aggiungendo Modifica calendario dipendenze dai runbook di Automation

Per far sì che le azioni di automazione rispettino Change Calendar, aggiungi un passaggio in un runbook di automazione che utilizzi l'azione. [aws:assertAwsResourceProperty](#) Configurare l'operazione per eseguire GetCalendarState per verificare che una voce di calendario specificata si trovi nello stato desiderato (OPEN o CLOSED). Il runbook di Automazione può solo proseguire al passaggio successivo, se lo stato del calendario è OPEN. Di seguito è riportato un estratto di YAML-based esempio di un runbook di Automation che non può passare alla fase successiva LaunchInstance, a meno che lo stato del calendario non OPEN corrisponda a quello specificato in DesiredValues

Di seguito è riportato un esempio di :

```
mainSteps:
 - name: MyCheckCalendarStateStep
 action: 'aws:assertAwsResourceProperty'
 inputs:
 Service: ssm
 Api: GetCalendarState
 CalendarNames: ["arn:aws:ssm:us-east-2:123456789012:document/SaleDays"]
 PropertySelector: '$.State'
 DesiredValues:
```

```
- OPEN
 description: "Use GetCalendarState to determine whether a calendar is open or
closed."
 nextStep: LaunchInstance
- name: LaunchInstance
 action: 'aws:executeScript'
 inputs:
 Runtime: python3.11
...
```

## Risoluzione dei problemi Modifica calendario

Utilizza le informazioni seguenti per risolvere i problemi relativi a Change Calendar, uno strumento di AWS Systems Manager.

### Argomenti

- [Errore “Importazione calendario non riuscita”](#)

### Errore “Importazione calendario non riuscita”

Problema: durante l'importazione di un file iCalendar (.ics), il sistema segnala che l'importazione del calendario non è riuscita.

- Soluzione 1: assicurati di importare un file esportato da un fornitore di calendari di terze parti supportato, che include quanto segue:
  - Google Calendar([Istruzioni per l'esportazione](#))
  - Microsoft Outlook ([Istruzioni per l'esportazione](#))
  - Calendario iCloud ([Istruzioni per l'esportazione](#))
- Soluzione 2: se il calendario di origine contiene eventi ricorrenti, assicurati che nessuna singola ricorrenza dell'evento sia stata annullata o eliminata. Attualmente, Change Calendar non supporta l'importazione di eventi ricorrenti con singoli annullamenti. Per risolvere il problema, rimuovere l'evento ricorrente dal calendario di origine, riesportare il calendario e reimportarlo in Change Calendar, quindi aggiungere l'evento ricorrente utilizzando l'interfaccia Change Calendar. Per informazioni, consulta [Creare un Modifica calendario evento](#).
- Soluzione 3: assicurati che il calendario di origine contenga almeno un evento. Caricamenti di file .ics che non contengono eventi non hanno esito positivo.

- Soluzione 4: se il sistema segnala che l'importazione non .ics è riuscita perché è troppo grande, assicurati di esportare solo i dettagli di base sulle voci del calendario. Se necessario, ridurre la durata del periodo di tempo esportato.
- Soluzione 5: Se Change Calendar non è in grado di determinare il fuso orario del calendario esportato quando si tenta di importarlo dalla scheda Eventi, è possibile che venga visualizzato il messaggio "Importazione calendario non riuscita. Change Calendar non è stato in grado di individuare un fuso orario valido". È possibile importare il calendario dal menu Modifica." In questo caso, scegliere Operazioni, Modifica, quindi provare a importare il file dalla pagina Modifica calendario.
- Soluzione 6: non modificare il file .ics prima dell'importazione. Il tentativo di modificare il contenuto del file può danneggiare i dati del calendario. Se il file è stato modificato prima di tentare l'importazione, esportare di nuovo il calendario dal calendario di origine e quindi riprovare il caricamento.

## AWS Systems Manager Change Manager

### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

Change Manager è un framework di gestione delle modifiche enterprise per la richiesta, l'approvazione, l'implementazione e la creazione di report sulle modifiche operative alla configurazione e all'infrastruttura delle applicazioni. Da un singolo account amministratore delegato, se lo utilizzi AWS Organizations, puoi gestire le modifiche su più Account AWS e più account. Regioni AWS In alternativa, utilizzando un account locale, è possibile gestire le modifiche di un singolo Account AWS. Change Manager Utilizzalo per gestire le modifiche alle AWS risorse e alle risorse locali. Per cominciare a utilizzare Change Manager, apri la [console di Systems Manager](#). Nel pannello di navigazione, scegli Change Manager.

Con Change Manager, è possibile utilizzare modelli di modifica pre-approvati al fine di automatizzare i processi di modifica delle risorse ed evitare risultati involontari quando si apportano modifiche operative. Ogni modello di modifica specifica quanto segue:

- Uno o più runbook di Automazione tra cui un utente può scegliere durante la creazione di una richiesta di modifica. Le modifiche apportate alle risorse vengono definite nei runbook di Automazione. È possibile includere runbook personalizzati o [Runbook gestiti da AWS](#) nei modelli di modifica creati. Quando un utente crea una richiesta di modifica, può scegliere quale dei runbook disponibili includere nella richiesta. Inoltre, è possibile creare modelli di modifica che consentono all'utente che effettua la richiesta di specificare qualsiasi runbook nella richiesta di modifica.
- Gli utenti dell'account che devono esaminare le richieste di modifica effettuate utilizzando tale modello di modifica.
- L'argomento Amazon Simple Notification Service (Amazon SNS) utilizzato per notificare agli approvatori assegnati che una richiesta di modifica è pronta per la revisione.
- L' CloudWatch allarme Amazon utilizzato per monitorare il flusso di lavoro del runbook.
- L'argomento Amazon SNS utilizzato per inviare notifiche sulle modifiche di stato per le richieste di modifica create utilizzando il modello di modifica.
- I tag da applicare al modello di modifica da utilizzare per categorizzare e filtrare i modelli di modifica.
- Se le richieste di modifica create dal modello di modifica possono essere eseguite senza una fase di approvazione (richieste approvate automaticamente).

Grazie alla sua integrazione con Change Calendar, che è un altro strumento di Systems Manager, consente Change Manager inoltre di implementare le modifiche in modo sicuro evitando conflitti di pianificazione con importanti eventi aziendali. Change Manager integra AWS Organizations e gestione Centro identità AWS IAM delle modifiche all'interno dell'organizzazione da un unico account utilizzando il sistema di gestione delle identità esistente. È possibile monitorare l'avanzamento delle modifiche da Change Manager e verifica le modifiche operative all'interno dell'organizzazione, fornendo maggiore visibilità e responsabilità.

Change Manager integra i controlli di sicurezza delle pratiche di integrazione [continua](#) (CI) e della metodologia di distribuzione [continua](#) (CD). Change Manager non è destinato alle modifiche apportate nell'ambito di un processo di rilascio automatico, come una CI/CD pipeline, a meno che non sia richiesta un'eccezione o un'approvazione.

## In che modo Change Manager funziona

Quando viene identificata la necessità di una modifica operativa standard o di emergenza, un utente dell'organizzazione crea una richiesta di modifica basata su uno dei modelli di modifica creati per l'utilizzo nell'organizzazione o nell'account.

Se la modifica richiesta richiede l'approvazione manuale, Change Manager notifica agli approvatori designati tramite una notifica Amazon SNS che una richiesta di modifica è pronta per la loro revisione. È possibile designare approvatori per le richieste di modifica nel modello di modifica oppure consentire agli utenti di designare gli approvatori nella richiesta di modifica stessa. È possibile assegnare revisori diversi a modelli diversi. Ad esempio, assegnare un utente, un gruppo di utenti o ruolo AWS Identity and Access Management (IAM) che deve approvare le richieste di modifica ai nodi gestiti e un altro utente, gruppo o ruolo IAM per le modifiche al database. Se il modello di modifica consente l'approvazione automatica e la policy utente del richiedente non lo proibisce, l'utente può anche scegliere di eseguire il runbook di Automazione per la propria richiesta senza un passaggio di revisione (ad eccezione degli eventi di blocco delle modifiche).

Per ogni modello di modifica, è possibile aggiungere fino a cinque livelli di approvatori. Ad esempio, è possibile richiedere ai revisori tecnici di approvare prima una richiesta di modifica creata da un modello di modifica e quindi richiedere un secondo livello di approvazione da parte di uno o più manager.

Change Manager è integrato con [AWS Systems Manager Modifica calendario](#). Quando viene approvata una modifica richiesta, il sistema determina innanzitutto se la richiesta è in conflitto con altre attività aziendali pianificate. Se viene rilevato un conflitto, Change Manager può bloccare la modifica o richiedere ulteriori approvazioni prima di avviare il flusso di lavoro del runbook. Ad esempio, potresti consentire le modifiche solo durante l'orario lavorativo per assicurarti che i team siano disponibili a gestire eventuali problemi imprevisti. Per eventuali modifiche eseguite al di fuori di tali orari, è possibile richiedere l'approvazione del management di livello superiore ovvero al Change Manager. Per le modifiche di emergenza, il Change Manager, dopo l'approvazione della richiesta di modifica, può omettere la fase di controllo del Change Calendar al fine di individuare conflitti o eventi che determinano un blocco.

Quando è il momento di implementare una modifica approvata, Change Manager esegue il runbook Automation specificato nella richiesta di modifica associata. Solo le operazioni definite nelle richieste di modifica approvate sono consentite durante l'esecuzione dei flussi di lavoro del runbook. Questo approccio aiuta ad evitare risultati involontari mentre le modifiche vengono implementate.

Oltre a limitare le modifiche che possono essere apportate durante l'esecuzione di un flusso di lavoro in runbook, Change Manager consente di controllare la concorrenza e le soglie di errore. Puoi scegliere su quante risorse può essere eseguito un flusso di lavoro runbook contemporaneamente e su quanti account può essere eseguito contemporaneamente. Puoi anche impostare il numero di errori da consentire prima che il processo si interrompa e, se il runbook include uno script di rollback, esegua il rollback. È possibile monitorare i progressi utilizzando gli allarmi. CloudWatch

Al termine di un flusso di lavoro del runbook, è possibile esaminare i dettagli sulle modifiche apportate. Questi dettagli includono il motivo di una richiesta di modifica, quale modello di modifica è stato utilizzato, chi ha richiesto e approvato le modifiche e come sono state implementate.

Ulteriori informazioni

[Presentazione di AWS Systems ManagerChange Manager](#) sul Blog News AWS

## Come può Change Manager favorire le mie operazioni?

Alcuni vantaggi di Change Manager sono i seguenti:

- Riduzione del rischio di interruzioni del servizio e del tempo di inattività

Change Manager può rendere più sicure le modifiche operative assicurando che solo le modifiche approvate vengano implementate quando viene eseguito un flusso di lavoro del runbook. È possibile bloccare le modifiche non pianificate e non riviste. Change Manager consente di evitare i tipi di risultati involontari causati da errori umani che richiedono ore costose di ricerca e backtracking.

- Revisione dettagliata e creazione di report sulle cronologie delle modifiche

Change Manager fornisce responsabilità con un modo coerente per segnalare e controllare le modifiche apportate all'organizzazione, l'intento delle modifiche e i dettagli su chi le ha approvate e implementate.

- Evitare conflitti di pianificazione o violazioni

Change Manager è in grado di rilevare conflitti di pianificazione, ad esempio festività o lanci di nuovi prodotti, in base al calendario delle modifiche attivo per l'organizzazione. È possibile consentire l'esecuzione dei flussi di lavoro dei runbook solo durante l'orario di lavoro o consentirli solo con approvazioni aggiuntive.

- Adattare i requisiti di cambiamento alla vostra azienda in evoluzione

Durante diversi periodi di lavoro, è possibile implementare requisiti di gestione delle modifiche diversi. Ad esempio, durante i rapporti di fine mese, la stagione fiscale o altri periodi aziendali critici, è possibile bloccare le modifiche o richiedere l'approvazione a livello di amministratore per le modifiche che potrebbero introdurre rischi operativi non necessari.

- Gestione centralizzata delle modifiche tra gli account

Attraverso la sua integrazione con le organizzazioni, Change Manager consente di gestire le modifiche in tutte le unità organizzative (UO) da un unico account amministratore delegato. Puoi attivare Change Manager da utilizzare con l'intera organizzazione o solo con alcune unità organizzative.

## Chi dovrebbe usare Change Manager?

Change Manager è adatto per i seguenti AWS clienti e organizzazioni:

- Qualsiasi AWS cliente che desideri migliorare la sicurezza e la governance delle modifiche operative apportate ai propri ambienti cloud o on-premise.
- Organizzazioni che desiderano aumentare la collaborazione e la visibilità tra i team, migliorare la disponibilità delle applicazioni evitando il tempo di inattività e ridurre i rischi associati ai processi manuali e ripetitivi.
- Organizations che devono rispettare le procedure consigliate per la gestione delle modifiche.
- Clienti che necessitano di una cronologia completamente verificabile delle modifiche apportate alla configurazione e all'infrastruttura delle applicazioni.

## Quali sono le caratteristiche principali di Change Manager?

Le caratteristiche principali del Change Manager comprendono:

- Supporto integrato per le best practice di gestione delle modifiche

Con Change Manager è possibile applicare procedure consigliate per la gestione delle modifiche selezionate alle proprie operazioni. Puoi scegliere una delle seguenti opzioni:

- Controlla Change Calendar per verificare se gli eventi sono attualmente limitati, in modo che le modifiche vengano apportate solo durante i periodi di calendario aperti.
- Consenti modifiche durante gli eventi con restrizioni con approvazioni aggiuntive dai revisori del blocco delle modifiche.
- Richiedi che CloudWatch gli allarmi siano specificati per tutti i modelli di modifica.
- Richiedi la revisione e l'approvazione di tutti i modelli di modifica creati nel tuo account prima che possano essere utilizzati per creare richieste di modifica.
- Diversi percorsi di approvazione per periodi di calendario chiusi e richieste di modifica di emergenza

È possibile consentire a un'opzione di controllare Change Calendar se esistano eventi con restrizioni e bloccare le richieste di modifica approvate fino al completamento dell'evento. Tuttavia, è anche possibile designare un secondo gruppo di approvatori, ovvero i revisori di blocco, che possono consentire la modifica anche se il calendario è chiuso. Inoltre, è possibile creare modelli di modifica di emergenza. Le richieste di modifica create da un modello di modifica di emergenza richiedono comunque approvazioni regolari, ma non sono soggette a restrizioni di calendario e non richiedono approvazioni di blocco delle modifiche.

- Controllare come e quando vengono avviati i flussi di lavoro del runbook

I flussi di lavoro del runbook possono essere avviati in base a una pianificazione o non appena vengono completate le approvazioni (in base alle regole di restrizione del calendario).

- Built-in supporto per le notifiche

Specificare chi deve esaminare e approvare i modelli di modifica e le richieste di modifica nell'organizzazione. Assegna un argomento Amazon SNS a un modello di modifica per inviare notifiche agli abbonati dell'argomento sulle modifiche di stato per le richieste di modifica create con tale modello di modifica.

- Integrazione con AWS Systems Manager Change Calendar

Change Manager consente agli amministratori di limitare le modifiche alla pianificazione durante periodi di tempo specificati. Ad esempio, puoi creare una politica che consenta modifiche solo durante l'orario lavorativo per assicurarti che il team sia disponibile a gestire eventuali problemi. È inoltre possibile limitare le modifiche durante eventi business importanti. Ad esempio, le aziende al dettaglio potrebbero limitare le modifiche durante eventi di vendita di grandi dimensioni. È inoltre possibile richiedere ulteriori approvazioni durante i periodi limitati.

- Integrazione Centro identità AWS IAM e supporto per Active Directory

Con l'integrazione di IAM Identity Center, i membri dell'organizzazione possono accedere agli Account AWS e gestire le proprie risorse utilizzando Systems Manager in base a un'identità utente comune. Utilizzando IAM Identity Center, è possibile assegnare agli utenti l'accesso agli account tramite AWS.

L'integrazione con Active Directory consente di assegnare utenti nell'account Active Directory come approvatori per i modelli di modifica creati per le operazioni Change Manager.

- Integrazione con gli CloudWatch allarmi Amazon



Change Manager è integrato con gli CloudWatch allarmi. Change Manager ascolta gli CloudWatch allarmi durante il flusso di lavoro del runbook e intraprende tutte le azioni, incluso l'invio di notifiche, definite per l'allarme.

- Integrazione con Lake AWS CloudTrail

Creando un data store di eventi in AWS CloudTrail Lake, puoi visualizzare informazioni verificabili sulle modifiche apportate dalle richieste di modifica eseguite nel tuo account o nella tua organizzazione. Le informazioni sull'evento archiviate includono dettagli simili ai seguenti:

- Le operazioni API eseguite
  - I parametri di richiesta inclusi per tali operazioni
  - L'utente che ha eseguito l'operazione
  - Le risorse che sono state aggiornate durante il processo
- Integrazione con AWS Organizations

Utilizzando le funzionalità cross-account fornite dalle Organizations, è possibile utilizzare un account amministratore delegato per la gestione operazioni di Change Manager nelle unità organizzative nell'organizzazione. Nell'account di gestione delle Organizations è possibile specificare quale account deve essere l'account amministratore delegato. Puoi anche controllare in quale delle tue unità organizzative puoi utilizzare Change Manager.

## L'utilizzo è a pagamento Change Manager?

Sì. Per Change Manager il prezzo è calcolato in base all'utilizzo effettivo. I prezzi sono calcolati solo in base all'uso effettivo. Per ulteriori informazioni, consulta [AWS Systems Manager Prezzi](#).

## Quali sono i componenti principali di Change Manager?

I componenti Change Manager utilizzati per gestire il processo di modifica nell'organizzazione o nell'account includono i seguenti:

### Account amministratore delegato

Se utilizzi Change Manager in un'organizzazione, è possibile utilizzare un account amministratore delegato. Questo è l' Account AWS designato come account per la gestione delle attività operative in Systems Manager, tra cui Change Manager. L'account amministratore delegato gestisce le attività di modifica all'interno dell'organizzazione. Quando configuri l'organizzazione per l'utilizzo con Change Manager, è possibile specificare quali account servono in questo ruolo. L'account amministratore

delegato deve essere l'unico membro dell'unità organizzativa (UO) a cui è assegnato. L'account amministratore delegato non è richiesto se lo si utilizza Change Manager con un Account AWS solo account.

 Important

Se utilizzi Change Manager in un'organizzazione, si consiglia di apportare sempre modifiche dall'account amministratore delegato. Sebbene sia possibile apportare modifiche da altri account dell'organizzazione, tali modifiche non verranno segnalate o visualizzate dall'account amministratore delegato.

## Modello di modifica

Un modello di modifica è una raccolta di impostazioni di configurazione in Change Manager che definiscono le approvazioni obbligatorie, i runbook disponibili e le opzioni di notifica per le richieste di modifica.

È possibile richiedere che i modelli di modifica creati dagli utenti dell'organizzazione o dell'account vengano sottoposti a un processo di approvazione prima che possano essere utilizzati.

Change Manager supporta due tipi di modelli di modifica. Per una richiesta di modifica approvata basata su un Modello di modifica di emergenza, la modifica richiesta può essere apportata anche se ci sono eventi di blocco in Change Calendar. Per una richiesta di modifica approvata basata su un Modello di modifica standard, la modifica richiesta non può essere apportata se ci sono eventi di blocco in Change Calendar, a meno che non vengano ricevute approvazioni aggiuntive dagli approvatori per l'evento di blocco in caso di modifica.

## Richiesta di modifica

Una richiesta di modifica è una richiesta di esecuzione Change Manager di un runbook di Automation che aggiorna una o più risorse negli ambienti aziendali AWS o locali. Una richiesta di modifica viene creata utilizzando un modello di modifica.

Quando si crea una richiesta di modifica, uno o più approvatori nell'organizzazione o nell'account devono esaminare e approvare la richiesta. Senza le approvazioni richieste, il flusso di lavoro del runbook, che applica le modifiche richieste, non può essere eseguito.

Nel sistema, le richieste di modifica sono un tipo di OpsItem input. AWS Systems Manager OpsCenter Tuttavia, OpsItems del tipo `/aws/changerequest` non vengono visualizzati in

OpsCenter. In quanto OpsItems, le richieste di modifica sono soggette alle stesse quote applicate di altri tipi di OpsItems.

Inoltre, per creare una richiesta di modifica a livello di codice, non chiamare l'operazione API `CreateOpsItem`. Usa invece l'operazione API [StartChangeRequestExecution](#). Prima dell'esecuzione, la richiesta di modifica deve essere approvata e non devono essere presenti eventi di blocco in Change Calendar che impediscono l'esecuzione del flusso di lavoro. Quando le approvazioni sono state ricevute e il calendario non è bloccato (o è stata concessa l'autorizzazione per bypassare il blocco degli eventi del calendario), l'`StartChangeRequestExecution` può essere completata.

### Flusso di lavoro di runbook

Un flusso di lavoro del runbook è il processo delle modifiche richieste apportate alle risorse di destinazione nel cloud o nell'ambiente on-premises. Ogni richiesta di modifica designa un singolo runbook Automation da utilizzare per apportare le modifiche richieste. Il flusso di lavoro del runbook si verifica dopo che tutte le approvazioni richieste sono state concesse e non ci sono eventi di blocco in Change Calendar. Se la modifica è stata pianificata per una data e un'ora specifiche, il flusso di lavoro del runbook non inizia fino alla pianificazione, anche se tutte le approvazioni sono state ricevute e il calendario non è bloccato.

### Argomenti

- [Configurazione Change Manager](#)
- [Lavorare con Change Manager](#)
- [Controllo e registrazione Change Manager activity](#)
- [Risoluzione dei problemi Change Manager](#)

## Configurazione Change Manager

### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

È possibile Change Manager utilizzarlo per gestire le modifiche per un'intera organizzazione, come configurato in AWS Organizations, o per una singola organizzazione Account AWS.

Se si utilizza Change Manager con un'organizzazione, iniziare con l'argomento [Configurazione Change Manager per un'organizzazione \(account di gestione\)](#) e procedere a [Configurazione Change Manager opzioni e best practice](#).

Se si utilizza Change Manager con un singolo account, procedere direttamente a [Configurazione Change Manager opzioni e best practice](#).

#### Note

Se si utilizza Change Manager con un singolo account, ma questo viene successivamente aggiunto a un'unità organizzativa per la quale Change Manager è consentito, le impostazioni dell'account singolo vengono ignorate.

## Argomenti

- [Configurazione Change Manager per un'organizzazione \(account di gestione\)](#)
- [Configurazione Change Manager opzioni e best practice](#)
- [Configurazione di ruoli e autorizzazioni per Change Manager](#)
- [Controllo dell'accesso ai flussi di lavoro del runbook di approvazione automatica](#)

## Configurazione Change Manager per un'organizzazione (account di gestione)

#### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

Le attività descritte in questo argomento si applicano se utilizzi un'organizzazione Change Manager con sede in AWS Organizations. Se desideri utilizzarle Change Manager solo con una singola Account AWS persona, passa all'argomento [Configurazione Change Manager opzioni e best practice](#).

Esegui le attività descritte in questa sezione in un account AWS che funge da account di gestione in Organizzazioni. Per informazioni sull'account di gestione e su altri concetti relativi alle organizzazioni, consulta [Concetti e terminologia AWS Organizations](#).

Se è necessario attivare Organizations e specificare il proprio account come account di gestione prima di procedere, consulta [Creating and managing an organization \(Creazione e gestione di un'organizzazione\)](#) nella Guida per l'utente AWS Organizations .

#### Note

Questo processo di configurazione non può essere eseguito nei seguenti modi Regioni AWS:

- Europa (Milano) (eu-south-1)
- Medio Oriente (Bahrein) (me-south-1)
- Africa (Città del Capo) (af-south-1)
- Asia Pacifico (Hong Kong) ap-east-1

Assicurati di lavorare in una regione diversa nel tuo account di gestione per questa procedura.

Durante la procedura di configurazione, esegui le seguenti attività principali in Quick Setup, uno strumento di AWS Systems Manager.

- Processo 1: registrare l'account amministratore delegato per l'organizzazione

I processi correlati alle modifiche eseguite utilizzando Change Manager sono gestite in uno dei tuoi account membri, da indicare come account amministratore delegato. L'account amministratore delegato registrato in Change Manager diventa l'account amministratore delegato per tutte le operazioni di Systems Manager. (Potresti avere account di amministratore delegato per altri account Servizi AWS). L'account di amministratore delegato per Change Manager, che non è uguale all'account di gestione, gestisce le attività di modifica all'interno dell'organizzazione, inclusi modelli di modifica, richieste di modifica e approvazioni per ciascuna di esse. Nell'account amministratore delegato è inoltre possibile specificare altre opzioni di configurazione per le operazioni Change Manager.

 Important

L'account amministratore delegato deve essere l'unico membro dell'unità organizzativa (UO) a cui è assegnato in Organizzazioni.

- Processo 2: definire e specificare i criteri di accesso al runbook per i ruoli del richiedente di modifica o le funzioni di processo personalizzate che si desidera utilizzare per le operazioni Change Manager

Per creare richieste di modifica inChange Manager, agli utenti degli account membri devono essere concesse le autorizzazioni AWS Identity and Access Management (IAM) che consentano loro di accedere solo ai runbook di Automation e ai modelli di modifica che scegli di rendere loro disponibili.

 Note

Quando un utente crea una richiesta di modifica, seleziona innanzitutto un modello di modifica. Questo modello di modifica potrebbe rendere disponibili più runbook, ma l'utente può selezionare un solo runbook per ogni richiesta di modifica. È inoltre possibile configurare i modelli di modifica per consentire agli utenti di includere qualsiasi runbook disponibile nelle proprie richieste.

Per concedere le autorizzazioni necessarie, Change Manager utilizza il concetto di funzioni di processo, che viene utilizzato anche da IAM. Tuttavia, a differenza delle [policy AWS gestite per le funzioni di processo](#) in IAM, è possibile specificare entrambi i nomi dell'utente Change Manager per le funzioni di processo e le autorizzazioni IAM per tali funzioni di processo.

Quando si configura una funzione di processo, si consiglia di creare una policy personalizzata e di fornire solo le autorizzazioni necessarie per eseguire i processi di gestione delle modifiche. Ad esempio, puoi specificare le autorizzazioni che limitano gli utenti a quel set specifico di runbook in base a funzioni di processo che definisci.

Ad esempio, è possibile creare una funzione di processo con il nome DBAdmin. Per questa funzione di processo, è possibile concedere solo le autorizzazioni necessarie per i runbook correlati ai database Amazon DynamoDB, ad esempio AWS-CreateDynamoDbBackup e AWSConfigRemediation-DeleteDynamoDbTable.

Ad esempio, potresti voler concedere ad alcuni utenti solo le autorizzazioni necessarie per lavorare con i runbook correlati ai bucket Amazon Simple Storage Service (Amazon S3), ad esempio `AWS-ConfigureS3BucketLogging` e `AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock`.

Il processo di configurazione in Quick Setup per Change Manager rende inoltre disponibile un set di autorizzazioni amministrative complete di Systems Manager da applicare a un ruolo amministrativo creato dall'utente.

Ogni configurazione Change Manager Quick Setup distribuita crea una funzione di processo nell'account amministratore delegato con autorizzazioni per l'esecuzione di modelli Change Manager e runbook di Automazione nelle unità organizzative selezionate. È possibile creare fino a 15 configurazioni Quick Setup per Change Manager.

- Processo 3: scegliere gli account membri dell'organizzazione da utilizzare con Change Manager

Puoi utilizzare Change Manager con tutti gli account membri in tutte le unità organizzative impostate in Organizzazioni e in tutte le Regioni AWS in cui operano. Se preferisci, puoi invece utilizzare Change Manager solo con alcune delle unità organizzative.

#### Important

Si consiglia vivamente, prima di iniziare questa procedura, di leggere i passaggi relativi per comprendere le scelte di configurazione che si stanno facendo e le autorizzazioni concesse. In particolare, pianificare le funzioni di processo personalizzate che verranno create e le autorizzazioni assegnate a ciascuna funzione di processo. In questo modo, quando successivamente si allegano i criteri delle funzioni di processo creati a singoli utenti, gruppi di utenti o ruoli IAM, vengono concesse solo le autorizzazioni che si intende disporre. Come procedura consigliata, inizia configurando l'account amministratore delegato utilizzando il login di un amministratore. Account AWS Configurare quindi le funzioni del processo e le relative autorizzazioni dopo aver creato i modelli di modifica e identificato i runbook utilizzati da ciascuno di essi.

Per configurare Change Manager per l'utilizzo con un'organizzazione, eseguire il seguente processo in Quick Setup della console Systems Manager.

Ripetere questo processo per ogni funzione di processo che si desidera creare per l'organizzazione. Ogni funzione di processo creata può disporre delle autorizzazioni per un set diverso di unità organizzative.

Per configurare un'organizzazione per Change Manager nell'account di gestione delle organizzazioni

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Quick Setup.
3. Nella scheda Change Manager, scegli Create (Crea).
4. In Account amministratore delegato (Abilita un account di amministratore delegato), immetti l'ID della Account AWS che si desidera utilizzare per la gestione di modelli di modifica, richieste di modifica e flussi di lavoro del runbook in Change Manager.

Se in precedenza è stato specificato un account amministratore delegato per Systems Manager, il relativo ID viene già segnalato in questo campo.

 Important

L'account amministratore delegato deve essere l'unico membro dell'unità organizzativa (UO) a cui è assegnato in Organizzazioni.

Se l'account amministratore delegato registrato viene successivamente annullato da tale ruolo, il sistema rimuove le autorizzazioni per la gestione delle operazioni di Systems Manager contemporaneamente. Tieni presente che sarà necessario per tornare a Quick Setup, designare un account amministratore delegato diverso e specificare nuovamente tutte le funzioni e le autorizzazioni di processo.

Se utilizzi Change Manager in un'organizzazione, si consiglia di apportare sempre modifiche dall'account amministratore delegato. Sebbene sia possibile apportare modifiche da altri account dell'organizzazione, tali modifiche non verranno segnalate o visualizzate dall'account amministratore delegato.

5. Nelle Permissions to request and make change (Autorizzazioni per richiedere e apportare modifiche), procedi come indicato di seguito.

 Note

Ogni configurazione di implementazione che è stata creata fornisce policy di autorizzazione per una sola funzione di processo. È possibile tornare a Quick Setup in



seguito per creare più funzioni di processo quando sono stati creati modelli di modifica da utilizzare nelle operazioni.

Per creare un ruolo amministrativo— Per una funzione di processo di amministratore che dispone di autorizzazioni IAM per tutte le operazioni AWS , procedere come descritto di seguito.

 Important

La concessione di autorizzazioni amministrative complete agli utenti deve essere eseguita con parsimonia e solo se i ruoli richiedono l'accesso completo a Systems Manager. Per informazioni importanti sulle considerazioni sulla sicurezza per l'accesso a Systems Manager, consulta [Gestione delle identità e degli accessi per AWS Systems Manager](#) e [Le migliori pratiche di sicurezza per Systems Manager](#).

1. Per Funzione di processo, immettere un nome per identificare questo ruolo e le relative autorizzazioni, ad esempio **My AWS Admin**.
2. Per l'opzione Ruolo e autorizzazioni, scegliere Autorizzazioni dell'amministratore.

Creare altre funzioni di processo; per creare un ruolo non amministrativo, procedere come segue:

1. Per Funzione di processo, immettere un nome per identificare questo ruolo e suggerirne le autorizzazioni. Il nome scelto dovrebbe rappresentare l'ambito dei runbook per i quali fornisci le autorizzazioni, ad esempio DBAdmin o S3Admin
2. Per l'opzione Ruolo e autorizzazioni, scegliere Autorizzazioni personalizzate.
3. Nell'Editor della policy di autorizzazione, immettere le autorizzazioni IAM, in formato JSON, da concedere a questa funzione di processo.

 Tip

Si consiglia di utilizzare l'editor della policy IAM per costruire il criterio e quindi incollare il criterio JSON nel file Policy delle autorizzazioni.

## Policy di esempio: gestione del database DynamoDB

Ad esempio, è possibile iniziare con il contenuto di policy che fornisce autorizzazioni per l'utilizzo dei documenti di Systems Manager (documenti SSM) a cui la funzione di processo deve accedere. Ecco un esempio di contenuto di policy che consente l'accesso a tutti i runbook di automazione AWS gestiti relativi ai database DynamoDB e a due modelli di modifica che sono stati creati nell'esempio Account AWS 123456789012, nella regione degli Stati Uniti orientali (Ohio) (). us-east-2

La policy include anche l'autorizzazione per l'operazione [StartChangeRequestExecution](#), necessaria per creare una richiesta di modifica in Change Calendar.

### Note

Questo esempio non è completo. Potrebbero essere necessarie autorizzazioni aggiuntive per lavorare con altre AWS risorse, come database e nodi.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:CreateDocument",
 "ssm:DescribeDocument",
 "ssm:DescribeDocumentParameters",
 "ssm:DescribeDocumentPermission",
 "ssm:GetDocument",
 "ssm:ListDocumentVersions",
 "ssm:ModifyDocumentPermission",
 "ssm:UpdateDocument",
 "ssm:UpdateDocumentDefaultVersion"
],
 "Resource": [
 "arn:aws:ssm:us-east-1:*:document/AWS-CreateDynamoDbBackup",
```

```

 "arn:aws:ssm:us-east-1:*:document/AWS-AWS-DeleteDynamoDbBackup",
 "arn:aws:ssm:us-east-1:*:document/AWS-DeleteDynamoDbTableBackups",
 "arn:aws:ssm:us-east-1:*:document/AWSConfigRemediation-DeleteDynamoDbTable",
 "arn:aws:ssm:us-east-1:*:document/AWSConfigRemediation-EnableEncryptionOnDynamoDbTable",
 "arn:aws:ssm:us-east-1:*:document/AWSConfigRemediation-EnablePITRForDynamoDbTable",
 "arn:aws:ssm:us-east-1:111122223333:document/MyFirstDBChangeTemplate",
 "arn:aws:ssm:us-east-1:111122223333:document/MySecondDBChangeTemplate"
]
},
{
 "Effect": "Allow",
 "Action": "ssm:ListDocuments",
 "Resource": "*"
},
{
 "Effect": "Allow",
 "Action": "ssm:StartChangeRequestExecution",
 "Resource": [
 "arn:aws:ssm:us-east-1:111122223333:document/*",
 "arn:aws:ssm:us-east-1:111122223333:automation-execution/*"
]
}
]
}

```

Per ulteriori informazioni sulle policy IAM, consulta [Gestione degli accessi per Risorse AWS](#) e [Creazione di policy IAM](#) nella Guida per l'utente IAM.

6. Nella sezione Destinazioni, scegli se concedere le autorizzazioni per la funzione di processo che stai creando per l'intera organizzazione o solo ad alcune unità organizzative.

Se si sceglie Intera organizzazione continuare con la fase 9.

Se si sceglie Personalizza continuare con la fase 8.

7. Nella sezione Unità organizzative di destinazione, seleziona le caselle di controllo delle unità organizzative da utilizzare con Change Manager.
8. Scegliere Create (Crea).

Al termine della configurazione del sistema Change Manager per l'organizzazione, visualizza un riepilogo delle implementazioni. Queste informazioni di riepilogo includono il nome del ruolo creato per la funzione di processo configurata. Ad esempio, `AWS-QuickSetup-SSMChangeMgr-DBAdminInvocationRole`.

#### Note

Quick Setup utilizza AWS CloudFormation StackSets per distribuire le tue configurazioni. È inoltre possibile visualizzare le informazioni su una configurazione di implementazione completata nella console CloudFormation. Per informazioni su StackSets, vedere [Lavorare con AWS CloudFormation StackSets](#) nella Guida per l'AWS CloudFormation utente.

La fase successiva consiste nel configurare ulteriori opzioni Change Manager. È possibile completare questo processo nell'account amministratore delegato o in qualsiasi account in un'unità organizzativa consentita per l'utilizzo con Change Manager. È possibile configurare opzioni quali la scelta di un'opzione di gestione delle identità utente, specificare gli utenti che possono esaminare e approvare o rifiutare i modelli di modifica e le richieste di modifica e scegliere le opzioni di best practice da consentire per l'organizzazione. Per informazioni, consulta [Configurazione Change Manager opzioni e best practice](#).

#### Configurazione Change Manager opzioni e best practice

#### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

Le attività descritte in questa sezione devono essere eseguite indipendentemente dal fatto che si utilizzi Change Manager uno strumento all'interno AWS Systems Manager, all'interno di un'organizzazione o in un'unica organizzazione Account AWS.

Se usi Change Manager per un'organizzazione, è possibile eseguire i seguenti processi nell'account amministratore delegato o in qualsiasi account in un'unità organizzativa consentita per l'utilizzo con Change Manager.

## Argomenti

- [Attività 1: Configurazione Change Manager gestione delle identità degli utenti e revisori dei modelli](#)
- [Attività 2: Configurazione Change Manager approvatori e best practice degli eventi di blocco delle modifiche](#)
- [Configurazione degli argomenti di Amazon SNS per Change Manager notifiche](#)

### Attività 1: Configurazione Change Manager gestione delle identità degli utenti e revisori dei modelli

Eseguire il processo in questa procedura la prima volta che si accede a Change Manager. È possibile aggiornare queste impostazioni di configurazione in un secondo momento tornando a Change Manager e scegliendo Modificare nella scheda Impostazioni.

Per configurare Change Manager gestione delle identità degli utenti e revisori dei modelli

1. Accedi alla Console di gestione AWS.

Se usi Change Manager per un'organizzazione, accedere utilizzando le credenziali per l'account amministratore delegato. L'utente deve disporre delle autorizzazioni AWS Identity and Access Management (IAM) necessarie per eseguire aggiornamenti alle impostazioni Change Manager.

2. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
3. Nel pannello di navigazione, scegli Change Manager.
4. Nella home page del servizio, a seconda delle opzioni disponibili, seguire la procedura riportata di seguito:

- Se stai utilizzando Change Manager con AWS Organizations , scegli Configura account delegato.
- Se utilizzi Change Manager un singolo utente Account AWS, scegli Configura Change Manager.

oppure

Scegliere Crea richiesta di modifica di esempio, Salta e quindi seleziona la scheda Impostazioni.

5. Per Gestione delle identità degli utenti scegliere una delle seguenti opzioni.
  - AWS Identity and Access Management (IAM): identifica gli utenti che effettuano e approvano le richieste ed eseguono altre azioni Change Manager utilizzando gli utenti, i gruppi e i ruoli esistenti.
  - Centro identità AWS IAM (IAM Identity Center): consenti [a](#) IAM Identity Center di creare e gestire identità o di connettersi alla fonte di identità esistente per identificare gli utenti che eseguono azioni in. Change Manager
6. Nella sezione Notifica del revisore del modello, specifica gli argomenti di Amazon Simple Notification Service (Amazon SNS) da utilizzare per notificare ai revisori che un nuovo modello di modifica o una versione del modello di modifica sono pronti per essere esaminati. Assicurati che l'argomento Amazon SNS che scegli sia configurato per inviare notifiche ai revisori dei modelli.

Per informazioni sulla creazione e la configurazione degli argomenti di Amazon SNS per le notifiche del revisore dei modelli di modifica, consulta [Configurazione degli argomenti di Amazon SNS per Change Manager notifiche](#).

1. Per specificare l'argomento Amazon SNS per la notifica del revisore dei modelli, scegli una delle seguenti opzioni:
  - Inserisci un SNS Amazon Resource Name (ARN) – Per argomento ARN immetti l'ARN di un argomento Amazon SNS esistente. Questo argomento può essere incluso in qualsiasi account dell'organizzazione.
  - Selezionare un argomento SNS esistente— Per Argomento notifica destinazione, seleziona l'ARN di un argomento Amazon SNS esistente nel tuo Account AWS. (Questa opzione non è disponibile se non hai ancora creato alcun argomento Amazon SNS nel tuo indirizzo attuale Account AWS ). Regione AWS

 Note

L'argomento Amazon SNS selezionato deve essere configurato in modo da specificare le notifiche inviate e gli abbonati a cui vengono inviati. La sua policy di accesso deve inoltre concedere autorizzazioni a Systems Manager in modo che Change Manager può inviare notifiche. Per informazioni, consulta [Configurazione degli argomenti di Amazon SNS per Change Manager notifiche](#).

2. Scegliere Add notification (Aggiungi notifica).

7. Nella sezione Modificare i revisori del modello, selezionare gli utenti dell'organizzazione o dell'account per la revisione dei nuovi modelli di modifica o per modificare le versioni dei modelli prima che possano essere utilizzati nelle operazioni.

I revisori dei modelli di modifica sono responsabili della verifica dell'idoneità e della sicurezza dei modelli inviati da altri utenti per l'utilizzo in flussi di lavoro del runbook Change Manager.

Selezionare i revisori dei modelli di modifica eseguendo le operazioni seguenti:

1. Scegliere Aggiungi.
  2. Selezionare la casella di controllo accanto al nome di ciascun utente, gruppo o ruolo IAM che desideri assegnare come revisore del modello di modifica.
  3. Scegliere Aggiungi approvatori.
8. Seleziona Invia.

Dopo aver completato questo processo di installazione iniziale, configurare Change Manager e procedure consigliate attenendosi alla procedura descritta in [Attività 2: Configurazione Change Manager approvatori e best practice degli eventi di blocco delle modifiche](#).

Attività 2: Configurazione Change Manager approvatori e best practice degli eventi di blocco delle modifiche

Dopo aver completato i passaggi descritti in [Attività 1: Configurazione Change Manager gestione delle identità degli utenti e revisori dei modelli](#), è possibile designare revisori aggiuntivi per le richieste di modifica durante gli eventi di blocco delle modifiche e specificare quali best practice disponibili si desidera consentire per le operazioni in Change Manager.

Un evento di blocco delle modifiche indica che sono in vigore delle restrizioni nel calendario delle modifiche corrente (lo stato del calendario è). AWS Systems Manager Change Calendar CLOSED In questi casi, oltre ai normali approvatori per le richieste di modifica o se la richiesta di modifica viene creata utilizzando un modello che consente l'approvazione automatica, gli approvatori del blocco delle modifiche devono concedere l'autorizzazione per l'esecuzione della richiesta di modifica. In caso contrario, la modifica non verrà elaborata fino a quando lo stato del calendario non sarà nuovamente OPEN.

Per configurare Change Manager approvatori e best practice degli eventi di blocco delle modifiche

1. Nel pannello di navigazione, scegli Change Manager.

2. Seleziona la scheda Web Settings (Impostazioni Web) e scegli Edit (Modifica).
3. Nella sezione Approvatori per gli eventi di blocco delle modifiche selezionare gli utenti dell'organizzazione o dell'account che possono approvare le modifiche da eseguire anche quando il calendario in uso in Change Calendar è CHIUSO.

 Note

Per consentire revisioni di blocco delle modifiche, è necessario attivare l'opzione Controlla calendario delle modifiche per eventi di modifiche limitati in Best practice.

Selezionare gli approvatori per gli eventi di blocco delle modifiche eseguendo le operazioni seguenti:

1. Scegliere Aggiungi.
2. Selezionare la casella di controllo accanto al nome di ciascun utente, gruppo o ruolo IAM che desideri assegnare come approvatore per gli eventi di blocco delle modifiche.
3. Scegliere Aggiungi approvatori.
4. Nella sezione Best practice, situata nella parte inferiore della pagina, attivare le procedure consigliate che si desidera applicare per ciascuna delle seguenti opzioni.

- Opzione: Controlla calendario delle modifiche per eventi di modifiche limitati

Per specificare che Change Manager controlla un calendario in Change Calendar per assicurarti che le modifiche non siano bloccate dagli eventi pianificati, seleziona prima la casella di controllo Abilitato e quindi seleziona il calendario per verificare la presenza di eventi limitati nell'elenco presente nell'elenco Calendario delle modifiche.

Per ulteriori informazioni su Change Calendar, consultare [AWS Systems Manager Modifica calendario](#).

- Opzione: Argomento SNS per approvatori di eventi chiusi
  1. Scegli una delle seguenti opzioni per specificare l'argomento Amazon Simple Notification Service (Amazon SNS) nel tuo account da utilizzare per inviare notifiche agli approvatori durante gli eventi di blocco delle modifiche. (Si noti che è necessario specificare anche i revisori nella sezione Approvatori per gli eventi di blocco delle modifiche sopra Best practice.)



- Inserisci un SNS Amazon Resource Name (ARN) – Per argomento ARN immetti l'ARN di un argomento Amazon SNS esistente. Questo argomento può essere incluso in qualsiasi account dell'organizzazione.
- Selezionare un argomento SNS esistente— Per Argomento notifica destinazione, seleziona l'ARN di un argomento Amazon SNS esistente nel tuo Account AWS. (Questa opzione non è disponibile se non hai ancora creato alcun argomento Amazon SNS nel tuo indirizzo attuale). Account AWS Regione AWS

 Note

L'argomento Amazon SNS selezionato deve essere configurato in modo da specificare le notifiche inviate e gli abbonati a cui vengono inviati. La sua policy di accesso deve inoltre concedere autorizzazioni a Systems Manager in modo che Change Manager può inviare notifiche. Per informazioni, consulta [Configurazione degli argomenti di Amazon SNS per Change Manager notifiche](#).

2. Scegliere Add notification (Aggiungi notifica).

- Opzione: Richiedi monitoraggi per tutti i modelli

Se vuoi assicurarti che tutti i modelli per la tua organizzazione o il tuo account specifichino un CloudWatch allarme Amazon per monitorare l'operazione di modifica, seleziona la casella di controllo **Abilitato**.

- Opzione: Richiedi revisione e approvazione del modello prima dell'uso

Per assicurarti che non vengano create richieste di modifica e che non vengano eseguiti flussi di lavoro di runbook senza basarsi su un modello che è stato esaminato e approvato, seleziona la casella di controllo **Abilitato**.

5. Selezionare Salva.

## Configurazione degli argomenti di Amazon SNS per Change Manager notifiche

 Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti

esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

Puoi configurare l'invio Change Manager di notifiche a un argomento di Amazon Simple Notification Service (Amazon SNS) per eventi relativi alle richieste di modifica e ai modelli di modifica. Completare i seguenti processi per ricevere le notifiche per eventi Change Manager a cui si aggiunge un argomento.

### Argomenti

- [Processo 1: Creazione e iscrizione a un argomento Amazon SNS](#)
- [Processo 2: Aggiornamento delle policy di accesso Amazon SNS](#)
- [Attività 3: \(Facoltativo\) Aggiorna il AWS Key Management Service policy d'accesso](#)

### Processo 1: Creazione e iscrizione a un argomento Amazon SNS

Come prima cosa crea e sottoscrivi un argomento Amazon SNS. Per ulteriori informazioni, consulta [Creazione di un argomento Amazon SNS](#) e [Iscrizione a un argomento Amazon SNS](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service.

#### Note

Per ricevere notifiche, devi specificare l'Amazon Resource Name (ARN) di un argomento Amazon SNS che si trova nello stesso account Regione AWS e nell'account di Account AWS amministratore delegato.

### Processo 2: Aggiornamento delle policy di accesso Amazon SNS

Utilizza la procedura seguente per aggiornare la policy di accesso in modo che Systems Manager possa pubblicare notifiche Change Manager nell'argomento Amazon SNS creato nel processo 1. Senza completare questo processo, Change Manager non dispone dell'autorizzazione per inviare notifiche per gli eventi per cui aggiungi l'argomento.

1. Accedi Console di gestione AWS e apri la console Amazon SNS all'indirizzo. <https://console.aws.amazon.com/sns/v3/home>
2. Nel pannello di navigazione, scegli Argomenti.

3. Scegli l'argomento creato nel processo 1, quindi seleziona Edit (Modifica).
4. Espandi Policy di accesso.
5. Aggiungi e aggiorna il seguente Sid blocco alla policy esistente e sostituisci ciascuno *user input placeholder* con le tue informazioni.

```
{
 "Sid": "Allow Change Manager to publish to this topic",
 "Effect": "Allow",
 "Principal": {
 "Service": "ssm.amazonaws.com"
 },
 "Action": "sns:Publish",
 "Resource": "arn:aws:sns:region:account-id:topic-name",
 "Condition": {
 "StringEquals": {
 "aws:SourceAccount": [
 "account-id"
]
 }
 }
}
```

Inserisci questo blocco dopo il Sid blocco esistente e sostituiscilo *region topic-name* con i valori appropriati per l'argomento che hai creato. *account-id*

6. Scegli Save changes (Salva modifiche).

Il sistema invia ora notifiche all'argomento Amazon SNS quando si verifica il tipo di evento che aggiungi all'argomento.

#### Important

Se hai configurato l'argomento Amazon SNS con una chiave di crittografia lato server AWS Key Management Service (AWS KMS), devi completare l'attività 3.

### Attività 3: (Facoltativo) Aggiorna il AWS Key Management Service policy d'accesso

Se hai attivato AWS Key Management Service (AWS KMS) la crittografia lato server per il tuo argomento Amazon SNS, devi aggiornare anche la politica di accesso scelta al momento della AWS

KMS key configurazione dell'argomento. Utilizza la procedura seguente per aggiornare la policy di accesso in modo che Systems Manager possa pubblicare notifiche di approvazione Change Manager per l'argomento Amazon SNS creato nel processo 1.

1. Apri la console all' AWS KMS indirizzo. <https://console.aws.amazon.com/kms>
2. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
3. Selezionare l'ID della chiave master del cliente scelta al momento della creazione dell'argomento.
4. Nella sezione Policy della chiave, scegli Passa alla visualizzazione della policy.
5. Scegli Modifica.
6. Immettere il seguente blocco Sid dopo uno dei blocchi Sid esistenti nella politica esistente. Sostituisci ogni *user input placeholder* con le tue informazioni.

```
{
 "Sid": "Allow Change Manager to decrypt the key",
 "Effect": "Allow",
 "Principal": {
 "Service": "ssm.amazonaws.com"
 },
 "Action": [
 "kms:Decrypt",
 "kms:GenerateDataKey*"
],
 "Resource": "arn:aws:kms:region:account-id:key/key-id",
 "Condition": {
 "StringEquals": {
 "aws:SourceAccount": [
 "account-id"
]
 }
 }
}
```

7. Ora immetti il seguente blocco Sid dopo uno dei blocchi Sid esistenti nella politica delle risorse per aiutare a prevenire il [problema del “confused deputy” di servizi incrociati](#).

Questo blocco utilizza le chiavi di contesto delle condizioni globali [aws:SourceArn](#) e [aws:SourceAccount](#) per limitare le autorizzazioni con cui Systems Manager fornisce un altro servizio alla risorsa.

Sostituisci ogni *user input placeholder* con le tue informazioni.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "Configure confused deputy protection for AWS KMS keys
used in Amazon SNS topic when called from Systems Manager",
 "Effect": "Allow",
 "Principal": {
 "Service": "ssm.amazonaws.com"
 },
 "Action": [
 "sns:Publish"
],
 "Resource": "arn:aws:sns:us-east-1:111122223333:topic-name",
 "Condition": {
 "ArnLike": {
 "aws:SourceArn": "arn:aws:ssm:us-east-1:111122223333:*"
 },
 "StringEquals": {
 "aws:SourceAccount": "111122223333"
 }
 }
 }
]
}
```

8. Scegli Save changes (Salva modifiche).

Configurazione di ruoli e autorizzazioni per Change Manager

#### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti

esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems ManagerChange Manager la modifica della disponibilità](#).

Per impostazione predefinita, Change Manager non è autorizzato a eseguire operazioni sulle tue risorse. È necessario concedere l'accesso utilizzando un ruolo di servizio AWS Identity and Access Management (IAM) o assumere un ruolo. Questo ruolo consente a Change Manager di eseguire in modo sicuro i flussi di lavoro dei runbook specificati in una richiesta di modifica approvata per tuo conto. Il ruolo concede [AssumeRole](#) fiducia a Servizio di token di sicurezza AWS Change Manager (AWS STS).

Fornendo a un ruolo queste autorizzazioni per agire per conto degli utenti di un'organizzazione, non è necessario che agli utenti venga concessa tale serie di autorizzazioni. Le operazioni consentite dalle autorizzazioni sono limitate solo alle operazioni approvate.

Quando gli utenti dell'account o dell'organizzazione creano una richiesta di modifica, possono selezionare questo ruolo assunto per eseguire le operazioni di modifica.

Puoi creare un nuovo ruolo assunto per Change Manager oppure aggiornare un ruolo esistente con le autorizzazioni necessarie.

Se devi creare un ruolo di servizio per Change Manager, completa le seguenti attività.

## Processi

- [Attività 1: Creazione di una politica di assunzione del ruolo per Change Manager](#)
- [Attività 2: creazione di un ruolo di assunzione per Change Manager](#)
- [Attività 3: Allegare la PassRole policy iam: ad altri ruoli](#)
- [Attività 4: Aggiungere criteri in linea a un ruolo di assunzione per richiamarne altri Servizi AWS](#)
- [Attività 5: Configurazione dell'accesso utente a Change Manager](#)

### Attività 1: Creazione di una politica di assunzione del ruolo per Change Manager

Utilizza la procedura seguente per creare la policy che sarà allegata al tuo ruolo assunto di Change Manager.

Creare una politica di assunzione del ruolo per Change Manager

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.

2. Nel riquadro di navigazione, seleziona Policies (Policy) e Create Policy (Crea policy).
3. Sulla pagina Create policy (Crea policy), scegli la scheda JSON e sostituisci il contenuto di default con quanto segue, che modificherai per le tue operazioni di Change Manager nelle fasi seguenti.

#### Note

Se stai creando una policy da utilizzare con una singola Account AWS organizzazione e non con più account Regioni AWS, puoi omettere il primo blocco di dichiarazioni. L'autorizzazione `iam:PassRole` non è richiesta nel caso in cui un singolo account utilizzi Change Manager.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "iam:PassRole",
 "Resource": "arn:aws:iam::111122223333:role/AWS-SystemsManager-job-functionAdministrationRole",
 "Condition": {
 "StringEquals": {
 "iam:PassedToService": "ssm.amazonaws.com"
 }
 }
 },
 {
 "Effect": "Allow",
 "Action": [
 "ssm:DescribeDocument",
 "ssm:GetDocument",
 "ssm:StartChangeRequestExecution"
],
 "Resource": [
 "arn:aws:ssm:us-east-1::document/template-name",
 "arn:aws:ssm:us-east-1:111122223333:automation-execution/*"
]
 }
]
}
```

```
 },
 {
 "Effect": "Allow",
 "Action": [
 "ssm:ListOpsItemEvents",
 "ssm:GetOpsItem",
 "ssm:ListDocuments",
 "ssm:DescribeOpsItems"
],
 "Resource": "*"
 }
]
}
```

4. Per l'operazione `iam:PassRole`, aggiorna il valore `Resource` in modo da includere gli ARN di tutte le funzioni di processo definite per l'organizzazione a cui desideri concedere le autorizzazioni per avviare i flussi di lavoro dei runbook.
5. Sostituisci i valori *regionaccount-id*, *template-namedelegated-admin-account-id*, e *job-function* segnaposto con valori per le tue operazioni. Change Manager
6. Per la seconda istruzione di `Resource`, modifica l'elenco in modo da includere tutti i modelli di modifica per i quali desideri concedere le autorizzazioni. In alternativa, specifica `"Resource": "*"`  per concedere le autorizzazioni per tutti i modelli di modifica nell'organizzazione.
7. Scegli Successivo: Tag.
8. (Facoltativo) Aggiungere una o più coppie tag chiave-valore per organizzare, monitorare o controllare l'accesso per questa policy.
9. Scegli Prossimo: Rivedi.
10. Nella pagina Review policy (Rivedi policy), immetti un nome nella casella Name (Nome), ad esempio **MyChangeManagerAssumeRole**, quindi immetti una descrizione facoltativa.
11. Scegli Create policy (Crea policy) e continua con [Attività 2: creazione di un ruolo di assunzione per Change Manager](#).

## Attività 2: creazione di un ruolo di assunzione per Change Manager

Utilizza la procedura seguente per creare un ruolo assunto di Change Manager, un tipo di ruolo di servizio, per Change Manager.



## Creare un ruolo di assunzione per Change Manager

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, scegli Ruoli e quindi Crea ruolo.
3. Per Select trusted entity (Seleziona un'entità attendibile), effettua le seguenti selezioni:
  1. Per Trusted entity type (Tipo di entità attendibile), scegli AWS service (Servizio)
  2. Per altri casi d'uso Servizi AWS, scegli Systems Manager
  3. Scegli Systems Manager, come mostrato nell'immagine seguente.

Service or use case

Systems Manager ▼

Choose a use case for the specified service.

Use case

- ☒ **Systems Manager**  
Allows SSM to call AWS services on your behalf
- ☐ **Systems Manager - Inventory and Maintenance Windows**  
Allow AWS Systems Manager to call AWS resources on your behalf.

4. Scegli Avanti.
5. Nella pagina Attached permissions policy (Policy delle autorizzazioni collegate), cerca la policy del ruolo da assegnare creato in [Attività 1: Creazione di una politica di assunzione del ruolo per Change Manager](#), ad esempio **MyChangeManagerAssumeRole**.
6. Seleziona la casella di controllo accanto al nome della policy, quindi scegli Next: Tags (Successivo: Tag).
7. Per Nome ruolo, inserisci un nome per il nuovo profilo dell'istanza, ad esempio **MyChangeManagerAssumeRole**.
8. (Facoltativo) Per Role description (Descrizione ruolo), aggiorna la descrizione di questo ruolo dell'istanza.
9. (Facoltativo) Aggiungere una o più coppie tag chiave-valore per organizzare, monitorare o controllare l'accesso per questo ruolo.
10. Scegli Prossimo: Rivedi.
11. (Facoltativo) Per Tags (Tag), aggiungi una o più coppie tag chiave-valore chiave per organizzare, monitorare o controllare l'accesso per questo ruolo, quindi scegli Create role (Crea ruolo). Il sistema ti riporta alla pagina Ruoli.

12. Scegliere Crea ruolo. Il sistema visualizza di nuovo la pagina Roles (Ruoli).
13. Nella pagina Ruoli, scegli il ruolo appena creato per aprire la pagina Riepilogo.

### Attività 3: Allegare la PassRole **policy** iam: ad altri ruoli

Procedi come segue per allegare la policy `iam:PassRole` a un profilo dell'istanza IAM o un ruolo di servizio IAM. (Il servizio Systems Manager utilizza i profili di istanza IAM per comunicare con le istanze EC2. Per i nodi gestiti non EC2 in un ambiente [ibrido e multicloud](#), viene invece utilizzato un ruolo di servizio IAM).

Allegando la policy `iam:PassRole`, il servizio Change Manager può passare le autorizzazioni del ruolo assunto ad altri servizi o ad altri strumenti di Systems Manager durante l'esecuzione di flussi di lavoro dei runbook.

Per allegare il **sono: PassRole** policy relativa a un profilo di istanza IAM o a un ruolo di servizio

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, seleziona Ruoli.
3. Cerca il ruolo assunto Change Manager creato, ad esempio **MyChangeManagerAssumeRole**, e selezionalo.
4. Nella pagina Riepilogo del ruolo assunto, scegli la scheda Autorizzazioni.
5. Scegli Add permissions, Create inline policy (Aggiungi autorizzazioni, Crea policy inline).
6. Nella pagina Create Policy (Crea policy), scegliere la scheda Visual editor (Editor visivo).
7. Scegliere Service (Servizio), quindi IAM.
8. Nella casella di testo Filtra azioni **PassRole**, inserisci, quindi scegli l'PassRole opzione.
9. Espandi Resources (Risorse). Verifica che l'opzione Specific (Specifico) sia selezionata, quindi scegliere Add ARN (Aggiungi ARN).
10. Nel campo Specify ARN for role (Specifica ARN per il ruolo), immetti l'ARN del ruolo del profilo dell'istanza IAM o del ruolo di servizio IAM a cui desideri passare le autorizzazioni del ruolo assunto. Il sistema popola automaticamente i campi Account e Role name with path (Nome ruolo con percorso).
11. Scegliere Add (Aggiungi).
12. Scegliere Review policy (Rivedi policy).
13. Per Name (Nome), inserisci un nome per identificare questa policy, quindi scegli Create policy (Crea policy).

## Ulteriori informazioni

- [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#)
- [Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud](#)

### Attività 4: Aggiungere criteri in linea a un ruolo di assunzione per richiamarne altri Servizi AWS

Quando una richiesta di modifica richiama un altro utente Servizi AWS utilizzando il Change Manager ruolo di assunzione, il ruolo di assunzione deve essere configurato con l'autorizzazione per richiamare tali servizi. Questo requisito si applica a tutti i runbook di AWS Automation (runbook AWS-\*) che potrebbero essere utilizzati in una richiesta di modifica, come, e runbook. AWS-ConfigureS3BucketLogging AWS-CreateDynamoDBBackup AWS-RestartEC2Instance. Questo requisito si applica anche a tutti i runbook personalizzati creati che richiamano altri utenti Servizi AWS utilizzando azioni che richiamano altri servizi. Ad esempio, se utilizzi le operazioni `aws:executeAwsApi`, `aws:CreateStack` o `aws:copyImage`, allora dovrai configurare il ruolo di servizio con l'autorizzazione per richiamare questi servizi. Puoi concedere autorizzazioni ad altri Servizi AWS aggiungendo una policy in linea IAM al ruolo.

Per aggiungere una policy in linea a un ruolo, assumi un ruolo per richiamarne un altro Servizi AWS (console IAM)

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, seleziona Ruoli.
3. Nell'elenco, scegli il nome del ruolo assunto che desideri aggiornare, ad esempio `MyChangeManagerAssumeRole`.
4. Scegli la scheda Autorizzazioni.
5. Scegli Add permissions, Create inline policy (Aggiungi autorizzazioni, Crea policy inline).
6. Scegli la scheda JSON.
7. Inserisci un documento di policy JSON per Servizi AWS quello che desideri richiamare. Di seguito sono riportati due documenti della policy JSON di esempio.

Esempio di **PutObject** e **GetObject** di Amazon S3

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "s3:PutObject",
 "s3:GetObject"
],
 "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
 }
]
}
```

Esempio di **CreateSnapshot** e **DescribeSnapshots** di Amazon EC2

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ec2:CreateSnapshot",
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": "ec2:DescribeSnapshots",
 "Resource": "*"
 }
]
}
```

Per informazioni sul linguaggio della policy IAM consulta [Riferimento alle policy JSON IAM](#) nella Guida per l'utente IAM.

8. Al termine, seleziona Review policy (Rivedi policy). In [Policy Validator](#) (Validatore di policy) vengono segnalati eventuali errori di sintassi.
9. Per Name (Nome), inserisci un nome per identificare la policy che stai creando. Consulta il Riepilogo della policy per visualizzare le autorizzazioni concesse dalla policy. Seleziona Create policy (Crea policy) per salvare il proprio lavoro.
10. Una volta creata, una policy inline viene automaticamente incorporata nel ruolo.

#### Attività 5: Configurazione dell'accesso utente a Change Manager

Se al tuo utente, gruppo o ruolo sono assegnate le autorizzazioni come amministratore, allora hai accesso a Change Manager. Se non disponi delle autorizzazioni di amministratore, un amministratore dovrà assegnare la policy gestita AmazonSSMFullAccess oppure una policy che conceda autorizzazioni analoghe all'utente, al gruppo o al ruolo.

Completa la procedura seguente per configurare un utente per l'utilizzo di Change Manager. L'utente scelto disporrà dell'autorizzazione necessaria per configurare ed eseguire Change Manager.

A seconda dell'applicazione di identità utilizzata nell'organizzazione, è possibile selezionare una delle tre opzioni disponibili per configurare l'accesso degli utenti. Durante la configurazione dell'accesso utente, assegna o aggiungi quanto segue:

1. Assegna la policy AmazonSSMFullAccess o una policy analoga che autorizzi l'accesso a Systems Manager.
2. Assegna la policy `iam:PassRole`.
3. Aggiungi l'ARN per il ruolo di assunzione Change Manager che hai copiato alla fine del [Attività 2: creazione di un ruolo di assunzione per Change Manager](#).

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.

A questo punto, la configurazione dei ruoli richiesti per Change Manager è stata completata. Ora puoi utilizzare l'ARN del ruolo assunto di Change Manager nelle operazioni di Change Manager.

Controllo dell'accesso ai flussi di lavoro del runbook di approvazione automatica

#### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

In ogni modello di modifica creato per l'organizzazione o l'account, è possibile specificare se le richieste di modifica create da tale modello possono essere eseguite come richieste di modifica approvate automaticamente, ovvero vengono eseguite automaticamente senza una fase di revisione (ad eccezione degli eventi di blocco delle modifiche).

Tuttavia, potresti voler impedire a determinati utenti, gruppi o ruoli AWS Identity and Access Management (IAM) di eseguire richieste di modifica approvate automaticamente anche se un modello di modifica lo consente. A tale scopo, è possibile utilizzare la chiave di condizione `ssm:AutoApprove` per l'operazione `StartChangeRequestExecution` in una policy IAM assegnata all'utente, al gruppo o al ruolo IAM.

È possibile aggiungere la policy seguente come policy inline, in cui la condizione è specificata come `false`, per impedire agli utenti di eseguire richieste di modifica approvabili automaticamente.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ssm:StartChangeRequestExecution",
 "Resource": "*",
 "Condition": {
 "BoolIfExists": {
 "ssm:AutoApprove": "false"
 }
 }
 }
]
}
```

Per informazioni su come specificare policy inline, consulta [Policy inline](#) e [Aggiunta e rimozione di autorizzazioni Identità IAM](#) nella Guida per l'utente IAM.

Per ulteriori informazioni su queste chiavi di condizione per le policy di Systems Manager, consulta la sezione [Chiavi di condizione per Systems Manager](#).

## Lavorare con Change Manager

### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

In questo modo Change Manager, gli utenti dell'organizzazione o di un singolo utente Account AWS possono eseguire attività relative alle modifiche per le quali sono state concesse le autorizzazioni necessarie. Change Manager le attività includono quanto segue:

- Creare, rivedere e approvare o rifiutare i modelli di modifica.

Un modello di modifica è una raccolta di impostazioni di configurazione in Change Manager che definiscono le approvazioni obbligatorie, i runbook disponibili e le opzioni di notifica per le richieste di modifica.

- Creare, esaminare e approvare o rifiutare le richieste di modifica.

Una richiesta di modifica è una richiesta di esecuzione Change Manager di un runbook di Automation che aggiorna una o più risorse negli ambienti aziendali AWS o locali. Una richiesta di modifica viene creata utilizzando un modello di modifica.

- Specificare gli utenti dell'organizzazione o dell'account che possono essere resi revisori per i modelli di modifica e le richieste di modifica.
- Modificare le impostazioni di configurazione, ad esempio la gestione delle identità utente in Change Manager e quale delle opzioni best practice vengono applicate nelle operazioni Change Manager. Per ulteriori informazioni sulla configurazione delle impostazioni consulta [Configurazione Change Manager opzioni e best practice](#).

## Argomenti

- [Utilizzo dei modelli di modifica](#)
- [Utilizzo delle richieste di modifica](#)
- [Analisi dei dettagli delle richieste di modifica, dei processi e delle tempistiche \(console\)](#)
- [Visualizzazione dei conteggi aggregati delle richieste di modifica \(riga di comando\)](#)

## Utilizzo dei modelli di modifica

### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la pagina Modifica della disponibilità](#).

Un modello di modifica è una raccolta di impostazioni di configurazione in Change Manager che definiscono le approvazioni obbligatorie, i runbook disponibili e le opzioni di notifica per le richieste di modifica.



 Note

AWS fornisce un esempio di modello di modifica di [Hello World](#) che puoi usare per provare Change Manager, uno strumento in AWS Systems Manager. Tuttavia, è possibile creare modelli di modifica personalizzati per definire le modifiche che si desidera consentire alle risorse dell'organizzazione o dell'account.

Le modifiche apportate quando viene eseguito un flusso di lavoro del runbook si basano sul contenuto di un runbook Automation. In ogni modello di modifica creato è possibile includere uno o più runbook Automation che l'utente che effettua una richiesta di modifica può scegliere per eseguire durante l'aggiornamento. È inoltre possibile creare modelli di modifica che consentono ai richiedenti di scegliere qualsiasi runbook Automation disponibile per la richiesta di modifica.

Per creare un modello di modifica, è possibile utilizzare il Builder nella pagina della console Crea modello per creare un modello di modifica. In alternativa, utilizzando l'opzione Editor, è possibile creare manualmente contenuto JSON o YAML con la configurazione desiderata per il flusso di lavoro del runbook. È inoltre possibile utilizzare uno strumento da riga di comando per creare un modello di modifica, con contenuto JSON per il modello di modifica memorizzato in un file esterno.

## Argomenti

- [Prova il AWS modello di modifica Hello World gestito](#)
- [Creazione di modelli di modifica](#)
- [Revisione e approvazione o rifiuto di modelli di modifica](#)
- [Eliminazione di modelli di modifica](#)

Prova il AWS modello di **modifica** Hello World gestito

 Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

È possibile utilizzare il modello di modifica di esempio `AWS-HelloWorldChangeTemplate`, che utilizza il runbook di esempio di `AutomationAWS-HelloWorld`, per testare il processo di revisione e approvazione al termine della configurazione `Change Manager`. Questo modello è progettato per testare o verificare le autorizzazioni configurate, le assegnazioni degli approvatori e il processo di approvazione. L'approvazione per l'utilizzo di questo modello di modifica nell'organizzazione o nell'account è già stata fornita da AWS. Qualsiasi richiesta di modifica basata su questo modello di modifica, tuttavia, deve essere comunque approvata dai revisori dell'organizzazione o dell'account.

Anziché apportare modifiche a una risorsa, il risultato del flusso di lavoro del runbook associato a questo modello consiste nel stampare un messaggio nell'output di un passaggio di automazione.

Prima di iniziare

Prima di iniziare, assicurati di aver completato le attività seguenti:

- Se lo utilizzi AWS Organizations per gestire le modifiche all'interno di un'organizzazione, completa le attività di configurazione dell'organizzazione descritte in [Configurazione Change Manager per un'organizzazione \(account di gestione\)](#).
- Configura `Change Manager` per l'account amministratore delegato o singolo account, come descritto in [Configurazione Change Manager opzioni e best practice](#).

 Note

Se è stata attivata l'opzione `Best Practice Richiedi monitor` per tutti i modellinelle impostazioni `Change Manager`, disattivarla temporaneamente durante il test del modello di modifica di `Hello World`.

Per provare il AWS modello di modifica `Hello World` gestito

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli `Change Manager`.
3. Scegliere `Creazione della richiesta`.
4. Scegliere il modello di modifica denominato `AWS-HelloWorldChangeTemplate` e quindi `Successivo`.
5. Per `Nome`, immettere un nome per la richiesta di modifica che consenta di identificarne lo scopo, ad esempio **`MyChangeRequestTest`**.

6. Per conoscere il resto dei passaggi per creare la richiesta di modifica, consulta [Creazione di richieste di modifica](#).

## Fasi successive

Per informazioni sull'approvazione delle richieste di modifica, consulta [Revisione e approvazione o rifiuto delle richieste di modifica](#).

Per visualizzare lo stato e i risultati della richiesta di modifica, scegliere il nome della richiesta di modifica nella scheda Richieste in Change Manager.

## Creazione di modelli di modifica

### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la pagina Modifica della disponibilità](#).

Un modello di modifica è una raccolta di impostazioni di configurazione in Change Manager che definiscono le approvazioni obbligatorie, i runbook disponibili e le opzioni di notifica per le richieste di modifica.

È possibile creare modelli di modifica per le operazioni in Change Manager, uno strumento di AWS Systems Manager, utilizzando la console, che include le opzioni Builder ed Editor o strumenti a riga di comando.

## Argomenti

- [Informazioni sulle approvazioni nei modelli di modifica](#)
- [Creazione di modelli di modifica utilizzando Builder](#)
- [Creazione di modelli di modifica mediante Editor](#)
- [Creazione di modelli di modifica utilizzando strumenti da riga di comando](#)

## Informazioni sulle approvazioni nei modelli di modifica

### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

Per ogni modello di modifica creato, puoi specificare fino a cinque livelli di approvazione per le richieste di modifica create da esso. Per ciascuno di questi livelli, puoi designare fino a cinque potenziali approvatori. Un approvatore non è limitato a un singolo utente. È inoltre possibile specificare un gruppo IAM o un ruolo IAM come approvatore individuale. Per i gruppi IAM e i ruoli IAM, uno o più utenti appartenenti al gruppo o al ruolo possono fornire le approvazioni necessarie per ricevere il numero totale di approvazioni necessarie per una richiesta di modifica. È inoltre possibile specificare un numero di approvatori superiore a quello richiesto dal modello di modifica.

Change Manager supporta due approcci principali alle approvazioni: approvazioni per livello e approvazioni per riga. In alcune situazioni è possibile utilizzare anche una combinazione dei due tipi. Ti consigliamo di utilizzare solo le approvazioni per livello nelle operazioni Change Manager.

### Per-level approvals

Consigliato. A partire dal 23 gennaio 2023, Change Manager supporta le approvazioni per livello. In questo modello, per ogni livello di approvazione nel modello di modifica, devi innanzitutto specificare quante approvazioni sono necessarie per quel livello. Quindi specifichi come minimo quel numero di approvatori per il livello e, volendo, altri approvatori. Tuttavia, per approvare la richiesta di modifica è sufficiente il solo numero di approvatori specificato per il livello. Ad esempio, puoi specificare cinque approvatori per un livello ma richiedere tre approvazioni.

Per esempi di visualizzazione da console e JSON di questo tipo di approvazione, consulta la pagina [the section called “Esempio di configurazione di approvazione per livello”](#).

### Per-line approvals

Supporto della compatibilità con le versioni precedenti. La versione originale di Change Manager supportava solo le approvazioni per riga. In questo modello, ogni approvatore specificato per un livello di approvazione è rappresentato come una riga di approvazione. Ogni approvatore

doveva approvare una richiesta di modifica affinché fosse approvata a quel livello. Prima del 23 gennaio 2023, questo era l'unico modello supportato per le approvazioni. I modelli di modifica creati prima di questa data continuano a supportare le approvazioni per riga, ma consigliamo invece di utilizzare le approvazioni per livello.

Per esempi di visualizzazione da console e JSON di questo tipo di approvazione, consulta la pagina [the section called “Esempio di configurazione di approvazione per riga”](#).

### Combined per-line and per-level approvals

Non consigliato. Nella console, la scheda Builder non supporta più l'aggiunta di approvazioni per riga. Tuttavia, in alcuni casi potresti ritrovarti con approvazioni sia per riga sia per livello in uno stesso modello di modifica. Ciò può verificarsi se aggiorni un modello di modifica creato prima del 23 gennaio 2023 o se crei o aggiorni un modello di modifica editando manualmente il contenuto YAML.

Per esempi di visualizzazione da console e JSON di questo tipo di approvazione, consulta la pagina [the section called “Esempio di configurazione di approvazione combinata per livello e per riga”](#).

#### Important

Sebbene sia possibile creare un modello di modifica che combini le approvazioni per riga e per livello, questa configurazione non è consigliata o necessaria. Qualunque tipo di approvazione richieda più approvazioni (approvazioni per riga o per livello) ha la precedenza. Ad esempio:

- Se un modello di modifica specifica tre approvazioni per livello ma cinque approvazioni per riga, sono necessarie cinque approvazioni.
- Se un modello di modifica specifica quattro approvazioni per livello ma due approvazioni per riga, sono necessarie quattro approvazioni.

Puoi creare un livello che includa approvazioni sia per riga sia per livello modificando manualmente il contenuto YAML o JSON. Quindi, la scheda Builder mostra i controlli per specificare il numero richiesto di approvazioni sia per il livello sia per le singole righe. Tuttavia, i nuovi livelli aggiunti utilizzando la console supportano ancora le configurazioni di approvazione soltanto per livello.

## Notifiche e rifiuti delle richieste di modifica

### Notifiche Amazon SNS

Quando viene creata una richiesta di modifica utilizzando il modello di modifica, le notifiche vengono inviate agli abbonati dell'argomento Amazon Simple Notification Service (Amazon SNS) che è stato designato per le notifiche di approvazione a quel livello. È possibile specificare l'argomento della notifica nel modello di modifica o consentire all'utente che crea la richiesta di modifica di specificarne uno.

Dopo avere ricevuto il numero minimo di approvazioni richieste a un livello, le notifiche vengono inviate agli approvatori abbonati all'argomento Amazon SNS per il livello successivo e così via.

#### Important

Assicurati che i ruoli, i gruppi e gli utenti IAM designati insieme forniscano un numero sufficiente di approvatori per soddisfare il numero richiesto di approvazioni specificato. Ad esempio, se si designa un solo gruppo IAM come approvatore contenente tre utenti, non è possibile specificare che a quel livello sono richieste cinque approvazioni, bensì solo tre o meno.

### Rifiuti delle richieste di modifica

Indipendentemente dal numero di livelli di approvazione e approvatori specificati, è necessario un solo rifiuto a una richiesta di modifica per evitare che il flusso di lavoro del runbook relativo a quella richiesta si verifichi.

### Change Manager esempi di tipi di approvazione

#### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

Gli esempi seguenti mostrano la visualizzazione della console e il contenuto JSON per i tre tipi di approvazione in Change Manager.

### Argomenti

- [Esempio di configurazione di approvazione per livello](#)
- [Esempio di configurazione di approvazione per riga](#)
- [Esempio di configurazione di approvazione combinata per livello e per riga](#)

### Esempio di configurazione di approvazione per livello

Nella configurazione del livello di approvazione per livello mostrata nell'immagine seguente, sono richieste tre approvazioni. Tali approvazioni possono provenire da qualsiasi combinazione di utenti, gruppi e ruoli IAM specificati come approvatori. Gli approvatori specificati includono due utenti IAM (John Stiles e Ana Carolina Silva), un gruppo di utenti che contiene tre membri (GroupOfThree) e un ruolo utente che rappresenta dieci utenti (RoleOfTen).

Se tutti e tre gli utenti del gruppo GroupOfThree approvano la richiesta di modifica, questa viene approvata per quel livello. Non è necessario ricevere un'approvazione da ogni utente, gruppo o ruolo. Il numero minimo di approvazioni può provenire da qualsiasi combinazione degli approvatori specificati. Nelle operazioni Change Manager, consigliamo di utilizzare le approvazioni per livello.

### First-level approvals

Remove level

Number of approvals required at this level

3 ▼

| Approver           | Type      |        |
|--------------------|-----------|--------|
| John Stiles        | IAM User  | Remove |
| Ana Carolina Silva | IAM User  | Remove |
| GroupOfThree       | IAM Group | Remove |
| RoleOfTen          | IAM Role  | Remove |

Add approver ▼

L'esempio seguente illustra parte del codice YAML per questa configurazione.

 Note

Questa versione del codice YAML include un input aggiuntivo, `MinRequiredApprovals` (con la M iniziale maiuscola). Il valore di questo input indica quante approvazioni sono necessarie tra tutti i revisori disponibili. Inoltre, nota che il valore di `minRequiredApprovals` (con la m iniziale minuscola) per ogni approvatore nell'elenco `Approvers` è `0` (zero). Ciò indica che l'approvatore può contribuire alle approvazioni complessive ma non è tenuto a farlo.

```
schemaVersion: "0.3"
emergencyChange: false
autoApprovable: false
mainSteps:
 - name: ApproveAction1
 action: aws:approve
 timeoutSeconds: 604800
 inputs:
 Message: Please approve this change request
 MinRequiredApprovals: 3
 EnhancedApprovals:
 Approvers:
 - approver: John Stiles
 type: IamUser
 minRequiredApprovals: 0
 - approver: Ana Carolina Silva
 type: IamUser
 minRequiredApprovals: 0
 - approver: GroupOfThree
 type: IamGroup
 minRequiredApprovals: 0
 - approver: RoleOfTen
 type: IamRole
 minRequiredApprovals: 0
templateInformation: >
 #### What is the purpose of this change?
 //truncated
```



## Esempio di configurazione di approvazione per riga

Nella configurazione del livello di approvazione mostrata nell'immagine seguente, sono specificati quattro approvatori. Questi includono due utenti IAM (John Stiles e Ana Carolina Silva), un gruppo di utenti che contiene tre membri (GroupOfThree) e un ruolo utente che rappresenta dieci utenti (). RoleOfTen Per-line le approvazioni sono supportate per la compatibilità con le versioni precedenti ma non consigliate.

| Approver           | Type      | Required |        |
|--------------------|-----------|----------|--------|
| John Stiles        | IAM User  | 1        | Remove |
| Ana Carolina Silva | IAM User  | 1        | Remove |
| GroupOfThree       | IAM Group | 1        | Remove |
| RoleOfTen          | IAM Role  | 1        | Remove |

Buttons: Add approver ▼, Remove level

Affinché la richiesta di modifica venga approvata in questa configurazione di approvazione per riga, deve essere approvata da tutte le linee di approvazione: John Stiles, Ana Carolina Silva, un membro del gruppo GroupOfThree e un membro del ruolo RoleOfTen.

L'esempio seguente illustra parte del codice YAML per questa configurazione.

### Note

Osserva che il valore per ogni approvatore `minRequiredApprovals` è 1. Ciò indica che è richiesta un'approvazione da parte di ogni approvatore.

```
schemaVersion: "0.3"
emergencyChange: false
autoApprovable: false
mainSteps:
 - name: ApproveAction1
 action: aws:approve
 timeoutSeconds: 10000
 inputs:
```

```
Message: Please approve this change request
EnhancedApprovals:
 Approvers:
 - approver: John Stiles
 type: IamUser
 minRequiredApprovals: 1
 - approver: Ana Carolina Silva
 type: IamUser
 minRequiredApprovals: 1
 - approver: GroupOfThree
 type: IamGroup
 minRequiredApprovals: 1
 - approver: RoleOfTen
 type: IamRole
 minRequiredApprovals: 1
 executableRunBooks:
 - name: AWS-HelloWorld
 version: $DEFAULT
 templateInformation: >
 #### What is the purpose of this change?
 //truncated
```

## Esempio di configurazione di approvazione combinata per livello e per riga

Nella configurazione di approvazione combinata per livello e per riga mostrata nell'immagine seguente, vengono specificate tre approvazioni per il livello, ma quattro approvazioni per le approvazioni per elemento di riga. Qualunque tipo di approvazione richieda più approvazioni ha la precedenza, quindi per questa configurazione sono necessarie quattro approvazioni. L'approvazione combinata per livello e per riga non è consigliata.

## First-level approvals

Remove level

Number of approvals required at this level

3 ▼

Approver

Type

Required

John Stiles

IAM User

1 ▼

Remove

Ana Carolina Silva

IAM User

1 ▼

Remove

GroupOfThree

IAM Group

1 ▼

Remove

RoleOfTen

IAM Role

1 ▼

Remove

Add approver ▼

```

schemaVersion: "0.3"
emergencyChange: false
autoApprovable: false
mainSteps:
 - name: ApproveAction1
 action: aws:approve
 timeoutSeconds: 604800
 inputs:
 Message: Please approve this change request
 MinRequiredApprovals: 3
 EnhancedApprovals:
 Approvers:
 - approver: John Stiles
 type: IamUser
 minRequiredApprovals: 1
 - approver: Ana Carolina Silva
 type: IamUser
 minRequiredApprovals: 1
 - approver: GroupOfThree
 type: IamGroup
 minRequiredApprovals: 1
 - approver: RoleOfTen
 type: IamRole
 minRequiredApprovals: 1
templateInformation: >
 #### What is the purpose of this change?
 //truncated

```

## Argomenti

- [Creazione di modelli di modifica utilizzando Builder](#)
- [Creazione di modelli di modifica mediante Editor](#)
- [Creazione di modelli di modifica utilizzando strumenti da riga di comando](#)

### Creazione di modelli di modifica utilizzando Builder

#### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

Utilizzando Builder for change templates in Change Manager, è possibile configurare il flusso di lavoro del runbook definito nel modello di modifica senza dover utilizzare la sintassi JSON o YAML. Dopo aver specificato le opzioni, il sistema converte l'input nel formato YAML che Systems Manager può utilizzare per eseguire i flussi di lavoro del runbook.

Per creare un modello di modifica utilizzando Builder

1. Apri la console all'indirizzo. AWS Systems Manager <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Change Manager.
3. Scegli Crea modello.
4. Per Nome, immettere un nome per il modello che consenta di identificarne lo scopo, ad esempio **UpdateEC2LinuxAMI**.
5. Nella sezione Change template details (Modifica i dettagli del modello), completa le operazioni descritte di seguito.
  - In Description (Descrizione), fornire una breve spiegazione di come e quando deve essere utilizzato il modello di modifica che si sta creando.

Questa descrizione consente agli utenti che creano richieste di modifica di determinare se utilizzano il modello di modifica corretto. Aiuta coloro che esaminano le richieste di modifica a capire se la richiesta deve essere approvata.

- In **Change template type** (Modifica del tipo di modello), specificare se si sta creando un modello di modifica standard o un modello di modifica di emergenza.

Un modello di modifica di emergenza viene utilizzato per le situazioni in cui è necessario apportare una modifica anche se le modifiche sono altrimenti bloccate da un evento nel calendario in uso da AWS Systems Manager Change Calendar. Le richieste di modifica create da un modello di modifica di emergenza devono essere comunque approvate dai responsabili approvatori designati, ma le modifiche richieste possono comunque essere eseguite anche quando il calendario è bloccato.

- Per **Opzioni runbook**, specificare i runbook tra cui gli utenti possono scegliere durante la creazione di una richiesta di modifica. È possibile aggiungere un singolo runbook o più runbook. In alternativa, è possibile consentire ai richiedenti di specificare il runbook da utilizzare. In uno di questi casi, è possibile includere un solo runbook nella richiesta di modifica.
- In **Runbook**, selezionare i nomi dei runbook e le versioni dei runbook tra cui gli utenti possono scegliere per le proprie richieste di modifica. Indipendentemente dal numero di runbook aggiunti al modello di modifica, è possibile selezionarne solo uno per ogni richiesta di modifica.

Non viene specificato un runbook se è stato scelto. È possibile utilizzare qualsiasi runbook in precedenza.

 **Tip**

Selezionare una versione di runbook e un runbook, quindi scegliere **Visualizzazione** per esaminare il contenuto del runbook nell'interfaccia **Documenti** di Systems Manager.

6. Nelle **Informazioni sul modello**, utilizzare **Markdown** per immettere informazioni per gli utenti che creano richieste di modifica da questo modello di modifica. Abbiamo fornito una serie di domande che puoi includere per gli utenti che creano richieste di modifica oppure puoi aggiungere altre informazioni e domande.

 **Note**

Markdown è un linguaggio di markup che consente di aggiungere descrizioni in stile wiki ai documenti e ai singoli passaggi all'interno del documento. Per ulteriori informazioni sull'utilizzo di Markdown, consulta [Utilizzo di Markdown in AWS](#).

Consigliamo di fornire agli utenti domande a cui rispondere sulle loro richieste di modifica per aiutare gli approvatori a decidere se concedere ciascuna richiesta di modifica, ad esempio elencando tutti i passaggi manuali necessari da eseguire come parte della modifica e un piano di rollback.

 **Tip**

Passa da Hide preview (Nascondi anteprima) a Show preview (Mostra anteprima) e viceversa per vedere come appare il contenuto della descrizione durante la composizione.

7. Nella sezione Requests (Richieste), procedere come segue:

- (Facoltativo) Se si desidera consentire l'esecuzione automatica delle richieste di modifica create da questo modello di modifica, senza revisione da parte di alcun approvatore (ad eccezione degli eventi di blocco delle modifiche), selezionare Abilitazione dell'approvazione automatica.

 **Note**

L'abilitazione delle approvazioni automatiche in un modello di modifica consente agli utenti di utilizzare l'opzione di bypassare i revisori. Possono comunque scegliere di specificare i revisori durante la creazione di una richiesta di modifica. Pertanto, è comunque necessario specificare le opzioni del revisore nel modello di modifica.

 **Important**

Se si abilita l'approvazione automatica per un modello di modifica, gli utenti possono inviare richieste di modifica utilizzando tale modello che non richiedono la revisione da parte dei revisori prima dell'esecuzione (ad eccezione degli approvatori degli eventi di blocco delle modifiche). Se si desidera limitare a un particolare utente, gruppo o ruolo IAM l'invio di richieste di approvazione automatica, è possibile utilizzare una condizione in una policy IAM a tale scopo. Per ulteriori informazioni, consulta [Controllo dell'accesso ai flussi di lavoro del runbook di approvazione automatica](#).

- In Numero di approvazioni richieste a questo livello, scegli il numero di approvazioni che le richieste di modifica create da questo modello di modifica devono ricevere per questo livello.
- Per aggiungere approvatori di primo livello obbligatori, scegliere Aggiungi approvatore e scegliere tra le seguenti opzioni:
  - Approvatori specificati del modello: scegliere uno o più utenti, gruppi o ruoli AWS Identity and Access Management (IAM) dall'account per approvare le richieste di modifica create da questo modello di modifica. Tutte le richieste di modifica create utilizzando questo modello devono essere esaminate e approvate da ciascun approvatore specificato.
  - Richiedi approvatori specificati: l'utente che effettua la richiesta di modifica specifica i revisori e può scegliere da un elenco di utenti nell'account.

Il numero immesso nella colonna Campo obbligatorio determina il numero di revisori che devono essere specificati da una richiesta di modifica che utilizza questo modello di modifica.

 Important

Prima del 23 gennaio 2023, la scheda Builder supportava solo la specifica delle approvazioni per riga. I nuovi modelli di modifica e i nuovi livelli che aggiungi ai modelli di modifica esistenti utilizzando la scheda Builder supportano solo le approvazioni per livello. Ti consigliamo di utilizzare solo le approvazioni per livello nelle operazioni Change Manager.

Per ulteriori informazioni, consulta [Informazioni sulle approvazioni nei modelli di modifica](#).

- Per Argomento SNS da notificare agli approvatori eseguire quanto segue:
  1. Scegli una delle seguenti opzioni per specificare l'argomento Amazon Simple Notification Service (Amazon SNS) nel tuo account da utilizzare per inviare notifiche agli approvatori che una richiesta di modifica è pronta per la loro revisione:
    - Inserisci un SNS Amazon Resource Name (ARN) – Per argomento ARN immetti l'ARN di un argomento Amazon SNS esistente. Questo argomento può essere incluso in qualsiasi account dell'organizzazione.
    - Selezionare un argomento SNS esistente— Per Argomento notifica destinazione, seleziona l'ARN di un argomento Amazon SNS esistente nel tuo Account AWS. (Questa opzione non è disponibile se non hai ancora creato alcun argomento di Amazon SNS nel tuo indirizzo attuale). Account AWS Regione AWS

- Specificare l'argomento SNS quando viene creata la richiesta di modifica: l'utente che crea una richiesta di modifica può specificare l'argomento Amazon SNS da utilizzare per le notifiche.

 Note

L'argomento Amazon SNS selezionato deve essere configurato in modo da specificare le notifiche inviate e gli abbonati a cui vengono inviati. La sua policy di accesso deve inoltre concedere autorizzazioni a Systems Manager in modo che Change Manager può inviare notifiche. Per informazioni, consulta [Configurazione degli argomenti di Amazon SNS per Change Manager notifiche](#).

2. Scegliere Add notification (Aggiungi notifica).

8. (Facoltativo) Per aggiungere un livello aggiuntivo di approvatori, scegliere Aggiungi livello di approvazione e scegliere tra approvatori specificati nel modello e approvatori specificati dalla richiesta per questo livello. Scegliere quindi un argomento SNS per notificare questo livello di approvatori.

Dopo che tutte le approvazioni sono state ricevute dagli approvatori di primo livello, gli approvatori di secondo livello vengono notificati e così via.

È possibile aggiungere un massimo di cinque livelli di approvatori in ciascun modello. È possibile, ad esempio, richiedere l'approvazione da parte degli utenti in ruoli tecnici per il primo livello, quindi l'approvazione manageriale per il secondo livello.

9. Nella sezione Monitoraggio, per monitorare l'CloudWatch allarme, inserisci il nome di un CloudWatch allarme Amazon nell'account corrente per monitorare l'avanzamento dei flussi di lavoro di Runbook basati su questo modello.

 Tip

Per creare un nuovo allarme o per rivedere le impostazioni di un avviso che desideri specificare, scegli Apri la console Amazon CloudWatch. Per informazioni sull'utilizzo degli CloudWatch allarmi, consulta [Using CloudWatch Alarms](#) nella Amazon CloudWatch User Guide.

10. Nella sezione Notifications (Notifiche) effettua le seguenti operazioni:



1. Scegli una delle seguenti opzioni per specificare l'argomento Amazon SNS nel tuo account da utilizzare per l'invio di notifiche sulle richieste di modifica create utilizzando questo modello di modifica:

- Inserisci un SNS Amazon Resource Name (ARN) – Per argomento ARN immetti l'ARN di un argomento Amazon SNS esistente. Questo argomento può essere incluso in qualsiasi account dell'organizzazione.
- Selezionare un argomento SNS esistente— Per Argomento notifica destinazione, seleziona l'ARN di un argomento Amazon SNS esistente nel tuo Account AWS. (Questa opzione non è disponibile se non hai ancora creato alcun argomento di Amazon SNS nel tuo indirizzo attuale Account AWS ). Regione AWS

 Note

L'argomento Amazon SNS selezionato deve essere configurato in modo da specificare le notifiche inviate e gli abbonati a cui vengono inviati. La sua policy di accesso deve inoltre concedere autorizzazioni a Systems Manager in modo che Change Manager può inviare notifiche. Per informazioni, consulta [Configurazione degli argomenti di Amazon SNS per Change Manager notifiche](#).

2. Scegliere Add notification (Aggiungi notifica).

11. (Facoltativo) Nella sezione Tag, applica una o più name/value coppie di chiavi tag al modello di modifica.

I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Ad esempio, è possibile applicare un tag a un modello di modifica per identificare il tipo di modifica apportato e l'ambiente in cui viene eseguita. In questo caso, puoi specificare le seguenti name/value coppie di chiavi:

- Key=TaskType, Value=InstanceRepair
- Key=Environment, Value=Production

12. Scegliere Salva e anteprima.

13. Rivedere i dettagli del modello di modifica che si sta creando.

Se si desidera apportare modifiche al modello di modifica prima di inviarlo per la revisione, scegliere Operazioni, Modifica.

Se il contenuto del modello di modifica è quello desiderato, selezionare **Invia** per una revisione. Gli utenti dell'organizzazione o dell'account che sono stati specificati come revisori modello nella scheda **Impostazioni** in **Change Manager** ricevono una notifica che li informa che un nuovo modello di modifica è in attesa della revisione.

Se è stato specificato un argomento Amazon SNS per i modelli di modifica, le notifiche vengono inviate quando il modello di modifica viene rifiutato o approvato. Se non ricevi notifiche relative a questo modello di modifica, puoi tornare a **Change Manager** più tardi al fine di verificare il suo stato.

## Creazione di modelli di modifica mediante Editor

### **Change Manager modifica della disponibilità**

AWS Systems Manager **Change Manager** non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo **Change Manager**, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager \*\*Change Manager\*\* la modifica della disponibilità](#).

Utilizza i passaggi descritti in questo argomento per configurare un modello di modifica **Change Manager** inserendo JSON o YAML invece di utilizzare i controlli della console.

Per creare un modello di modifica utilizzando Editor

1. Nel pannello di navigazione, scegli **Change Manager**.
2. Scegli **Crea modello**.
3. In **Nome**, immettere un nome per il modello che consenta di identificarne lo scopo, ad esempio **RestartEC2LinuxInstance**.
4. Sopra **Modifica del modello di modifica**, scegliere **Editor**.
5. In **Editor documenti**, scegliere **Modifica**, quindi immettere il contenuto JSON o YAML per il modello di modifica.

Di seguito è riportato un esempio di :

 Note

Il parametro `minRequiredApprovals` viene utilizzato per specificare il numero di revisori a un livello specificato che devono approvare una richiesta di modifica creata utilizzando questo modello.

In questo esempio vengono illustrati due livelli di approvazione. È possibile specificare fino a cinque livelli di approvazione, ma è necessario un solo livello.

Nel primo livello, l'utente specifico "John-Doe" deve approvare ogni richiesta di modifica.

Dopodiché, tre membri del ruolo IAM Admin devono approvare la richiesta di modifica.

Per ulteriori informazioni sulle approvazioni nei modelli di modifica, consulta la pagina

[Informazioni sulle approvazioni nei modelli di modifica](#).

## YAML

```
description: >-
 This change template demonstrates the feature set available for creating
 change templates for Change Manager. This template starts a Runbook workflow
 for the Automation runbook called AWS-HelloWorld.
templateInformation: >
 ### Document Name: HelloWorldChangeTemplate

 ## What does this document do?

 This change template demonstrates the feature set available for creating
 change templates for Change Manager. This template starts a Runbook workflow
 for the Automation runbook called AWS-HelloWorld.

 ## Input Parameters

 * ApproverSnsTopicArn: (Required) Amazon Simple Notification Service ARN for
 approvers.

 * Approver: (Required) The name of the approver to send this request to.

 * ApproverType: (Required) The type of reviewer.
 * Allowed Values: IamUser, IamGroup, IamRole, SS0Group, SS0User

 ## Output Parameters
```

```
This document has no outputs
schemaVersion: '0.3'
parameters:
 ApproverSnsTopicArn:
 type: String
 description: Amazon Simple Notification Service ARN for approvers.
 Approver:
 type: String
 description: IAM approver
 ApproverType:
 type: String
 description: >-
 Approver types for the request. Allowed values include IamUser, IamGroup,
 IamRole, SSOGroup, and SSUser.
executableRunBooks:
 - name: AWS-HelloWorld
 version: '1'
emergencyChange: false
autoApprovable: false
mainSteps:
 - name: ApproveAction1
 action: 'aws:approve'
 timeoutSeconds: 3600
 inputs:
 Message: >-
 A sample change request has been submitted for your review in Change
 Manager. You can approve or reject this request.
 EnhancedApprovals:
 NotificationArn: '{{ ApproverSnsTopicArn }}'
 Approvers:
 - approver: John-Doe
 type: IamUser
 minRequiredApprovals: 1
 - name: ApproveAction2
 action: 'aws:approve'
 timeoutSeconds: 3600
 inputs:
 Message: >-
 A sample change request has been submitted for your review in Change
 Manager. You can approve or reject this request.
 EnhancedApprovals:
 NotificationArn: '{{ ApproverSnsTopicArn }}'
 Approvers:
 - approver: Admin
```

```
type: IamRole
minRequiredApprovals: 3
```

## JSON

```
{
 "description": "This change template demonstrates the feature set available
for creating
change templates for Change Manager. This template starts a Runbook workflow
for the Automation runbook called AWS-HelloWorld",
 "templateInformation": "### Document Name: HelloWorldChangeTemplate\n\n
 ## What does this document do?\n
 This change template demonstrates the feature set available for creating
change templates for Change Manager.
 This template starts a Runbook workflow for the Automation runbook called
AWS-HelloWorld.\n\n
 ## Input Parameters\n* ApproverSnsTopicArn: (Required) Amazon Simple
Notification Service ARN for approvers.\n
 * Approver: (Required) The name of the approver to send this request to.\n
 * ApproverType: (Required) The type of reviewer. * Allowed Values: IamUser,
IamGroup, IamRole, SSOGroup, SSOUser\n\n
 ## Output Parameters\nThis document has no outputs\n",
 "schemaVersion": "0.3",
 "parameters": {
 "ApproverSnsTopicArn": {
 "type": "String",
 "description": "Amazon Simple Notification Service ARN for approvers."
 },
 "Approver": {
 "type": "String",
 "description": "IAM approver"
 },
 "ApproverType": {
 "type": "String",
 "description": "Approver types for the request. Allowed values include
IamUser, IamGroup, IamRole, SSOGroup, and SSOUser."
 }
 },
 "executableRunBooks": [
 {
 "name": "AWS-HelloWorld",
 "version": "1"
 }
]
}
```

```

],
 "emergencyChange": false,
 "autoApprovable": false,
 "mainSteps": [
 {
 "name": "ApproveAction1",
 "action": "aws:approve",
 "timeoutSeconds": 3600,
 "inputs": {
 "Message": "A sample change request has been submitted for your
review in Change Manager. You can approve or reject this request.",
 "EnhancedApprovals": {
 "NotificationArn": "{{ ApproverSnsTopicArn }}",
 "Approvers": [
 {
 "approver": "John-Doe",
 "type": "IamUser",
 "minRequiredApprovals": 1
 }
]
 }
 }
 },
 {
 "name": "ApproveAction2",
 "action": "aws:approve",
 "timeoutSeconds": 3600,
 "inputs": {
 "Message": "A sample change request has been submitted for your
review in Change Manager. You can approve or reject this request.",
 "EnhancedApprovals": {
 "NotificationArn": "{{ ApproverSnsTopicArn }}",
 "Approvers": [
 {
 "approver": "Admin",
 "type": "IamRole",
 "minRequiredApprovals": 3
 }
]
 }
 }
 }
]
 }
}

```

```
}
```

6. Scegliere Salva e anteprima.
7. Rivedere i dettagli del modello di modifica che si sta creando.

Se si desidera apportare modifiche al modello di modifica prima di inviarlo per la revisione, scegliere Operazioni, Modifica.

Se il contenuto del modello di modifica è quello desiderato, selezionare Invia per una revisione. Gli utenti dell'organizzazione o dell'account che sono stati specificati come revisori modello nella scheda Impostazioni in Change Manager ricevono una notifica che li informa che un nuovo modello di modifica è in attesa della revisione.

Se è stato specificato un argomento Amazon Simple Notification Service (Amazon SNS), le notifiche vengono inviate quando il modello di modifica viene rifiutato o approvato. Se non ricevi notifiche relative a questo modello di modifica, puoi tornare a Change Manager più tardi per verificare il suo stato.

## Creazione di modelli di modifica utilizzando strumenti da riga di comando

### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

Le procedure seguenti descrivono come utilizzare AWS Command Line Interface (AWS CLI) (su Linux, macOS, o Windows Server) o AWS Tools for Windows PowerShell creare una richiesta di modifica in Change Manager.

Per creare un modello di modifica

1. Installa e configura AWS CLI o AWS Strumenti per PowerShell, se non l'hai già fatto.

Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

2. Sul proprio computer locale creare un file JSON denominato ad esempio `MyChangeTemplate.json`, quindi incollare il contenuto del modello di modifica.

#### Note

I modelli di modifica utilizzano una versione dello schema 0.3 che non include lo stesso supporto dei runbook Automation.

Di seguito è riportato un esempio di :

#### Note

Il parametro `minRequiredApprovals` viene utilizzato per specificare il numero di revisori a un livello specificato che devono approvare una richiesta di modifica creata utilizzando questo modello.

In questo esempio vengono illustrati due livelli di approvazione. È possibile specificare fino a cinque livelli di approvazione, ma è necessario un solo livello.

Nel primo livello, l'utente specifico "John-Doe" deve approvare ogni richiesta di modifica. Dopodiché, tre membri del ruolo IAM Admin devono approvare la richiesta di modifica. Per ulteriori informazioni sulle approvazioni nei modelli di modifica, consulta la pagina [Informazioni sulle approvazioni nei modelli di modifica](#).

```
{
 "description": "This change template demonstrates the feature set available for
creating
change templates for Change Manager. This template starts a Runbook workflow
for the Automation runbook called AWS-HelloWorld",
 "templateInformation": "### Document Name: HelloWorldChangeTemplate\n\n
 ## What does this document do?\n
 This change template demonstrates the feature set available for creating change
templates for Change Manager.
 This template starts a Runbook workflow for the Automation runbook called AWS-
HelloWorld.\n\n
 ## Input Parameters\n* ApproverSnsTopicArn: (Required) Amazon Simple
Notification Service ARN for approvers.\n
 * Approver: (Required) The name of the approver to send this request to.\n
}
```



```

 * ApproverType: (Required) The type of reviewer. * Allowed Values: IamUser,
 IamGroup, IamRole, SSOGroup, SSOUser\n\n
 ## Output Parameters\nThis document has no outputs\n",
 "schemaVersion": "0.3",
 "parameters": {
 "ApproverSnsTopicArn": {
 "type": "String",
 "description": "Amazon Simple Notification Service ARN for approvers."
 },
 "Approver": {
 "type": "String",
 "description": "IAM approver"
 },
 "ApproverType": {
 "type": "String",
 "description": "Approver types for the request. Allowed values include
IamUser, IamGroup, IamRole, SSOGroup, and SSOUser."
 }
 },
 "executableRunBooks": [
 {
 "name": "AWS-HelloWorld",
 "version": "1"
 }
],
 "emergencyChange": false,
 "autoApprovable": false,
 "mainSteps": [
 {
 "name": "ApproveAction1",
 "action": "aws:approve",
 "timeoutSeconds": 3600,
 "inputs": {
 "Message": "A sample change request has been submitted for your review
in Change Manager. You can approve or reject this request.",
 "EnhancedApprovals": {
 "NotificationArn": "{{ ApproverSnsTopicArn }}",
 "Approvers": [
 {
 "approver": "John-Doe",
 "type": "IamUser",
 "minRequiredApprovals": 1
 }
]
 }
 }
 }
]

```

```

 }
 },
 {
 "name": "ApproveAction2",
 "action": "aws:approve",
 "timeoutSeconds": 3600,
 "inputs": {
 "Message": "A sample change request has been submitted for your review
in Change Manager. You can approve or reject this request.",
 "EnhancedApprovals": {
 "NotificationArn": "{{ ApproverSnsTopicArn }}",
 "Approvers": [
 {
 "approver": "Admin",
 "type": "IamRole",
 "minRequiredApprovals": 3
 }
]
 }
 }
 }
]
}

```

3. Esegui il comando seguente per creare il modello di modifica.

#### Linux & macOS

```

aws ssm create-document \
 --name MyChangeTemplate \
 --document-format JSON \
 --document-type Automation.ChangeTemplate \
 --content file://MyChangeTemplate.json \
 --tags Key=tag-key,Value=tag-value

```

#### Windows

```

aws ssm create-document ^
 --name MyChangeTemplate ^
 --document-format JSON ^
 --document-type Automation.ChangeTemplate ^
 --content file://MyChangeTemplate.json ^

```

```
--tags Key=tag-key,Value=tag-value
```

## PowerShell

```
$json = Get-Content -Path "C:\path\to\file\MyChangeTemplate.json" | Out-String
New-SSMDocument `
 -Content $json `
 -Name "MyChangeTemplate" `
 -DocumentType "Automation.ChangeTemplate" `
 -Tags "Key=tag-key,Value=tag-value"
```

Per informazioni sulle altre opzioni che è possibile specificare, consulta [create-document](#).

Il sistema restituisce informazioni simili alle seguenti.

```
{
 "DocumentDescription":{
 "CreateDate":1.585061751738E9,
 "DefaultVersion":"1",
 "Description":"Use this template to update an EC2 Linux AMI. Requires one
request.",
 "DocumentFormat":"JSON",
 "DocumentType":"Automation",
 "DocumentVersion":"1",
 "Hash":"0d3d879b3ca072e03c12638d0255ebd004d2c65bd318f8354fcde820dEXAMPLE",
 "HashType":"Sha256",
 "LatestVersion":"1",
 "Name":"MyChangeTemplate",
 "Owner":"123456789012",
 "Parameters":[
 {
 "DefaultValue": "",
 "Description": "Level one approvers",
 "Name": "LevelOneApprovers",
 "Type": "String"
 },
 {
 "DefaultValue": "",
 "Description": "Level one approver type",
 "Name": "LevelOneApproverType",
 "Type": "String"
 }
]
 }
}
```

```
 },
 "cloudWatchMonitors": {
 "monitors": [
 "my-cloudwatch-alarm"
]
 },
 "PlatformTypes": [
 "Windows",
 "Linux"
],
 "SchemaVersion": "0.3",
 "Status": "Creating",
 "Tags": [
]
 }
}
```

Gli utenti dell'organizzazione o dell'account che sono stati specificati come revisori modello nella scheda Impostazioni Scheda in Change Manager vengono notificati che un nuovo modello di modifica è in attesa della revisione.

Se è stato specificato un argomento Amazon Simple Notification Service (Amazon SNS), le notifiche vengono inviate quando il modello di modifica viene rifiutato o approvato. Se non ricevi notifiche relative a questo modello di modifica, puoi tornare a Change Manager più tardi per verificare il suo stato.

Revisione e approvazione o rifiuto di modelli di modifica

#### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

Se sei indicato come revisore per i modelli di modifica in Change Manager, come tool in AWS Systems Manager, riceverai una notifica quando un nuovo modello di modifica o una nuova versione

di un modello di modifica è in attesa di revisione. Le notifiche vengono inviate da un argomento Amazon Simple Notification Service (Amazon SNS).

#### Note

Questa funzionalità dipende dal fatto che il tuo account sia stato configurato per utilizzare un argomento Amazon SNS per inviare notifiche di revisione del modello di modifica. Per informazioni sulla specifica di un argomento di notifica del revisore modello, consulta [Attività 1: Configurazione Change Manager gestione delle identità degli utenti e revisori dei modelli](#).

Per rivedere il modello di modifica, segui il link nella notifica, accedi e segui i passaggi di questa procedura. Console di gestione AWS

Per rivedere e approvare o rifiutare un modello di modifica

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Change Manager.
3. Nella sezione Modelli di modifica in fondo alla scheda Panoramica, scegliere il numero in Revisione in sospeso.
4. Nell'elenco Modelli di modifica, individuare e scegliere il nome del modello di modifica da rivedere.
5. Nella pagina di riepilogo esaminare il contenuto proposto del modello di modifica ed effettuare una delle seguenti operazioni:
  - Per approvare il modello di modifica, che consente di utilizzarlo nelle richieste di modifica, scegli Approve (Approva).
  - Per rifiutare il modello di modifica, che ne impedisce l'utilizzo nelle richieste di modifica, selezionare Reject (Rifiuta).

Eliminazione di modelli di modifica

#### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti

esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems ManagerChange Manager la modifica della disponibilità](#).

Questo argomento descrive come eliminare i modelli creati inChange Manager. Se stai usando Change Manager per un'organizzazione, questa procedura verrà eseguita nell'account amministratore delegato.

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Change Manager.
3. Scegliere la scheda Templates (Modelli).
4. Scegli il nome del modello da eliminare.
5. Scegli Actions, Delete template (Operazioni, Elimina modello).
6. Nella finestra di dialogo di conferma inserisci la parola **DELETE** e quindi scegli Elimina.

Utilizzo delle richieste di modifica

#### Change Manager modifica della disponibilità

AWS Systems ManagerChange Managernon sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarloChange Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems ManagerChange Manager la modifica della disponibilità](#).

Una richiesta di modifica è una richiesta di esecuzione Change Manager di un runbook di Automation che aggiorna una o più risorse negli ambienti aziendali AWS o locali. Una richiesta di modifica viene creata utilizzando un modello di modifica.

Quando si crea una richiesta di modifica inChange Manager, uno o più approvatori dell'organizzazione o dell'account devono esaminare e approvare la richiesta. Senza le approvazioni richieste, il flusso di lavoro del runbook, che apporta le modifiche richieste, non può essere eseguito.

Argomenti

- [Creazione di richieste di modifica](#)

- [Revisione e approvazione o rifiuto delle richieste di modifica](#)

## Creazione di richieste di modifica

### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

Quando si crea una richiesta di modifica in Change Manager, il modello di modifica selezionato in genere esegue le seguenti operazioni:

- Designa gli approvatori per la richiesta di modifica o specifica il numero di approvazioni necessarie
- Specifica l'argomento Amazon Simple Notification Service (Amazon SNS) da utilizzare per notificare agli approvatori la richiesta di modifica
- Specifica un CloudWatch allarme Amazon per monitorare il flusso di lavoro del runbook per la richiesta di modifica
- Identificare i runbook Automation tra cui è possibile scegliere per apportare la modifica richiesta

In alcuni casi, è possibile configurare un modello di modifica in modo da specificare il runbook Automation da utilizzare e specificare chi deve esaminare e approvare la richiesta.

### Important

Se utilizzi Change Manager in un'organizzazione, si consiglia di apportare sempre modifiche dall'account amministratore delegato. Sebbene sia possibile apportare modifiche da altri account dell'organizzazione, tali modifiche non verranno segnalate o visualizzate dall'account amministratore delegato.

## Argomenti

- [Informazioni sulle approvazioni delle richieste di modifica](#)
- [Creazione di richieste di modifica \(console\)](#)

- [Creazione di richieste di modifica \(AWS CLI\)](#)

## Informazioni sulle approvazioni delle richieste di modifica

A seconda dei requisiti specificati in un modello di modifica, le richieste di modifica create da esso possono richiedere l'approvazione di un massimo di cinque livelli prima che possa verificarsi il flusso di lavoro del runbook per la richiesta. Per ognuno di questi livelli, il creatore del modello può specificare fino a cinque potenziali approvatori. Un approvatore non è limitato a un singolo utente. Un approvatore in questo senso può anche essere un gruppo IAM o un ruolo IAM. Per i gruppi IAM e i ruoli IAM, uno o più utenti appartenenti al gruppo o al ruolo possono fornire le approvazioni necessarie per ricevere il numero totale di approvazioni necessarie per una richiesta di modifica. I creatori di modelli possono anche specificare più approvatori di quelli richiesti dal modello di modifica.

## Flussi di lavoro di approvazione originali e approvazioni aggiornate and/or

Se si utilizzano i modelli di modifica creati prima del 23 gennaio 2023, è necessario ricevere un'approvazione da ogni approvatore specificato affinché la richiesta di modifica venga approvata a quel livello. Ad esempio, nell'impostazione del livello di approvazione mostrata nell'immagine seguente, vengono specificati quattro approvatori. Gli approvatori specificati includono due utenti (John Stiles e Ana Carolina Silva), un gruppo di utenti che contiene tre membri (GroupOfThree) e un ruolo utente che rappresenta dieci utenti (). RoleOfTen

First-level approvals

Remove level

| Approver           | Type      | Required |        |
|--------------------|-----------|----------|--------|
| John Stiles        | IAM User  | 1        | Remove |
| Ana Carolina Silva | IAM User  | 1        | Remove |
| GroupOfThree       | IAM Group | 1        | Remove |
| RoleOfTen          | IAM Role  | 1        | Remove |

Add approver ▼

Affinché la richiesta di modifica venga approvata a questo livello, deve essere approvata da John Stiles, Ana Carolina Silva, un membro del gruppo GroupOfThree e un membro del ruolo RoleOfTen.

Se si utilizzano i modelli di modifica creati a partire dal 23 gennaio 2023, i creatori di modelli possono specificare un numero totale complessivo di approvazioni richieste per ciascun livello di



approvazione. Tali approvazioni possono provenire da qualsiasi combinazione di utenti, gruppi e ruoli specificati come approvatori. Un modello di modifica può richiedere una singola approvazione per un livello ma specificare, ad esempio, due singoli utenti, due gruppi e un ruolo come potenziali approvatori.

Ad esempio, nell'area del livello di approvazione mostrata nell'immagine seguente, sono necessarie tre approvazioni. Gli approvatori specificati nel modello includono due utenti (John Stiles e Ana Carolina Silva), un gruppo di utenti che contiene tre membri (GroupOfThree) e un ruolo utente che rappresenta dieci utenti (RoleOfTen).

**First-level approvals** Remove level

Number of approvals required at this level

3 ▼

| Approver           | Type      |                     |
|--------------------|-----------|---------------------|
| John Stiles        | IAM User  | <span>Remove</span> |
| Ana Carolina Silva | IAM User  | <span>Remove</span> |
| GroupOfThree       | IAM Group | <span>Remove</span> |
| RoleOfTen          | IAM Role  | <span>Remove</span> |

Add approver ▼

Se tutti e tre gli utenti del gruppo GroupOfThree approvano la richiesta di modifica, questa viene approvata per quel livello. Non è necessario ricevere un'approvazione da ogni utente, gruppo o ruolo. Il numero minimo di approvazioni può provenire da qualsiasi combinazione di potenziali approvatori.

Quando viene creata la richiesta di modifica, le notifiche vengono inviate agli abbonati dell'argomento Amazon SNS specificato per le notifiche di approvazione a quel livello. L'autore del modello di modifica potrebbe aver specificato l'argomento di notifica da utilizzare o aver consentito all'utente di specificarne uno.

Dopo aver ricevuto il numero minimo di approvazioni richieste a un livello, le notifiche vengono inviate agli approvatori abbonati all'argomento Amazon SNS per il livello successivo e così via.

Indipendentemente dal numero di livelli di approvazione e approvatori specificati, è necessario un solo rifiuto a una richiesta di modifica per evitare che il flusso di lavoro del runbook relativo a quella richiesta si verifichi.

### Creazione di richieste di modifica (console)

Nella procedura seguente viene descritto come annullare la registrazione di un computer ibrido utilizzando la console Systems Manager.

Per creare una richiesta di modifica (console)

1. Apri la console all'indirizzo. AWS Systems Manager <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Change Manager.
3. Scegliere Creazione della richiesta.
4. Cercare e selezionare un modello di modifica che si desidera utilizzare per questa richiesta di modifica.
5. Scegli Avanti.
6. Per Nome, immettere un nome per la richiesta di modifica che consenta di identificarne lo scopo, ad esempio **UpdateEC2LinuxAMI-us-east-2**.
7. Per Runbook, selezionare il runbook che si desidera utilizzare per apportare le modifiche richieste.

#### Note

Se l'opzione per selezionare un runbook non è disponibile, l'autore del modello di modifica ha specificato quale runbook deve essere utilizzato.

8. Per Informazioni sulla richiesta di modifica, utilizzare Markdown al fine di fornire ulteriori informazioni sulla richiesta di modifica per aiutare i revisori a decidere se approvare o rifiutare la richiesta di modifica. L'autore del modello che stai utilizzando potrebbe aver fornito istruzioni o domande a cui rispondere.

 Note

Markdown è un linguaggio di markup che consente di aggiungere descrizioni in stile wiki ai documenti e ai singoli passaggi all'interno del documento. Per ulteriori informazioni sull'utilizzo di Markdown, consulta [Utilizzo di Markdown in AWS](#).

9. Nell'Ora di inizio workflow scegliere una delle seguenti opzioni:

- Eseguire l'operazione a un'ora pianificata— Per Orario di inizio richiesto, immettere la data e l'ora proposte per l'esecuzione del flusso di lavoro del runbook per questa richiesta. Per Ora di fine stimata immettere la data e l'ora in cui si prevede di completare il flusso di lavoro del runbook. (Questa volta è una stima che stai fornendo solo ai revisori.)

 Tip

Scegli Visualizza calendario delle modifiche per verificare eventuali eventi di blocco per il periodo specificato.

- Eseguire l'operazione il prima possibile dopo l'approvazione: se la richiesta di modifica viene approvata, il flusso di lavoro del runbook viene eseguito non appena è presente un periodo non limitato in cui è possibile apportare modifiche.

10. Nella sezione Requests (Richieste), procedere come segue:

1. Se si visualizzano opzioni per il tipo di approvazione, scegliere una delle seguenti opzioni:

- Approvazione automatica: il modello di modifica selezionato è configurato per consentire l'esecuzione automatica delle richieste di modifica senza revisione da parte di alcun approvatore. Continua alla fase 11.

 Note

Le autorizzazioni specificate nelle politiche IAM che regolano l'uso di Systems Manager non devono impedirti di inviare richieste di modifica con approvazione automatica affinché vengano eseguite automaticamente.

- Specificare gli approvatori: è necessario aggiungere uno o più utenti, gruppi o ruoli IAM per esaminare e approvare questa richiesta di modifica.

 Note

È possibile scegliere di specificare i revisori anche se le autorizzazioni specificate nei criteri IAM che regolano l'utilizzo di Systems Manager consentono di eseguire richieste di modifica dell'approvazione automatica.

2. Scegli **Aggiungi approvatore**, quindi seleziona uno o più utenti, gruppi o ruoli AWS Identity and Access Management (IAM) dagli elenchi dei revisori disponibili.

 Note

È possibile che siano già stati specificati uno o più approvatori. Ciò significa che gli approvatori obbligatori sono già specificati nel modello di modifica selezionato. Non è possibile rimuovere questi approvatori dalla richiesta. Se il pulsante **Aggiungi approvatore** non è disponibile, il modello scelto non consente l'aggiunta di revisori aggiuntivi alle richieste.

Per informazioni sull'approvazione delle richieste di modifica, consulta la pagina [Informazioni sulle approvazioni delle richieste di modifica](#).

3. In **Argomento SNS** per notificare agli approvatori, scegli una delle seguenti opzioni per specificare l'argomento Amazon SNS nel tuo account da utilizzare per inviare notifiche agli approvatori che stai aggiungendo a questa richiesta di modifica.

 Note

Se l'opzione per specificare un argomento Amazon SNS non è disponibile, il modello di modifica selezionato specifica già l'argomento SNS di Amazon da utilizzare.

- Inserisci un SNS Amazon Resource Name (ARN) – Per argomento ARN immetti l'ARN di un argomento Amazon SNS esistente. Questo argomento può essere incluso in qualsiasi account dell'organizzazione.
- Selezionare un argomento SNS esistente— Per l'Argomento notifica destinazione, seleziona l'ARN di un argomento Amazon SNS esistente nel tuo account corrente. (Questa

opzione non è disponibile se non hai ancora creato alcun argomento Amazon SNS nel tuo indirizzo attuale Account AWS ). Regione AWS

 Note

L'argomento Amazon SNS selezionato deve essere configurato in modo da specificare le notifiche inviate e gli abbonati a cui vengono inviati. La sua policy di accesso deve inoltre concedere autorizzazioni a Systems Manager in modo che Change Manager può inviare notifiche. Per informazioni, consulta [Configurazione degli argomenti di Amazon SNS per Change Manager notifiche](#).

4. Scegliere Add notification (Aggiungi notifica).

11. Scegli Avanti.

12. Per il Ruolo IAM seleziona un ruolo IAM nel tuo account corrente che dispone delle autorizzazioni necessarie per eseguire i runbook specificati per questa richiesta di modifica.

Questo ruolo viene anche definito ruolo di servizio, o assumere ruolo, per l'automazione. Per ulteriori informazioni su questo ruolo, consulta [Configurazione del servizio di automazione](#).

13. Nella Posizione di implementazione, scegli una delle seguenti opzioni:

 Note

Se lo utilizzi Change Manager con un Account AWS solo utente e non con un'organizzazione configurata AWS Organizations, non è necessario specificare un luogo di distribuzione.

- Applica modifiche a questo account: il flusso di lavoro del runbook viene eseguito solo nell'account corrente. Per un'organizzazione, questo è l'account amministratore delegato.
- Applica modifiche a più unità organizzative (UO), effettua le seguenti operazioni:
  1. Per Account e unità organizzative (UO), immetti l'ID di un account membro nella tua organizzazione, nel formato **123456789012** o l'ID di un'unità organizzativa, nel formato **o-o96EXAMPLE**.
  2. (Facoltativo) Per Nome del ruolo di esecuzione, immettere il nome del ruolo IAM nell'account di destinazione unità organizzativa che dispone delle autorizzazioni necessarie per eseguire i runbook specificati per questa richiesta di modifica. Tutti gli

account in qualsiasi unità organizzativa specificata devono utilizzare lo stesso nome per questo ruolo.

3. (Facoltativo) Scegli Aggiungi un'altra posizione di destinazione per ogni account aggiuntivo o unità organizzativa che si desidera specificare e ripetere i passaggi a e b.
4. Per Target Regione AWS, seleziona la regione in cui effettuare la modifica, ad esempio Ohio (us-east-2) per la regione Stati Uniti orientali (Ohio).
5. Espandee Rate control (Controllo velocità).

Per Concorrenza, immettere un numero, quindi dall'elenco selezionare se rappresenta il numero o la percentuale di account in cui è possibile eseguire contemporaneamente il flusso di lavoro del runbook.

Per Soglia errore, immettere un numero, quindi dall'elenco selezionare se rappresenta il numero o la percentuale di account in cui il flusso di lavoro del runbook può avere esito negativo prima che l'operazione venga arrestata.

#### 14. In Obiettivi di implementazione, procedi come indicato di seguito:

##### 1. Seleziona una delle seguenti opzioni:

- Singola risorsa— La modifica deve essere apportata per una sola risorsa. Ad esempio, un singolo nodo o una singola Amazon Machine Image (AMI), a seconda dell'operazione definita nei runbook per questa richiesta di modifica.
- Più risorse— Per Parametro, selezionare uno dei parametri disponibili dai runbook per questa richiesta di modifica. Questa selezione riflette il tipo di risorsa da aggiornare.

Ad esempio, se il runbook per questa richiesta di modifica è AWS-RetartEC2Instance è possibile scegliere InstanceId, quindi definire le istanze da aggiornare selezionando una delle seguenti opzioni:

- Specificare tag: immettere una coppia chiave-valore con cui tutte le risorse da aggiornare sono contrassegnate.
- Scelta di un gruppo di risorse— Scegliere il nome del gruppo di risorse a cui appartengono tutte le risorse da aggiornare.
- Specificare i valori dei parametri— Identificare le risorse da aggiornare nella sezione Parametri Runbook.
- Approvazioni come target – apporta la modifica su tutti i nodi gestiti nei percorsi di destinazione.

##### 2. Se hai scelto Più risorse, espandi Rate control (Controllo velocità).

Per Concorrenza, immettere un numero, quindi dall'elenco selezionare se rappresenta il numero o la percentuale di destinazioni che il flusso di lavoro del runbook può aggiornare contemporaneamente.

Per Soglia errore, immettere un numero, quindi dall'elenco selezionare se rappresenta il numero o la percentuale di destinazioni in cui l'aggiornamento può avere esito negativo prima dell'interruzione dell'operazione.

15. Se hai scelto Specificare i valori dei parametri per aggiornare più risorse nel passaggio precedente: nella sezione Parametri Runbook specificare i valori per i parametri di input obbligatori. I valori dei parametri che è necessario fornire si basano sul contenuto dei runbook Automation associati al modello di modifica scelto.

Ad esempio, se il modello di modifica utilizza il `AWS-RetartEC2Instance` runbook, devi inserire uno o più ID di istanza per il `InstanceId` parametro. In alternativa, scegliere Mostra selettore istanza interattivo e selezionare le istanze disponibili una per una.

16. Seleziona Successivo.
17. Nella pagina Esaminare e inviare, controllare due volte le risorse e le opzioni specificate per questa richiesta di modifica.

Selezionare Modificare per qualsiasi sezione a cui vuoi apportare modifiche.

Quando si è soddisfatti dei dettagli della richiesta di modifica, selezionare Invio per approvazione.

Se un argomento Amazon SNS è stato specificato nel modello di modifica scelto per la richiesta, le notifiche vengono inviate quando la richiesta viene rifiutata o approvata. Se non ricevi notifiche per la richiesta, puoi tornare a Change Manager per verificare lo stato della richiesta.

## Creazione di richieste di modifica (AWS CLI)

È possibile creare una richiesta di modifica utilizzando AWS Command Line Interface (AWS CLI) specificando le opzioni e i parametri per la richiesta di modifica in un file JSON e utilizzando l'`--cli-input-json` opzione per includerla nel comando.

## Per creare una richiesta di modifica (AWS CLI)

1. Installa e configura il AWS CLI o il AWS Strumenti per PowerShell, se non l'hai già fatto.

Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

2. Sul computer locale creare un file JSON denominato ad esempio `MyChangeRequest.json`, quindi incollarvi i seguenti contenuti.

Sostituisci *placeholders* con valori per la tua richiesta di modifica.

#### Note

Questo JSON di esempio crea una richiesta di modifica utilizzando il modello di modifica `AWS-HelloWorldChangeTemplate` e il runbook `AWS-HelloWorld`. Per adattare questo esempio alle tue richieste di modifica, consulta [StartChangeRequestExecution](#) nella Documentazione di riferimento API di AWS Systems Manager per informazioni su tutti i parametri disponibili.

Per informazioni sull'approvazione delle richieste di modifica, consulta la pagina [Informazioni sulle approvazioni delle richieste di modifica](#).

```
{
 "ChangeRequestName": "MyChangeRequest",
 "DocumentName": "AWS-HelloWorldChangeTemplate",
 "DocumentVersion": "$DEFAULT",
 "ScheduledTime": "2021-12-30T03:00:00",
 "ScheduledEndTime": "2021-12-30T03:05:00",
 "Tags": [
 {
 "Key": "Purpose",
 "Value": "Testing"
 }
],
 "Parameters": {
 "Approver": [
 "JohnDoe"
],
 "ApproverType": [
 "IamUser"
],
 "ApproverSnsTopicArn": [
 "arn:aws:sns:us-east-2:123456789012:MyNotificationTopic"
]
 }
}
```



```

]
 },
 "Runbooks": [
 {
 "DocumentName": "AWS-HelloWorld",
 "DocumentVersion": "1",
 "MaxConcurrency": "1",
 "MaxErrors": "1",
 "Parameters": {
 "AutomationAssumeRole": [
 "arn:aws:iam::123456789012:role/MyChangeManagerAssumeRole"
]
 }
 }
],
 "ChangeDetails": "### Document Name: HelloWorldChangeTemplate\n\n## What does this document do?\nThis change template demonstrates the feature set available for creating change templates for Change Manager. This template starts a Runbook workflow for the Automation document called AWS-HelloWorld.\n\n## Input Parameters\n\n* ApproverSnsTopicArn: (Required) Amazon Simple Notification Service ARN for approvers.\n* Approver: (Required) The name of the approver to send this request to.\n* ApproverType: (Required) The type of reviewer.\n * Allowed Values: IamUser, IamGroup, IamRole, SS0Group, SS0User\n\n## Output Parameters\nThis document has no outputs \n"
}

```

3. Nella directory in cui è stato creato il file JSON, eseguire il comando seguente.

```
aws ssm start-change-request-execution --cli-input-json file://MyChangeRequest.json
```

Il sistema restituisce informazioni simili alle seguenti.

```

{
 "AutomationExecutionId": "b3c1357a-5756-4839-8617-2d2a4EXAMPLE"
}

```

## Revisione e approvazione o rifiuto delle richieste di modifica

### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la pagina Modifica della disponibilità](#).

Se sei stato indicato come revisore per una richiesta di modifica in Change Manager, uno strumento di AWS Systems Manager, riceverai una notifica tramite un argomento Amazon Simple Notification Service (Amazon SNS), quando una richiesta di modifica è in attesa di revisione.

### Note

Questa funzionalità dipende dal fatto che nel modello di modifica sia stato specificato un Amazon SNS per l'invio delle notifiche di revisione. Per informazioni, consulta [Configurazione degli argomenti di Amazon SNS per Change Manager notifiche](#).

Per esaminare la richiesta di modifica, puoi seguire il link nella notifica oppure accedere Console di gestione AWS direttamente alla richiesta e seguire i passaggi di questa procedura.

### Note

Se un argomento Amazon SNS viene assegnato ai revisori in un modello di modifica, le notifiche vengono inviate agli abbonati dell'argomento quando la richiesta di modifica cambia lo stato.

Per informazioni sull'approvazione delle richieste di modifica, consulta la pagina [Informazioni sulle approvazioni delle richieste di modifica](#).

## Revisione e approvazione o rifiuto delle richieste di modifica (console)

Le seguenti procedure descrivono come utilizzare la console di Systems Manager per rivedere e approvare o rifiutare le richieste di modifica.

## Revisione e approvazione o rifiuto di una singola richiesta di modifica

1. Apri il link nella notifica e-mail che hai ricevuto e accedi a Console di gestione AWS, che ti reindirizza alla richiesta di modifica per la revisione.
2. Nella pagina di riepilogo esaminare il contenuto proposto della richiesta di modifica.

Per approvare la richiesta di modifica, scegliere Approve (Approva). Nella finestra di dialogo, specifica i commenti che desideri aggiungere per l'approvazione, quindi scegli Approva. Il flusso di lavoro del runbook rappresentato da questa richiesta inizia a essere eseguito quando è pianificato o non appena le modifiche non vengono bloccate da alcuna restrizione.

oppure

Per rifiutare la richiesta di modifica, scegliere Rifiuta. Nella finestra di dialogo, specifica i commenti che desideri aggiungere per questo rifiuto, quindi seleziona Rifiuta.

## Revisione e approvazione o rifiuto di richieste di modifica in blocco

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Change Manager.
3. Seleziona la scheda Approvals (Approvazioni).
4. (Facoltativo) Rivedi i dettagli delle richieste in attesa di approvazione selezionando il nome di ciascuna richiesta, quindi torna alla scheda Approvals (Approvazioni).
5. Seleziona la casella di controllo di ciascuna richiesta di modifica che desideri approvare.

oppure

Seleziona la casella di controllo di ciascuna richiesta di modifica che desideri rifiutare.

6. Nella finestra di dialogo, immetti eventuali commenti che desideri aggiungere per l'approvazione o il rifiuto.
7. A seconda che tu stia approvando o rifiutando le richieste di modifica selezionate, scegli Approve (Approva) o Reject (Rifiuta).

## Revisione e approvazione o rifiuto di una richiesta di modifica (riga di comando)

La procedura seguente descrive come utilizzare AWS Command Line Interface (AWS CLI) (su Linux/macOS, or Windows Server) per esaminare e approvare o rifiutare una richiesta di modifica.

Per rivedere e approvare o rifiutare una richiesta di modifica

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Crea un file JSON sul tuo computer locale che specifichi i parametri per la AWS CLI chiamata.

```
{
 "OpsItemFilters":
 [
 {
 "Key": "OpsItemType",
 "Values": ["/aws/changerequest"],
 "Operator": "Equal"
 }
],
 "MaxResults": number
}
```

Puoi filtrare i risultati per un approvatore specifico specificando il nome della Amazon Resource Name (ARN) dell'approvatore nel file JSON. Ecco un esempio.

```
{
 "OpsItemFilters":
 [
 {
 "Key": "OpsItemType",
 "Values": ["/aws/changerequest"],
 "Operator": "Equal"
 },
 {
 "Key": "ChangeRequestByApproverArn",
 "Values": ["arn:aws:iam::account-id:user/user-name"],
 "Operator": "Equal"
 }
],
}
```

```
"MaxResults": number
}
```

3. Eseguire questo comando per visualizzare il numero massimo di richieste di modifica specificato nel file JSON.

#### Linux & macOS

```
aws ssm describe-ops-items \
--cli-input-json file://filename.json
```

#### Windows

```
aws ssm describe-ops-items ^
--cli-input-json file://filename.json
```

4. Eseguire questo comando per approvare o rifiutare una richiesta di modifica.

#### Linux & macOS

```
aws ssm send-automation-signal \
--automation-execution-id ID \
--signal-type Approve_or_Reject \
--payload Comment="message"
```

#### Windows

```
aws ssm send-automation-signal ^
--automation-execution-id ID ^
--signal-type Approve_or_Reject ^
--payload Comment="message"
```

Se nel modello di modifica scelto per la richiesta è stato specificato un argomento Amazon SNS, le notifiche vengono inviate quando la richiesta viene rifiutata o approvata. Se non ricevi notifiche per la richiesta, puoi tornare a Change Manager per verificare lo stato della richiesta. Per informazioni sulle altre opzioni disponibili durante l'utilizzo di questo comando, consulta [send-automation-signal](#) nella sezione AWS Systems Manager del Riferimento ai comandi AWS CLI .

## Analisi dei dettagli delle richieste di modifica, dei processi e delle tempistiche (console)

### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la pagina Modifica della disponibilità](#).

È possibile visualizzare le informazioni su una richiesta di modifica, incluse le richieste per le quali le modifiche sono già state elaborate, nel pannello di controllo di Change Manager, uno strumento di AWS Systems Manager. Questi dettagli includono un collegamento all'operazione di automazione che esegue i runbook che apportano la modifica. Un ID di esecuzione di automazione viene generato quando viene creata la richiesta, ma il processo non viene eseguito finché non sono state fornite tutte le approvazioni e non sono in vigore restrizioni per bloccare la modifica.

Per esaminare i dettagli della richiesta di modifica, i processi e le tempistiche

1. Nel pannello di navigazione, scegli Change Manager.
2. Seleziona la scheda Richieste.
3. Nella sezione Richieste di modifica, cercare la richiesta di modifica che si desidera rivedere.

Puoi utilizzare il plugin Creare un intervallo di date per limitare i risultati a un periodo di tempo specifico.

È possibile filtrare le richieste in base alle seguenti proprietà:

- Status
- Request ID
- Approver
- Requester

Ad esempio, per visualizzare i dettagli su tutte le richieste di modifica completate correttamente nelle ultime 24 ore, procedi come segue:

1. Per Creare un intervallo di date, scegliere 1d.
2. Nella casella di ricerca, seleziona Stato, CompletedWithSuccess.

3. Nei risultati, scegliere il nome della richiesta di modifica completata correttamente per cui esaminare i risultati.
4. Visualizzare le informazioni sulla richiesta di modifica nelle schede seguenti:
  - **Dettagli della richiesta:** consente di visualizzare i dettagli di base sulla richiesta di modifica, inclusi il richiedente, il modello di modifica e i runbook di automazione selezionati per la modifica. Puoi anche seguire un link ai dettagli dell'operazione di automazione e visualizzare le informazioni sui parametri del runbook specificati nella richiesta, sugli CloudWatch allarmi Amazon assegnati alla richiesta di modifica e sulle approvazioni e i commenti forniti per la richiesta.
  - **Processo:** consente di visualizzare informazioni sul processo di modifica, inclusi lo stato del processo per le richieste di modifica completate, le risorse di destinazione, i passaggi nei runbook di automazione associati e i dettagli relativi alla soglia di errore e concorrenza.
  - **Pianificazione:** visualizza un riepilogo di tutti gli eventi associati alla richiesta di modifica, elencati per data e ora. Il riepilogo indica quando è stata creata la richiesta di modifica, le operazioni degli approvatori assegnati, una nota relativa alla pianificazione dell'esecuzione delle richieste di modifica approvate, i dettagli del flusso di lavoro del runbook e le modifiche di stato per il processo di modifica generale e per ogni passaggio del runbook.
  - **Eventi associati:** visualizza i dettagli verificabili sulle richieste di modifica registrate in [Data Lake AWS CloudTrail](#). I dettagli includono quali operazioni API sono state eseguite, i parametri di richiesta inclusi per tali operazioni, l'account utente che ha eseguito l'azione, le risorse aggiornate durante il processo e altro ancora.

Quando CloudTrail abiliti il monitoraggio degli eventi di CloudTrail Lake, Lake crea un archivio dati sugli eventi relativi alle tue richieste di modifica. I dettagli dell'evento sono disponibili per l'account o l'organizzazione in cui è stata eseguita la richiesta di modifica. Puoi attivare il monitoraggio degli eventi di CloudTrail Lake da qualsiasi richiesta di modifica nel tuo account o organizzazione. Per informazioni sull'attivazione dell'integrazione con CloudTrail Lake e sulla creazione di un archivio dati di eventi, consulta [Monitoraggio degli eventi della richiesta di modifica](#).

 **Note**

L'utilizzo di CloudTrail Lake è a pagamento. Per informazioni dettagliate, consulta [Prezzi di AWS CloudTrail](#).

## Visualizzazione dei conteggi aggregati delle richieste di modifica (riga di comando)

### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la pagina Modifica della disponibilità](#).

Puoi visualizzare i conteggi aggregati delle richieste di modifica in Change Manager, a tool in AWS Systems Manager, utilizzando l'operazione [GetOpsSummary](#) API. Questa operazione API può restituire i conteggi per un singolo account Account AWS in una Regione AWS o per più account e più regioni.

### Note

Se desideri visualizzare i conteggi aggregati delle richieste di modifica per più Account AWS e più richieste Regioni AWS, devi impostare e configurare una sincronizzazione dei dati delle risorse. Per ulteriori informazioni, consulta [Creazione di un Resource Data Sync per Inventario](#).

La procedura seguente descrive come utilizzare AWS Command Line Interface (AWS CLI) (su Linux o Windows Server) per visualizzare i conteggi aggregati delle richieste di modifica.

Per visualizzare i conteggi aggregati delle richieste di modifica

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Eseguire uno dei seguenti comandi.

Account singolo e Regione

Questo comando restituisce un conteggio di tutte le richieste di modifica per Account AWS e Regione AWS per le quali è configurata la AWS CLI sessione.



## Linux & macOS

```
aws ssm get-ops-summary \
--filters Key=AWS:OpsItem.OpsItemType,Values="/aws/changerequests",Type=Equal \
--aggregators AggregatorType=count,AttributeName=Status,TypeName=AWS:OpsItem
```

## Windows

```
aws ssm get-ops-summary ^
--filters Key=AWS:OpsItem.OpsItemType,Values="/aws/changerequests",Type=Equal ^
--aggregators AggregatorType=count,AttributeName=Status,TypeName=AWS:OpsItem
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
 "Entities": [
 {
 "Data": {
 "AWS:OpsItem": {
 "Content": [
 {
 "Count": "38",
 "Status": "Open"
 }
]
 }
 }
 }
]
}
```

## Account multipli, and/or regioni

Questo comando restituisce un conteggio di tutte le richieste di modifica per Account AWS e Regioni AWS specificate nella sincronizzazione dei dati delle risorse.

## Linux & macOS

```
aws ssm get-ops-summary \

```

```
--sync-name resource_data_sync_name \
--filters Key=AWS:OpsItem.OpsItemType,Values="/aws/
changerequests",Type=Equal \
--aggregators AggregatorType=count,AttributeName=Status,TypeName=AWS:OpsItem
```

## Windows

```
aws ssm get-ops-summary ^
--sync-name resource_data_sync_name ^
--filters Key=AWS:OpsItem.OpsItemType,Values="/aws/
changerequests",Type=Equal ^
--aggregators AggregatorType=count,AttributeName=Status,TypeName=AWS:OpsItem
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
 "Entities": [
 {
 "Data": {
 "AWS:OpsItem": {
 "Content": [
 {
 "Count": "43",
 "Status": "Open"
 },
 {
 "Count": "2",
 "Status": "Resolved"
 }
]
 }
 }
 }
]
}
```

## Più account e una regione specifica

Questo comando restituisce un conteggio di tutte le richieste di modifica per gli Account AWS specificate nella sincronizzazione dei dati delle risorse. Tuttavia, restituisce solo i dati della regione specificata nel comando.

## Linux & macOS

```
aws ssm get-ops-summary \
 --sync-name resource_data_sync_name \
 --filters Key=AWS:OpsItem.SourceRegion,Values='Region',Type=Equal
Key=AWS:OpsItem.OpsItemType,Values="/aws/changerequests",Type=Equal \
 --aggregators AggregatorType=count,AttributeName=Status,TypeName=AWS:OpsItem
```

## Windows

```
aws ssm get-ops-summary ^
 --sync-name resource_data_sync_name ^
 --filters Key=AWS:OpsItem.SourceRegion,Values='Region',Type=Equal
Key=AWS:OpsItem.OpsItemType,Values="/aws/changerequests",Type=Equal ^
 --aggregators AggregatorType=count,AttributeName=Status,TypeName=AWS:OpsItem
```

## Più account e Regioni con output raggruppati per Regione

Questo comando restituisce il conteggio di tutte le richieste di modifica per Account AWS e Regioni AWS specificate nella sincronizzazione dei dati delle risorse. L'output visualizza le informazioni sul conteggio per regione.

## Linux & macOS

```
aws ssm get-ops-summary \
 --sync-name resource_data_sync_name \
 --filters Key=AWS:OpsItem.OpsItemType,Values="/aws/
changerequests",Type=Equal \
 --aggregators
 '[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"Status","Aggregat
[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"SourceRegion"}]]]'
```

## Windows

```
aws ssm get-ops-summary ^
 --sync-name resource_data_sync_name ^
 --filters Key=AWS:OpsItem.OpsItemType,Values="/aws/
changerequests",Type=Equal ^
```

```
--aggregators
'[{ "AggregatorType": "count", "TypeName": "AWS:OpsItem", "AttributeName": "Status", "Aggregat
[{ "AggregatorType": "count", "TypeName": "AWS:OpsItem", "AttributeName": "SourceRegion" }]]'
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
 "Entities": [
 {
 "Data": {
 "AWS:OpsItem": {
 "Content": [
 {
 "Count": "38",
 "SourceRegion": "us-east-1",
 "Status": "Open"
 },
 {
 "Count": "4",
 "SourceRegion": "us-east-2",
 "Status": "Open"
 },
 {
 "Count": "1",
 "SourceRegion": "us-west-1",
 "Status": "Open"
 },
 {
 "Count": "2",
 "SourceRegion": "us-east-2",
 "Status": "Resolved"
 }
]
 }
 }
 }
]
}
```

Più account e regioni con output raggruppati per account e regioni

Questo comando restituisce il conteggio di tutte le richieste di modifica per Account AWS e Regioni AWS specificate nella sincronizzazione dei dati delle risorse. L'output raggruppa le informazioni di conteggio in base ad account e Regioni.

## Linux & macOS

```
aws ssm get-ops-summary \
 --sync-name resource_data_sync_name \
 --filters Key=AWS:OpsItem.OpsItemType,Values="/aws/
changerequests",Type=Equal \
 --aggregators
 '[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"Status","Aggregat
[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"SourceAccountId","A
[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"SourceRegion"}]]]]]
```

## Windows

```
aws ssm get-ops-summary ^
 --sync-name resource_data_sync_name ^
 --filters Key=AWS:OpsItem.OpsItemType,Values="/aws/
changerequests",Type=Equal ^
 --aggregators
 '[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"Status","Aggregat
[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"SourceAccountId","A
[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"SourceRegion"}]]]]]
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
 "Entities": [
 {
 "Data": {
 "AWS:OpsItem": {
 "Content": [
 {
 "Count": "38",
 "SourceAccountId": "123456789012",
 "SourceRegion": "us-east-1",
 "Status": "Open"
 }
],
 }
 }
 }
],
}
```

```

 {
 "Count": "4",
 "SourceAccountId": "111122223333",
 "SourceRegion": "us-east-2",
 "Status": "Open"
 },
 {
 "Count": "1",
 "SourceAccountId": "111122223333",
 "SourceRegion": "us-west-1",
 "Status": "Open"
 },
 {
 "Count": "2",
 "SourceAccountId": "444455556666",
 "SourceRegion": "us-east-2",
 "Status": "Resolved"
 },
 {
 "Count": "1",
 "SourceAccountId": "222222222222",
 "SourceRegion": "us-east-1",
 "Status": "Open"
 }
]
}

```

## Controllo e registrazione Change Manager activity

### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

Puoi controllare l'attività Change Manager utilizzando Amazon CloudWatch e gli AWS CloudTrail allarmi.

Per ulteriori informazioni sulle opzioni di verifica e registrazione per Systems Manager, consulta [Registrazione e monitoraggio AWS Systems Manager](#).

#### Audit Change Manager attività tramite allarmi CloudWatch

È possibile configurare e assegnare un CloudWatch allarme a un modello di modifica. Se vengono soddisfatte le condizioni definite nell'allarme, vengono intraprese le azioni specificate per l'allarme. Nella configurazione dell'allarme, puoi specificare un argomento Amazon Simple Notification Service (Amazon SNS) per notificare quando viene soddisfatta una condizione di allarme.

Per informazioni sulla creazione del modello Change Manager, consulta [Utilizzo dei modelli di modifica](#).

Per informazioni sulla creazione di CloudWatch allarmi, consulta [Using CloudWatch Alarms](#) nella Amazon CloudWatch User Guide.

#### Audit Change Manager attività utilizzando CloudTrail

CloudTrail acquisisce le chiamate API effettuate nella console di Systems Manager, AWS Command Line Interface (AWS CLI) e Systems Manager SDK. Puoi visualizzare le informazioni nella CloudTrail console o in un bucket Amazon Simple Storage Service (Amazon S3), dove sono archiviate. Viene utilizzato un bucket per tutti i CloudTrail log del tuo account.

I log delle operazioni Change Manager mostrano la creazione dei documenti del modello di modifica, le approvazioni e i rifiuti delle richieste di modifica e dei modelli di modifica, l'attività generata dai runbook di Automazione e altro ancora. Per ulteriori informazioni sulla visualizzazione e l'utilizzo dei CloudTrail registri delle attività di Systems Manager, vedere [Registrazione dei log AWS Systems Manager Chiamate API con AWS CloudTrail](#).

#### Risoluzione dei problemi Change Manager

##### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

Utilizza le informazioni seguenti per risolvere i problemi relativi a Change Manager, uno strumento di AWS Systems Manager.

## Argomenti

- [«Gruppo {GUID} errore «non trovato» durante l'approvazione delle richieste di modifica quando si utilizza Active Directory \(gruppi\)](#)

«Gruppo **{GUID}** errore «non trovato» durante l'approvazione delle richieste di modifica quando si utilizza Active Directory (gruppi)

Problema: quando Centro identità AWS IAM (IAM Identity Center) viene utilizzato per la gestione delle identità degli utenti, un membro di un gruppo di Active Directory a cui vengono concesse le autorizzazioni di approvazione Change Manager riceve un errore «non autorizzato» o «gruppo non trovato».

- Soluzione: quando si selezionano i gruppi di Active Directory in IAM Identity Center per l'accesso a Console di gestione AWS, il sistema pianifica una sincronizzazione periodica che copia le informazioni da tali gruppi di Active Directory in IAM Identity Center. Questo processo deve essere completato prima che gli utenti autorizzati tramite l'appartenenza al gruppo di Active Directory possano approvare correttamente una richiesta. Per ulteriori informazioni, consulta [Connetti una Microsoft AD](#) nella Guida per l'utente Centro identità AWS IAM .

## AWS Systems Manager Documenti di

Un AWS Systems Manager documento (documento SSM) definisce le azioni che Systems Manager esegue sulle istanze gestite. Systems Manager include più di 100 documenti preconfigurati che è possibile utilizzare specificando i parametri nel runtime (tempo di esecuzione). I documenti preconfigurati si possono trovare nella console Documenti di Systems Manager scegliendo la scheda Owned by Amazon (Di proprietà di Amazon) o specificando Amazon per il filtro Owner quando si chiama l'operazione dell'API `ListDocuments`. I documenti utilizzano JavaScript Object Notation (JSON) o YAML e includono passaggi e parametri specificati dall'utente.

Per una maggiore sicurezza, a partire dal 14 luglio 2025, i documenti SSM supportano l'interpolazione delle variabili di ambiente durante l'elaborazione dei parametri. Questa funzionalità, disponibile nella versione 2.2 dello schema e nella versione 3.3.2746.0 SSM Agent o successiva, aiuta a prevenire gli attacchi di iniezione di comandi.



Per iniziare a utilizzare i documenti SSM, apri la [console di Systems Manager](#). Nel pannello di navigazione, scegli Documenti.

 Important

In Systems Manager, un documento Amazon-owned SSM è un documento creato e gestito da Amazon Web Services stesso. Amazon-ownedi documenti includono un prefisso come AWS- \* nel nome del documento. Il proprietario del documento è considerato Amazon, non un account utente specifico al suo interno AWS. Questi documenti sono disponibili al pubblico e possono essere utilizzati da tutti.

Come può lo strumento Documenti essere vantaggioso per la mia organizzazione?

Documents offre i seguenti vantaggi:

- Categorie di documenti

Per trovare i documenti di cui hai bisogno, scegli una categoria a seconda del tipo di documento che stai cercando. Per ampliare la ricerca, è possibile scegliere più categorie dello stesso tipo di documento. La scelta di categorie di diversi tipi di documento non è supportata. Le categorie sono supportate solo per i documenti di proprietà di Amazon.

- Versioni dei documenti

È possibile creare e salvare diverse versioni dei documenti. È quindi possibile specificare una versione predefinita per ogni documento. La versione predefinita di un documento può essere aggiornata a una versione più recente o ripristinata a una versione precedente. Quando si modificano i contenuti di un documento, Systems Manager incrementa automaticamente la versione del documento. È possibile recuperare o utilizzare qualsiasi versione di un documento specificando la versione del documento nella console, nei comandi AWS Command Line Interface (AWS CLI) o nelle chiamate API.

- Personalizzazione di documenti per le proprie esigenze

Se desideri personalizzare le fasi e le operazioni in un documento, puoi creare un documento tuo. Il sistema memorizza il documento con il tuo nome utente Account AWS in Regione AWS cui lo crei. Per ulteriori informazioni su come creare un documento SSM, consultare [Creazione del contenuto del documento SSM](#).

- Tagging di documenti

È possibile applicare tag ai documenti per consentire ai clienti di individuarli rapidamente. Ad esempio, è possibile contrassegnare mediante tag documenti per ambienti, reparti, utenti, gruppi o periodi specifici. Puoi anche limitare l'accesso ai documenti creando una policy AWS Identity and Access Management (IAM) che specifica i tag a cui un utente o un gruppo può accedere.

- Condivisione di documenti

È possibile rendere i documenti pubblici o condividerli con Account AWS specifici nella stessa Regione AWS. La condivisione di documenti tra gli account può essere utile, ad esempio, se si desidera che tutte le istanze di Amazon Elastic Compute Cloud (Amazon EC2) fornite ai clienti e ai dipendenti abbiano la stessa configurazione. Oltre a mantenere aggiornate le applicazioni o le patch sulle istanze, è possibile limitare l'accesso a determinate attività da parte delle istanze dei clienti. Oppure potresti voler assicurarti che alle istanze utilizzate dagli account dei dipendenti in tutta l'organizzazione sia concesso l'accesso a risorse interne specifiche. Per ulteriori informazioni, consulta [Condivisione di documenti SSM](#).

## Chi deve utilizzare i documenti?

- Qualsiasi AWS cliente che desideri utilizzare gli strumenti di Systems Manager per migliorare la propria efficienza operativa su larga scala, ridurre gli errori associati all'intervento manuale e ridurre i tempi di risoluzione dei problemi comuni.
- Esperti di infrastruttura che desiderano automatizzare le attività di implementazione e configurazione.
- Amministratori che desiderano risolvere in modo affidabile i problemi comuni, migliorare l'efficienza della risoluzione dei problemi e ridurre le operazioni ripetitive.
- Utenti che desiderano automatizzare un'attività che in genere eseguono manualmente.

## Quali sono i tipi di documenti SSM?

La tabella seguente illustra i diversi tipi di documenti SSM e il loro utilizzo.

| Tipo                     | Utilizzo con                  | Informazioni                                                                     |
|--------------------------|-------------------------------|----------------------------------------------------------------------------------|
| ApplicationConfiguration | <a href="#">AWS AppConfig</a> | AWS AppConfig consente di creare, gestire e distribuire rapidamente le configura |

| Tipo                           | Utilizzo con | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ApplicationConfigurationSchema |              | <p>zioni delle applicazioni. È possibile archiviare i dati di configurazione in un documento SSM creando un documento che utilizza il tipo di documento <code>ApplicationConfiguration</code>. Per ulteriori informazioni, consulta <a href="#">Configurazioni in forma libera</a> nella Guida per l'utente di AWS AppConfig.</p> <p>Se crei una configurazione in un documento SSM, devi specificare o creare uno schema JSON corrispondente. Lo schema utilizza il tipo di documento <code>ApplicationConfigurationSchema</code> e, come un insieme di regole, definisce le proprietà consentite per ogni impostazione di configurazione dell'applicazione. Per ulteriori informazioni, consulta <a href="#">Informazioni sui validatori</a> nella Guida per l'utente di AWS AppConfig.</p> |

| Tipo               | Utilizzo con                                                                                        | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| runbook Automation | <a href="#">Automazione</a><br><a href="#">State Manager</a><br><a href="#">Maintenance Windows</a> | <p>Utilizza i runbook di Automazione durante l'esecuzione di attività comuni di manutenzione e implementazione, ad esempio la creazione o l'aggiornamento di una Amazon Machine Image (AMI). State Manager utilizza i runbook di Automazione per applicare una configurazione. Queste operazioni possono essere eseguite su una o più destinazioni in qualsiasi momento durante il ciclo di vita di un'istanza. Maintenance Windows utilizza i runbook di Automazione per eseguire attività comuni di manutenzione e implementazione in base alla pianificazione specificata.</p> <p>Tutti i runbook di automazione supportati per i sistemi Linux-based operativi sono supportati anche sulle istanze EC2 per macOS</p> |

| Tipo                          | Utilizzo con                    | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Documento Modifica calendario | <a href="#">Change Calendar</a> | <p>Change Calendar utilizza il tipo di documento. ChangeCalendar Un documento Change Calendar memorizza una voce del calendario e gli eventi associati che possono consentire o impedire alle operazioni di automazione di modificare l'ambiente. In Change Calendar, un documento memorizza i dati <a href="#">iCalendar 2.0</a> in formato testo normale.</p> <p>Change Calendar non è supportato nelle istanze EC2 per macOS.</p> |

| Tipo                       | Utilizzo con                       | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AWS CloudFormation modello | <a href="#">AWS CloudFormation</a> | <p>AWS CloudFormation i modelli descrivono le risorse di cui desideri fornire nei tuoi CloudFormation stack. Archiviando CloudFormation i modelli come documenti di Systems Manager, è possibile trarre vantaggio dalle funzionalità dei documenti di Systems Manager. Questi includono la creazione e il confronto di più versioni del modello e la condivisione del modello con altri account nella stessa Regione AWS.</p> <p>È possibile creare e modificare e CloudFormation modelli e stack utilizzando Application Manager. Per ulteriori informazioni, consulta <a href="#">Lavorare con CloudFormation modelli e impilabili Application Manager</a>.</p> |

| Tipo                 | Utilizzo con                                                                                        | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Documento di comando | <a href="#">Run Command</a><br><a href="#">State Manager</a><br><a href="#">Maintenance Windows</a> | <p>Run Command utilizza i documenti Command per eseguire comandi. State Manager utilizza i documenti di comando per applicare una configurazione. Queste azioni possono essere eseguite su uno o più obiettivi in qualsiasi momento durante il ciclo di vita di un'istanza. Maintenance Windows utilizza i documenti Command per applicare una configurazione basata sulla pianificazione specificata.</p> <p>La maggior parte dei documenti Command è supportata su tutti i sistemi operativi Linux e Windows Server compatibile con Systems Manager. I seguenti documenti Command sono supportati nelle istanze EC2 per macOS:</p> <ul style="list-style-type: none"><li>• AWS-ConfigureAWSPackage</li><li>• AWS-RunPatchBaseline</li><li>• AWS-RunPatchBaselineAssociation</li><li>• AWS-RunShellScript</li></ul> |

| Tipo                                          | Utilizzo con                | Informazioni                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AWS Config modello di pacchetto di conformità | <a href="#">AWS Config</a>  | <p>AWS Config i modelli di pacchetti di conformità sono documenti in formato YAML utilizzati per creare pacchetti di conformità che contengono o l'elenco delle regole e delle azioni correttive gestite o personalizzate. AWS Config</p> <p>Per ulteriori informazioni, consulta la pagina <a href="#">Pacchetti di conformità</a>.</p>                                         |
| Documento del pacchetto                       | <a href="#">Distributor</a> | <p>InDistributor, un pacchetto è rappresentato da un documento SSM. Un documento di un pacchetto include file di archivio ZIP allegati che contengono software o asset da installare e su istanze gestite. La creazione di un pacchetto in Distributor genera il documento del pacchetto.</p> <p>Distributor non è supportato da Oracle Linux e dalle istanze gestite macOS.</p> |



| Tipo                             | Utilizzo con                                                                        | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Documento di policy              | <a href="#">State Manager</a>                                                       | <p>Inventory utilizza il documento <code>AWS-GatherSoftwareInventory</code> Policy con un'associazione State Manager e per raccogliere i dati di inventario dalle istanze gestite. Durante la creazione dei documenti SSM, i runbook Automation e i documenti Command sono il metodo preferito per applicare una policy su un'istanza gestita.</p> <p>L'inventario di Systems Manager e il documento di policy <code>AWS-GatherSoftwareInventory</code> sono supportati su tutti i sistemi operativi compatibili con Systems Manager.</p> |
| Post-incident modello di analisi | <a href="#">Analisi post-imprevisto dello Strumento di gestione degli incidenti</a> | <p>Incident Manager utilizza il modello di analisi post-incidente per creare un'analisi basata sulle migliori pratiche di gestione delle AWS operazioni.</p> <p>Usare il modello per creare un'analisi che il team può utilizzare per individuare i miglioramenti apportati alla risposta agli imprevisti.</p>                                                                                                                                                                                                                            |

| Tipo                  | Utilizzo con                    | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Documento di sessione | <a href="#">Session Manager</a> | <p>Session Manager utilizza i documenti di sessione per determinare il tipo di sessione da avviare. Gli esempi includono sessioni di port forwarding, sessioni di comando interattive e tunnel SSH.</p> <p>I documenti di sessione sono supportati su tutti i sistemi operativi Linux e Windows Server compatibili con Systems Manager. I seguenti documenti Command sono supportati nelle istanze EC2 per macOS:</p> <ul style="list-style-type: none"><li>• AWS-PasswordReset</li><li>• AWS-StartInteractiveCommand</li><li>• AWS-StartPortForwardingSession</li><li>• AWS-StartPortForwardingSessionToSocket</li><li>• AWS-StartSSHSession</li></ul> |

## Quote del documento SSM

Per informazioni sulle quote del documento SSM, consulta [Service quotas di Systems Manager](#) nella Riferimenti generali di Amazon Web Services.

## Argomenti

- [Componenti del documento](#)
- [Creazione del contenuto del documento SSM](#)
- [Utilizzo dei documenti](#)
- [Risoluzione dei problemi di gestione dei parametri](#)

## Componenti del documento

In questa sezione sono incluse informazioni sui componenti che compongono i documenti SSM.

### Indice

- [Schemi, funzionalità ed esempi](#)
- [Elementi di dati e parametri](#)
- [Documentazione di riferimento del plugin per i documenti di comando](#)

### Schemi, funzionalità ed esempi

AWS Systems Manager I documenti (SSM) utilizzano le seguenti versioni dello schema.

- I documenti di tipo `Command` possono utilizzare le versioni dello schema 1.2, 2.0 e 2.2. Se si utilizzano documenti con lo schema 1.2, consigliamo di creare documenti con la versione 2.2 dello schema.
- I documenti di tipo `Policy` devono utilizzare la versione dello schema 2.0 o una versione successiva.
- I documenti di tipo `Automation` devono utilizzare la versione dello schema 0.3.
- I documenti di tipo `Session` devono utilizzare la versione dello schema 1.0.
- Puoi creare documenti in formato JSON o YAML.

Per ulteriori informazioni sull'utilizzo del documento schema `Session`, consulta [Schema documento di sessione](#).

Utilizzando la versione più recente dello schema per documenti `Command` e `Policy`, puoi sfruttare le seguenti funzionalità.

## Funzionalità dei documenti con versione dello schema 2.2

| Funzionalità                        | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modifica dei documenti              | Ora i documenti possono essere aggiornati. Con la versione 1.2, qualsiasi aggiornamento a un documento doveva essere salvato con un nome diverso.                                                                                                                                                                                                                                                                                                                                                                                      |
| Controllo delle versioni automatico | Qualsiasi aggiornamento a un documento crea una nuova versione. Non si tratta di una versione dello schema, ma di una versione del documento.                                                                                                                                                                                                                                                                                                                                                                                          |
| Versione predefinita                | Se disponi di più versioni di un documento, puoi specificare quale versione è il documento predefinito.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Sequenziamento                      | I plugin o le fasi in un documento vengono eseguiti nell'ordine specificato.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Cross-platform supporto             | Cross-platform il supporto consente di specificare diversi sistemi operativi per diversi plugin all'interno dello stesso documento SSM. Cross-platform support utilizza il <code>precondition</code> parametro all'interno di un passaggio.                                                                                                                                                                                                                                                                                            |
| Interpolazione dei parametri        | Interpolazione significa inserire o sostituire un valore variabile in una stringa. Immagina che sia come riempire uno spazio vuoto con valori effettivi, prima che la stringa venga utilizzata. Nel contesto dei documenti SSM, l'interpolazione dei parametri consente di interpolare i parametri delle stringhe in variabili di ambiente prima dell'esecuzione del comando, offrendo una maggiore sicurezza contro le iniezioni di comandi. Se impostato su <code>ENV_VAR</code> , l'agente crea una variabile di ambiente denominat |

| Funzionalità | Informazioni                                                         |
|--------------|----------------------------------------------------------------------|
|              | a SSM_ <i>parameter-name</i> , che contiene il valore del parametro. |

### Note

È necessario mantenere AWS Systems Manager SSM Agent le istanze aggiornate con la versione più recente per utilizzare le nuove funzionalità di Systems Manager e le funzionalità dei documenti SSM. Per ulteriori informazioni, consulta [Aggiornamento di SSM Agent utilizzando Run Command](#).

Nella tabella seguente vengono elencate le differenze tra le versioni principali dello schema.

| Versione 1.2  | Versione 2.2 (versione più recente) | Informazioni                                                                                                                                                                                 |
|---------------|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| runtimeConfig | mainSteps                           | Nella versione 2.2, la sezione <code>mainSteps</code> sostituisce <code>runtimeConfig</code> . La sezione <code>mainSteps</code> consente a Systems Manager di eseguire le fasi in sequenza. |
| properties    | inputs                              | Nella versione 2.2, la sezione <code>inputs</code> sostituisce la sezione <code>properties</code> . La sezione <code>inputs</code> accetta parametri per le fasi.                            |
| commands      | runCommand                          | Nella versione 2.2, la sezione <code>inputs</code> richiede il parametro <code>runCommand</code> anziché il parametro <code>commands</code> .                                                |

| Versione 1.2    | Versione 2.2 (versione più recente) | Informazioni                                                                                        |
|-----------------|-------------------------------------|-----------------------------------------------------------------------------------------------------|
| id              | operazione                          | Nella versione 2.2, <code>Action</code> sostituisce ID. Si tratta di una semplice modifica di nome. |
| non applicabile | nome                                | Nella versione 2.2, <code>name</code> è un qualsiasi nome definito dall'utente per una fase.        |

## Utilizzo del parametro Precondition

Con la versione dello schema 2.2 o successiva, è possibile utilizzare il parametro `precondition` per specificare il sistema operativo di destinazione per ciascun plugin o convalidare i parametri di input definiti nel documento SSM. Il parametro `precondition` supporta il riferimento ai parametri di input del documento SSM e `platformType` utilizzando i valori di Linux, MacOS, e Windows. Soltanto l'operatore `StringEquals` è supportato.

Per i documenti che utilizzano la versione dello schema 2.2 o successiva, se `precondition` non è specificato, ogni plugin viene eseguito o ignorato in base alla relativa compatibilità con il sistema operativo. La compatibilità dei plugin con il sistema operativo viene valutata prima di `precondition`. Per i documenti che utilizzano la versione dello schema 2.0 o precedente, i plugin non compatibili generano un errore.

Ad esempio, in un documento della versione 2.2 dello schema, se `precondition` non è specificato e il `aws:runShellScript` plug-in è elencato, il passaggio viene eseguito sulle istanze Linux ma viene saltato sulle istanze Windows Server. Questo perché `aws:runShellScript` non è compatibile con Windows Server. In un documento con schema versione 2.0, la specificazione `aws:runShellScript` e l'esecuzione del documento su un'istanza Windows Server causa il fallimento dell'esecuzione.

## Versione dello schema 2.2

### Top-level elementi

L'esempio seguente mostra gli elementi di primo livello di un documento SSM che utilizza la versione dello schema 2.2.

## YAML

```

schemaVersion: "2.2"
description: A description of the document.
parameters:
 parameter 1:
 property 1: "value"
 property 2: "value"
 parameter 2:
 property 1: "value"
 property 2: "value"
mainSteps:
- action: Plugin name
 name: A name for the step.
 inputs:
 input 1: "value"
 input 2: "value"
 input 3: "{{ parameter 1 }}"
```

## JSON

```
{
 "schemaVersion": "2.2",
 "description": "A description of the document.",
 "parameters": {
 "parameter 1": {
 "property 1": "value",
 "property 2": "value"
 },
 "parameter 2": {
 "property 1": "value",
 "property 2": "value"
 }
 },
 "mainSteps": [
 {
 "action": "Plugin name",
 "name": "A name for the step.",
 "inputs": {
 "input 1": "value",
 "input 2": "value",
 "input 3": "{{ parameter 1 }}"
 }
 }
]
}
```

```
 }
 }
]
}
```

## Esempio con per la versione dello schema 2.2

L'esempio seguente utilizza il `aws:runPowerShellScript` plugin per eseguire un PowerShell comando sulle istanze di destinazione.

## YAML

```

schemaVersion: "2.2"
description: "Example document"
parameters:
 Message:
 type: "String"
 description: "Example parameter"
 default: "Hello World"
 allowedValues:
 - "Hello World"
mainSteps:
 - action: "aws:runPowerShellScript"
 name: "example"
 inputs:
 timeoutSeconds: '60'
 runCommand:
 - "Write-Output {{Message}}"
```

## JSON

```
{
 "schemaVersion": "2.2",
 "description": "Example document",
 "parameters": {
 "Message": {
 "type": "String",
 "description": "Example parameter",
 "default": "Hello World",
 "allowedValues": ["Hello World"]
 }
 }
}
```



```

 },
 "mainSteps": [
 {
 "action": "aws:runPowerShellScript",
 "name": "example",
 "inputs": {
 "timeoutSeconds": "60",
 "runCommand": [
 "Write-Output {{Message}}"
]
 }
 }
]
 }
}

```

## Esempi del parametro Precondition per la versione dello schema 2.2

La versione dello schema 2.2 offre il supporto multiplatforma. Ciò significa che all'interno di un singolo documento SSM è possibile specificare diversi sistemi operativi per diversi plugin. Cross-platform support utilizza il precondition parametro all'interno di un passaggio, come mostrato nell'esempio seguente. È possibile utilizzare il parametro precondition anche per convalidare i parametri di input definiti nel documento SSM. Ne è la riprova il secondo dei seguenti esempi.

### YAML

```

schemaVersion: '2.2'
description: cross-platform sample
mainSteps:
- action: aws:runPowerShellScript
 name: PatchWindows
 precondition:
 StringEquals:
 - platformType
 - Windows
 inputs:
 runCommand:
 - cmds
- action: aws:runShellScript
 name: PatchLinux
 precondition:
 StringEquals:

```

```
- platformType
- Linux
inputs:
 runCommand:
 - cmds
```

## JSON

```
{
 "schemaVersion": "2.2",
 "description": "cross-platform sample",
 "mainSteps": [
 {
 "action": "aws:runPowerShellScript",
 "name": "PatchWindows",
 "precondition": {
 "StringEquals": [
 "platformType",
 "Windows"
]
 },
 "inputs": {
 "runCommand": [
 "cmds"
]
 }
 },
 {
 "action": "aws:runShellScript",
 "name": "PatchLinux",
 "precondition": {
 "StringEquals": [
 "platformType",
 "Linux"
]
 },
 "inputs": {
 "runCommand": [
 "cmds"
]
 }
 }
]
}
```

```
}
```

## YAML

```

schemaVersion: '2.2'
parameters:
 action:
 type: String
 allowedValues:
 - Install
 - Uninstall
 confirmed:
 type: String
 allowedValues:
 - True
 - False
mainSteps:
- action: aws:runShellScript
 name: InstallAwsCLI
 precondition:
 StringEquals:
 - "{{ action }}"
 - "Install"
 inputs:
 runCommand:
 - sudo apt install aws-cli
- action: aws:runShellScript
 name: UninstallAwsCLI
 precondition:
 StringEquals:
 - "{{ action }}" "{{ confirmed }}"
 - "Uninstall True"
 inputs:
 runCommand:
 - sudo apt remove aws-cli
```

## JSON

```
{
 "schemaVersion": "2.2",
 "parameters": {
```

```
"action": {
 "type": "String",
 "allowedValues": [
 "Install",
 "Uninstall"
]
},
"confirmed": {
 "type": "String",
 "allowedValues": [
 true,
 false
]
}
},
"mainSteps": [
 {
 "action": "aws:runShellScript",
 "name": "InstallAwsCLI",
 "precondition": {
 "StringEquals": [
 "{{ action }}",
 "Install"
]
 },
 "inputs": {
 "runCommand": [
 "sudo apt install aws-cli"
]
 }
 },
 {
 "action": "aws:runShellScript",
 "name": "UninstallAwsCLI",
 "precondition": {
 "StringEquals": [
 "{{ action }} {{ confirmed }}",
 "Uninstall True"
]
 },
 "inputs": {
 "runCommand": [
 "sudo apt remove aws-cli"
]
 }
 }
]
```

```

 }
 }
]
}

```

### Esempio di interpolazione dello schema versione 2.2 con Agente SSM versioni precedenti alla 3.3.2746.0

Nelle versioni SSM Agent precedenti alla 3.3.2746.0, l'agente ignora il parametro `interpolationType` ed esegue invece una sostituzione di stringhe non elaborate. Se si fa riferimento in modo esplicito a `SSM_parameter-name`, è necessario impostarlo in modo esplicito. Nell'esempio seguente per Linux, la variabile di ambiente `SSM_Message` viene referenziata in modo esplicito.

```

{
 "schemaVersion": "2.2",
 "description": "An example document",
 "parameters": {
 "Message": {
 "type": "String",
 "description": "Message to be printed",
 "default": "Hello",
 "interpolationType" : "ENV_VAR",
 "allowedPattern": "^[^"]*$"
 }
 },
 "mainSteps": [{
 "action": "aws:runShellScript",
 "name": "printMessage",
 "inputs": {
 "runCommand": [
 "if [-z \"${SSM_Message+x}\"]; then",
 " export SSM_Message=\"${Message}\"",
 "fi",
 "",
 "echo $SSM_Message"
]
 }
]
}

```

```
}
```

### Note

`allowedPattern` non è tecnicamente necessario, se un documento SSM non utilizza le parentesi graffe: `{{ }}`

## Versione dello schema 2.2 State Manager example

È possibile utilizzare il seguente documento SSM con State Manager per scaricare e installare il software antivirus ClamAV. State Manager impone una configurazione specifica, il che significa che ogni volta che viene eseguita l'associazione, il sistema controlla se il software ClamAV è installato. Se così non fosse, State Manager esegue nuovamente questo documento.

### YAML

```

schemaVersion: '2.2'
description: State Manager Bootstrap Example
parameters: {}
mainSteps:
- action: aws:runShellScript
 name: configureServer
 inputs:
 runCommand:
 - sudo yum install -y httpd24
 - sudo yum --enablerepo=epel install -y clamav
```

### JSON

```
{
 "schemaVersion": "2.2",
 "description": "State Manager Bootstrap Example",
 "parameters": {},
 "mainSteps": [
 {
 "action": "aws:runShellScript",
 "name": "configureServer",
 "inputs": {
 "runCommand": [
```

```
 "sudo yum install -y httpd24",
 "sudo yum --enablerepo=epel install -y clamav"
]
}
}
```

Esempio di versione dello schema 2.2 per un inventario

È possibile utilizzare il seguente documento SSM con State Manager per raccogliere i metadati di inventario sulle istanze.

## YAML

```

schemaVersion: '2.2'
description: Software Inventory Policy Document.
parameters:
 applications:
 type: String
 default: Enabled
 description: "(Optional) Collect data for installed applications."
 allowedValues:
 - Enabled
 - Disabled
 awsComponents:
 type: String
 default: Enabled
 description: "(Optional) Collect data for AWS Components like amazon-ssm-agent."
 allowedValues:
 - Enabled
 - Disabled
 networkConfig:
 type: String
 default: Enabled
 description: "(Optional) Collect data for Network configurations."
 allowedValues:
 - Enabled
 - Disabled
 windowsUpdates:
 type: String
```

```

 default: Enabled
 description: "(Optional) Collect data for all Windows Updates."
 allowedValues:
 - Enabled
 - Disabled
 instanceDetailedInformation:
 type: String
 default: Enabled
 description: "(Optional) Collect additional information about the instance,
including
 the CPU model, speed, and the number of cores, to name a few."
 allowedValues:
 - Enabled
 - Disabled
 customInventory:
 type: String
 default: Enabled
 description: "(Optional) Collect data for custom inventory."
 allowedValues:
 - Enabled
 - Disabled
 mainSteps:
 - action: aws:softwareInventory
 name: collectSoftwareInventoryItems
 inputs:
 applications: "{{ applications }}"
 awsComponents: "{{ awsComponents }}"
 networkConfig: "{{ networkConfig }}"
 windowsUpdates: "{{ windowsUpdates }}"
 instanceDetailedInformation: "{{ instanceDetailedInformation }}"
 customInventory: "{{ customInventory }}"

```

## JSON

```

{
 "schemaVersion": "2.2",
 "description": "Software Inventory Policy Document.",
 "parameters": {
 "applications": {
 "type": "String",
 "default": "Enabled",
 "description": "(Optional) Collect data for installed applications.",
 "allowedValues": [

```



```
 "Enabled",
 "Disabled"
]
},
"awsComponents": {
 "type": "String",
 "default": "Enabled",
 "description": "(Optional) Collect data for AWS Components like amazon-ssm-agent.",
 "allowedValues": [
 "Enabled",
 "Disabled"
]
},
"networkConfig": {
 "type": "String",
 "default": "Enabled",
 "description": "(Optional) Collect data for Network configurations.",
 "allowedValues": [
 "Enabled",
 "Disabled"
]
},
"windowsUpdates": {
 "type": "String",
 "default": "Enabled",
 "description": "(Optional) Collect data for all Windows Updates.",
 "allowedValues": [
 "Enabled",
 "Disabled"
]
},
"instanceDetailedInformation": {
 "type": "String",
 "default": "Enabled",
 "description": "(Optional) Collect additional information about the instance, including\nthe CPU model, speed, and the number of cores, to name a few.",
 "allowedValues": [
 "Enabled",
 "Disabled"
]
},
"customInventory": {
```

```

 "type": "String",
 "default": "Enabled",
 "description": "(Optional) Collect data for custom inventory.",
 "allowedValues": [
 "Enabled",
 "Disabled"
]
 },
 "mainSteps": [
 {
 "action": "aws:softwareInventory",
 "name": "collectSoftwareInventoryItems",
 "inputs": {
 "applications": "{{ applications }}",
 "awsComponents": "{{ awsComponents }}",
 "networkConfig": "{{ networkConfig }}",
 "windowsUpdates": "{{ windowsUpdates }}",
 "instanceDetailedInformation": "{{ instanceDetailedInformation }}",
 "customInventory": "{{ customInventory }}"
 }
 }
]
}

```

Esempio con **AWS-ConfigureAWSPackage** per la versione dello schema 2.2

L'esempio seguente mostra il documento AWS-ConfigureAWSPackage. La sezione mainSteps include il plugin aws:configurePackage nella fase action.

#### Note

Sui sistemi operativi Linux sono supportati solo i pacchetti AmazonCloudWatchAgent e AWSSupport-EC2Rescue.

## YAML

```

schemaVersion: '2.2'
description: 'Install or uninstall the latest version or specified version of an AWS

```

```

package. Available packages include the following: AWSPVDriver, AwsEnaNetworkDriver,
 AwsVssComponents, and AmazonCloudWatchAgent, and AWSSupport-EC2Rescue.'
parameters:
 action:
 description: "(Required) Specify whether to install or uninstall the package."
 type: String
 allowedValues:
 - Install
 - Uninstall
 name:
 description: "(Required) The package to install/uninstall."
 type: String
 allowedPattern: "^arn:[a-z0-9][-.a-z0-9]{0,62}:[a-z0-9][-.a-z0-9]{0,62}:([a-
z0-9][-.a-z0-9]{0,62})?:([a-z0-9][-.a-z0-9]{0,62})?:package\\/[a-zA-Z][a-zA-Z0-9\\-
]{0,39}$|^([a-zA-Z][a-zA-Z0-9\\-]{0,39})$"
 version:
 type: String
 description: "(Optional) A specific version of the package to install or
uninstall."
mainSteps:
- action: aws:configurePackage
 name: configurePackage
 inputs:
 name: "{{ name }}"
 action: "{{ action }}"
 version: "{{ version }}"

```

## JSON

```

{
 "schemaVersion": "2.2",
 "description": "Install or uninstall the latest version or specified version
of an AWS package. Available packages include the following: AWSPVDriver,
 AwsEnaNetworkDriver, AwsVssComponents, and AmazonCloudWatchAgent, and AWSSupport-
 EC2Rescue.",
 "parameters": {
 "action": {
 "description": "(Required) Specify whether to install or uninstall the
package.",
 "type": "String",
 "allowedValues": [
 "Install",
 "Uninstall"
]
 }
 }
}

```

```

]
 },
 "name": {
 "description": "(Required) The package to install/uninstall.",
 "type": "String",
 "allowedPattern": "^arn:[a-z0-9][-.a-z0-9]{0,62}:[a-z0-9][-.a-z0-9]{0,62}:([a-z0-9][-.a-z0-9]{0,62})?:([a-z0-9][-.a-z0-9]{0,62})?:package\\/[a-zA-Z][a-zA-Z0-9\\-_]{0,39}$|^([a-zA-Z][a-zA-Z0-9\\-_]{0,39})$"
 },
 "version": {
 "type": "String",
 "description": "(Optional) A specific version of the package to install or uninstall."
 }
},
"mainSteps":[
{
 "action": "aws:configurePackage",
 "name": "configurePackage",
 "inputs": {
 "name": "{{ name }}",
 "action": "{{ action }}",
 "version": "{{ version }}"
 }
}
]
}

```

## Versione dello schema 1.2

L'esempio seguente mostra gli elementi di primo livello di un documento che utilizza la versione dello schema 1.2.

```

{
 "schemaVersion":"1.2",
 "description":"A description of the SSM document.",
 "parameters":{
 "parameter 1":{
 "one or more parameter properties"
 },
 "parameter 2":{
 "one or more parameter properties"
 }
 }
}

```

```

 },
 "parameter 3":{
 "one or more parameter properties"
 }
 },
 "runtimeConfig":{
 "plugin 1":{
 "properties":[
 {
 "one or more plugin properties"
 }
]
 }
 }
}

```

### Schema versione 1.2 aws:run example **ShellScript**

L'esempio seguente mostra il documento SSM AWS-RunShellScript. La sezione runtimeConfig include il plugin aws:runShellScript.

```

{
 "schemaVersion":"1.2",
 "description":"Run a shell script or specify the commands to run.",
 "parameters":{
 "commands":{
 "type":"StringList",
 "description":"(Required) Specify a shell script or a command to run.",
 "minItems":1,
 "displayType":"textarea"
 },
 "workingDirectory":{
 "type":"String",
 "default":"",
 "description":"(Optional) The path to the working directory on your
instance.",
 "maxChars":4096
 },
 "executionTimeout":{
 "type":"String",
 "default":"3600",

```

```

 "description": "(Optional) The time in seconds for a command to complete
 before it is considered to have failed. Default is 3600 (1 hour). Maximum is 172800
 (48 hours).",
 "allowedPattern": "([1-9][0-9]{0,3})|(1[0-9]{1,4})|(2[0-7][0-9]{1,3})|
 (28[0-7][0-9]{1,2})|(28800)"
 },
 "runtimeConfig": {
 "aws:runShellScript": {
 "properties": [
 {
 "id": "0.aws:runShellScript",
 "runCommand": "{{ commands }}",
 "workingDirectory": "{{ workingDirectory }}",
 "timeoutSeconds": "{{ executionTimeout }}"
 }
]
 }
 }
}

```

### Versione dello schema 0.3

#### Top-level elementi

L'esempio seguente mostra gli elementi di primo livello di un runbook Automation che utilizza la versione dello schema 0.3 in formato JSON.

```

{
 "description": "document-description",
 "schemaVersion": "0.3",
 "assumeRole": "{{assumeRole}}",
 "parameters": {
 "parameter1": {
 "type": "String",
 "description": "parameter-1-description",
 "default": ""
 },
 "parameter2": {
 "type": "String",
 "description": "parameter-2-description",
 "default": ""
 }
 }
}

```

```
 },
 "variables": {
 "variable1": {
 "type": "StringMap",
 "description": "variable-1-description",
 "default": {}
 },
 "variable2": {
 "type": "String",
 "description": "variable-2-description",
 "default": "default-value"
 }
 },
 "mainSteps": [
 {
 "name": "myStepName",
 "action": "action-name",
 "maxAttempts": 1,
 "inputs": {
 "Handler": "python-only-handler-name",
 "Runtime": "runtime-name",
 "Attachment": "script-or-zip-name"
 },
 "outputs": {
 "Name": "output-name",
 "Selector": "selector.value",
 "Type": "data-type"
 }
 }
],
 "files": {
 "script-or-zip-name": {
 "checksums": {
 "sha256": "checksum"
 },
 "size": 1234
 }
 }
}
```

## Esempio di runbook Automation YAML

L'esempio seguente mostra il contenuto di un runbook Automation, in formato YAML. Questo esempio d'uso della versione 0.3 dello schema del documento dimostra anche l'utilizzo di Markdown per formattare le descrizioni dei documenti.

```
description: >-
 ##Title: LaunchInstanceAndCheckState

 Purpose: This Automation runbook first launches an EC2 instance
 using the AMI ID provided in the parameter ``imageId``. The second step of
 this document continuously checks the instance status check value for the
 launched instance until the status ``ok`` is returned.

 ##Parameters:

 Name | Type | Description | Default Value

 ----- | ----- | ----- | -----

 assumeRole | String | (Optional) The ARN of the role that allows Automation to
 perform the actions on your behalf. | -

 imageId | String | (Optional) The AMI ID to use for launching the instance.
 The default value uses the latest Amazon Linux AMI ID available. | {{
 ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-x86_64 }}
schemaVersion: '0.3'
assumeRole: 'arn:aws:iam::111122223333::role/AutomationServiceRole'
parameters:
 imageId:
 type: String
 default: '{{ ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-
x86_64 }}'
 description: >-
 (Optional) The AMI ID to use for launching the instance. The default value
 uses the latest released Amazon Linux AMI ID.
 tagValue:
 type: String
 default: ' LaunchedBySsmAutomation'
 description: >-
```



(Optional) The tag value to add to the instance. The default value is `LaunchedBySsmAutomation`.

`instanceType:`

`type: String`

`default: t2.micro`

`description: >-`

(Optional) The instance type to use for the instance. The default value is `t2.micro`.

`mainSteps:`

- `name: LaunchEc2Instance`

`action: 'aws:executeScript'`

`outputs:`

- `Name: payload`

`Selector: $.Payload`

`Type: StringMap`

`inputs:`

`Runtime: python3.11`

`Handler: launch_instance`

`Script: ''`

`InputPayload:`

`image_id: '{{ imageId }}'`

`tag_value: '{{ tagValue }}'`

`instance_type: '{{ instanceType }}'`

`Attachment: launch.py`

`description: >-`

`**About This Step**`

This step first launches an EC2 instance using the `aws:executeScript` action and the provided python script.

- `name: WaitForInstanceStatusOk`

`action: 'aws:executeScript'`

`inputs:`

`Runtime: python3.11`

`Handler: poll_instance`

`Script: |-`

`def poll_instance(events, context):`

`import boto3`

`import time`

`ec2 = boto3.client('ec2')`

`instance_id = events['InstanceId']`

```

print('[INFO] Waiting for instance status check to report ok', instance_id)

instance_status = "null"

while True:
 res = ec2.describe_instance_status(InstanceIds=[instance_id])

 if len(res['InstanceStatuses']) == 0:
 print("Instance status information is not available yet")
 time.sleep(5)
 continue

 instance_status = res['InstanceStatuses'][0]['InstanceStatus']['Status']

 print('[INFO] Polling to get status of the instance', instance_status)

 if instance_status == 'ok':
 break

 time.sleep(10)

 return {'Status': instance_status, 'InstanceId': instance_id}
InputPayload: '{{ LaunchEc2Instance.payload }}'
description: >-
 About This Step

```

The python script continuously polls the instance status check value for the instance launched in Step 1 until the ``ok`` status is returned.

files:

```

launch.py:
checksums:
 sha256: 18871b1311b295c43d0f...[truncated]...772da97b67e99d84d342ef4aEXAMPLE

```

## Esempi di gestione sicura dei parametri

Gli esempi seguenti illustrano la gestione sicura dei parametri mediante variabili `interpolationType` di ambiente.

## Esecuzione sicura dei comandi di base

Questo esempio mostra come gestire in modo sicuro un parametro di comando:

 Note

`allowedPattern` non è tecnicamente necessario, se un documento SSM non utilizza le doppie parentesi graffe: `{{ }}`

## YAML

```

schemaVersion: '2.2'
description: An example document.
parameters:
 Message:
 type: String
 description: "Message to be printed"
 default: Hello
 interpolationType: ENV_VAR
 allowedPattern: "^[^"]*$"
mainSteps:
- action: aws:runShellScript
 name: printMessage
 precondition:
 StringEquals:
 - platformType
 - Linux
 inputs:
 runCommand:
 - echo {{Message}}
```

## JSON

```
{
 "schemaVersion": "2.2",
 "description": "An example document.",
 "parameters": {
 "Message": {
 "type": "String",
 "description": "Message to be printed",
 "default": "Hello",
 "interpolationType": "ENV_VAR",
 "allowedPattern": "^[^"]*$"
```

```

 }
 },
 "mainSteps": [{
 "action": "aws:runShellScript",
 "name": "printMessage",
 "precondition": {
 "StringEquals": ["platformType", "Linux"]
 },
 "inputs": {
 "runCommand": [
 "echo {{Message}}"
]
 }
 }]
}

```

## Utilizzo dei parametri nei linguaggi interpretati

Questo esempio dimostra la gestione sicura dei parametri in Python:

### YAML

```

schemaVersion: '2.2'
description: 'Secure Python script execution'
parameters:
 inputData:
 type: String
 description: 'Input data for processing'
 interpolationType: 'ENV_VAR'
mainSteps:
- action: aws:runPowerShellScript
 name: runPython
 inputs:
 runCommand:
 - |
 python3 -c '
 import os
 import json

 # Safely access parameter through environment variable
 input_data = os.environ.get("SSM_inputData", "")

```

```
Process the data
try:
 processed_data = json.loads(input_data)
 print(f"Successfully processed: {processed_data}")
except json.JSONDecodeError:
 print("Invalid JSON input")
,
```

## Esempio di compatibilità retroattiva

Questo esempio mostra come gestire i parametri in modo sicuro mantenendo la compatibilità retroattiva:

### YAML

```

schemaVersion: '2.2'
description: 'Backwards compatible secure parameter handling'
parameters:
 userInput:
 type: String
 description: 'User input to process'
 interpolationType: 'ENV_VAR'
 allowedPattern: '^[^"]*$'

mainSteps:
 - action: aws:runShellScript
 name: processInput
 inputs:
 runCommand:
 - |
 # Handle both modern and legacy agent versions
 if [-z "${SSM_userInput+x}"]; then
 # Legacy agent - fall back to direct parameter reference
 export SSM_userInput="{{userInput}}"
 fi

 # Process the input securely
 echo "Processing input: $SSM_userInput"
```

 Note

`allowedPattern` non è tecnicamente necessario, se un documento SSM non utilizza le doppie parentesi graffe: `{{ }}`

## Best practice sulla sicurezza dei parametri

È necessario seguire queste best practice, quando si gestiscono i parametri nei documenti SSM:

- Utilizzo dell'interpolazione delle variabili di ambiente: usare sempre `interpolationType`: "ENV\_VAR" per i parametri di stringa che verranno utilizzati nelle esecuzioni dei comandi.
- Implementazione della convalida dell'input: usare `allowedPattern` per limitare i valori dei parametri a modelli sicuri.
- Gestione dei sistemi legacy: includere la logica di fallback per le versioni SSM Agent precedenti, che non supportano l'interpolazione delle variabili di ambiente.
- Evitare i caratteri speciali: quando si utilizzano i valori dei parametri nei comandi, evitare adeguatamente i caratteri speciali, per impedire che la shell li interpreti.
- Limitazione dell'ambito dei parametri: utilizzare i modelli di parametri più restrittivi possibili per il proprio caso d'uso.

## Elementi di dati e parametri

Questo argomento descrive gli elementi di dati utilizzati nei documenti SSM. La versione dello schema utilizzata per creare un documento definisce la sintassi e gli elementi di dati accettati. Per i documenti di comando è consigliabile utilizzare la versione dello schema 2.2 o successiva. I runbook Automation utilizzano la versione dello schema 0.3. Inoltre, i runbook di Automation supportano l'uso di Markdown, un linguaggio di markup, che consente di aggiungere descrizioni in stile wiki ai documenti e ai singoli passaggi all'interno del documento. Per ulteriori informazioni sull'utilizzo di Markdown, consulta [Utilizzo di Markdown nella console](#) nella Guida alle operazioni di base di Console di gestione AWS .

La sezione seguente descrive gli elementi di dati che si possono includere in un documento SSM.

## Top-level elementi di dati

### schemaVersion

La versione dello schema da utilizzare.

Tipo: Versione

Obbligatorio: sì

### description

Le informazioni fornite per descrivere lo scopo del documento. È inoltre possibile utilizzare questo campo per specificare se un parametro richiede un valore per l'esecuzione di un documento o se è facoltativo fornire un valore per il parametro. I parametri obbligatori e facoltativi possono essere visualizzati negli esempi in questo argomento.

─Tipo: stringa

Obbligatorio: no

### parametri

Una struttura che definisce i parametri accettati dal documento.

Per una maggiore sicurezza durante la gestione dei parametri delle stringhe, è possibile utilizzare l'interpolazione delle variabili di ambiente specificando la proprietà di `interpolationType`. Se impostato su `ENV_VAR`, l'agente crea una variabile di ambiente denominata `SSM_parameter-name`, che contiene il valore del parametro.

Di seguito è riportato un esempio di parametro che utilizza una variabile di ambiente di `interpolationType`:

```
{
 "schemaVersion": "2.2",
 "description": "An example document.",
 "parameters": {
 "Message": {
 "type": "String",
 "description": "Message to be printed",
 "default": "Hello",
 "interpolationType" : "ENV_VAR",
 "allowedPattern": "^[^"]*$"
```

```
 }
 },
 "mainSteps": [{
 "action": "aws:runShellScript",
 "name": "printMessage",
 "precondition" : {
 "StringEquals" : ["platformType", "Linux"]
 },
 "inputs": {
 "runCommand": [
 "echo {{Message}}"
]
 }
]
}
```

#### Note

`allowedPattern` non è tecnicamente necessario, se un documento SSM non utilizza le doppie parentesi graffe: `{{ }}`

Per i parametri che usi spesso, ti consigliamo di memorizzarli in Parameter Store. Puoi quindi definire i parametri nel tuo documento che si riferiscono ai parametri Parameter Store come valore predefinito. Per fare riferimento al parametro Parameter Store, utilizza la sintassi seguente.

```
{{ssm:parameter-name}}
```

È possibile utilizzare un parametro che fa riferimento al parametro Parameter Store allo stesso modo di qualsiasi altro parametro del documento. Nell'esempio seguente, il valore predefinito per il parametro `commands` è il valore del parametro Parameter Store `myShellCommands`. Specificando il valore del parametro `commands` come stringa `runCommand`, il documento esegue i comandi memorizzati nel parametro `myShellCommands`.

#### YAML

```

schemaVersion: '2.2'
description: runShellScript with command strings stored as Parameter Store
parameter
```



```

parameters:
 commands:
 type: StringList
 description: "(Required) The commands to run on the instance."
 default: ["{{ ssm:myShellCommands }}"],
 interpolationType : 'ENV_VAR'
 allowedPattern: '^^[^"]*$'

mainSteps:
- action: aws:runShellScript
 name: runShellScriptDefaultParams
 inputs:
 runCommand:"{{ commands }}"

```

## JSON

```

{
 "schemaVersion": "2.2",
 "description": "runShellScript with command strings stored as Parameter Store parameter",
 "parameters": {
 "commands": {
 "type": "StringList",
 "description": "(Required) The commands to run on the instance.",
 "default": ["{{ ssm:myShellCommands }}"],
 "interpolationType" : "ENV_VAR"
 }
 },
 "mainSteps": [
 {
 "action": "aws:runShellScript",
 "name": "runShellScriptDefaultParams",
 "inputs": {
 "runCommand": [
 "{{ commands }}"
]
 }
 }
]
}

```

 Note

Puoi fare riferimento ai parametri `String`, `StringList` e `Parameter Store` nella sezione `parameters` del documento. Non si può fare riferimento ai parametri `SecureString` `Parameter Store`.

Per ulteriori informazioni su `Parameter Store`, consultare [AWS Systems Manager Parameter Store](#).

Tipo: Struttura

La struttura `parameters` accetta i seguenti campi e valori:

- `type`: (Obbligatorio) I valori consentiti sono i seguenti: `String`, `StringList`, `Integer`, `Boolean`, `MapList` e `StringMap`. Per visualizzare esempi di ciascun tipo, consulta [Esempi di tipi di parametri di documento SSM](#) nella sezione successiva.

 Note

I documenti di tipo di comando supportano solo i tipi di parametri `String` e `StringList`.

- `description`: (facoltativo) una descrizione del parametro.
- `default`: (facoltativo) il valore predefinito del parametro o un riferimento a un parametro in `Parameter Store`.
- `allowedValues`: (facoltativo) una matrice dei valori consentiti per il parametro. La definizione dei valori consentiti per il parametro convalida l'input dell'utente. Se un utente inserisce un valore non consentito, l'esecuzione non viene avviata.

YAML

```
DirectoryType:
 type: String
 description: "(Required) The directory type to launch."
 default: AwsMad
 allowedValues:
 - AdConnector
 - AwsMad
 - SimpleAd
```

## JSON

```
"DirectoryType": {
 "type": "String",
 "description": "(Required) The directory type to launch.",
 "default": "AwsMad",
 "allowedValues": [
 "AdConnector",
 "AwsMad",
 "SimpleAd"
]
}
```

- **allowedPattern:** (facoltativo) un'espressione regolare che convalida se l'input dell'utente corrisponde al modello definito per il parametro. Se l'input dell'utente non corrisponde al modello consentito, l'esecuzione non viene avviata.



### Note

Systems Manager esegue due convalide per **allowedPattern**. La prima convalida viene eseguita utilizzando la [libreria Java regex](#) a livello di API quando si utilizza un documento. La seconda convalida viene eseguita su SSM Agent utilizzando la [libreria di GO regexp](#) prima di elaborare il documento.

## YAML

```
InstanceId:
 type: String
 description: "(Required) The instance ID to target."
 allowedPattern: "^i-(?:[a-f0-9]{8}|[a-f0-9]{17})$"
 default: ''
```

## JSON

```
"InstanceId": {
 "type": "String",
 "description": "(Required) The instance ID to target.",
 "allowedPattern": "^i-(?:[a-f0-9]{8}|[a-f0-9]{17})$",
 "default": ""
```

```
}
```

- **displayType:** (Facoltativo) Utilizzato per visualizzare a `textField` o `textarea` a nel Console di gestione AWS. `textField` è una casella di testo a riga singola. `textarea` è un'area di testo a più righe.
- **minItems:** (facoltativo) il numero minimo di elementi consentiti.
- **maxItems:** (facoltativo) il numero massimo di elementi consentiti.
- **minChars:** (facoltativo) il numero minimo di caratteri del parametro consentiti.
- **maxChars:** (facoltativo) il numero massimo di caratteri del parametro consentiti.
- **interpolationType:** (facoltativo) definisce come i valori dei parametri vengono elaborati prima dell'esecuzione del comando. Se impostato su `ENV_VAR`, il valore del parametro viene reso disponibile come variabile di ambiente denominata `SSM_parameter-name`. Questa funzionalità previene l'iniezione di comandi trattando i valori di parametro come stringhe letterali.

Tipo: stringa

Valori validi: `ENV_VAR`

Campo obbligatorio: no

## variables

(Solo versione 0.3 dello schema) Valori a cui è possibile fare riferimento o da aggiornare durante i passaggi di un runbook Automation. Le variabili sono simili ai parametri, ma presentano una differenza molto rilevante. Nel contesto di un runbook, i valori dei parametri sono statici mentre quelli delle variabili possono essere modificati. Quando si aggiorna il valore di una variabile, il tipo di dati deve corrispondere al tipo di dati definito. Per informazioni sull'aggiornamento dei valori delle variabili in un'automazione, consulta la pagina [aws:updateVariable: aggiorna un valore per una variabile di runbook](#)

Tipo: Boolean | Integer | | String | | MapList StringList StringMap

Obbligatorio: no

YAML

```
variables:
 payload:
```

```
type: StringMap
default: "{}"
```

## JSON

```
{
 "variables": [
 "payload": {
 "type": "StringMap",
 "default": "{}"
 }
]
}
```

## runtimeConfig

(Solo versione dello schema 1.2) La configurazione per l'istanza applicata da uno o più plugin di Systems Manager. Non è garantito che l'esecuzione dei plugin avvenga in sequenza.

Tipo: Dictionary<String, > PluginConfiguration

Obbligatorio: no

## mainSteps

(Solo versione dello schema 0.3, 2.0 e 2.2) Un oggetto che può includere più fasi (plugin). I plugin sono definiti all'interno delle fasi. Le fasi vengono eseguite nell'ordine sequenziale indicato nel documento.

Tipo: Dictionary<String, > PluginConfiguration

Obbligatorio: sì

## outputs

(Solo versione dello schema 0.3) Dati generati dall'esecuzione di questo documento che possono essere utilizzati in altri processi. Ad esempio, se il documento ne crea uno nuovoAMI, puoi specificare "CreateImage.ImageId" come valore di output e quindi utilizzare questo output per creare nuove istanze in una successiva esecuzione di automazione. Per ulteriori informazioni sugli output, consulta [Utilizzo degli output delle operazioni come input](#).

Digitare: Dictionary<String, > OutputConfiguration

Obbligatorio: no

## files

(Solo versione dello schema 0.3) I file di script (e i relativi checksum) collegati al documento ed eseguiti durante un'esecuzione dell'automazione. Si applica solo ai documenti che includono l'operazione `aws:executeScript` e per i quali gli allegati sono stati specificati in una o più fasi.

Per ulteriori informazioni sui runtime supportati dai runbook Automation, vedere [aws:ExecuteScript – Esegue uno script](#). Per ulteriori informazioni sull'inclusione di script nei runbook Automation, consultare [Utilizzo di script nei runbook](#) e [Esperienza di progettazione visiva per i runbook Automation](#).

Quando si crea un runbook di automazione con allegati, è inoltre necessario specificare i file allegati utilizzando l' `--attachments` opzione (per AWS CLI) o `Attachments` (per API e SDK). È possibile specificare la posizione del file sia per i documenti SSM che per i file archiviati nei bucket Amazon Simple Storage Service (Amazon S3). Per ulteriori informazioni, consulta [Allegati](#) nell'API Reference. AWS Systems Manager

## YAML

```

files:
 launch.py:
 checksums:
 sha256: 18871b1311b295c43d0f...
[truncated]...772da97b67e99d84d342ef4aEXAMPLE
```

## JSON

```
{
 "files": {
 "launch.py": {
 "checksums": {
 "sha256": "18871b1311b295c43d0f...
[truncated]...772da97b67e99d84d342ef4aEXAMPLE"
 }
 }
 }
}
```

Digita: Dictionary<String, > FilesConfiguration

Obbligatorio: no

## Esempi di tipi di parametri di documento SSM

I tipi di parametri nei documenti SSM sono statici. Ciò significa che il tipo di parametro non può essere modificato dopo che è stato definito. Quando si utilizzano parametri con plugin del documento SSM, il tipo di parametro non può essere modificato dinamicamente all'interno dell'input di un plugin. Ad esempio, non è possibile fare riferimento a un parametro `Integer` all'interno dell'input `runCommand` del plugin `aws:runShellScript` perché questo input accetta una stringa o un elenco di stringhe. Per utilizzare un parametro per un input di plugin, il tipo di parametro deve corrispondere al tipo accettato. Ad esempio, è necessario specificare un tipo di parametro `Boolean` per l'input `allowDowngrade` del plugin `aws:updateSsmAgent`. Se il tipo di parametro non corrisponde al tipo di input per un plugin, il documento SSM non viene convalidato e il sistema non crea il documento. Ciò vale anche quando si utilizzano parametri a valle all'interno degli input per altri plugin o azioni di automazione. AWS Systems Manager Ad esempio, non è possibile fare riferimento a un parametro di `StringList` nell'input `documentParameters` del plugin `aws:runDocument`. L'input di `documentParameters` accetta una mappa di stringhe anche se il tipo di parametro del documento SSM a valle è un parametro `StringList` e corrisponde al parametro a cui si fa riferimento.

Quando si utilizzano parametri con operazioni di automazione di , nella maggior parte dei casi i tipi di parametro non vengono convalidati quando si crea il documento SSM. Solo quando si utilizza l'operazione `aws:runCommand`, i tipi di parametro vengono convalidati quando si crea il documento SSM. In tutti gli altri casi, la convalida dei parametri avviene durante l'esecuzione dell'automazione quando l'input di un'operazione viene verificato prima dell'esecuzione. Ad esempio, se il parametro di input è `String` e si fa riferimento ad esso come valore per l'input `MaxInstanceCount` dell'operazione `aws:runInstances`, viene creato il documento SSM. Tuttavia, quando si esegue il documento, l'automazione non riesce durante la convalida dell'operazione `aws:runInstances` perché l'input `MaxInstanceCount` richiede un valore `Integer`.

Di seguito sono riportati alcuni esempi di ciascun parametro type.

### Stringa

Una sequenza di zero o più caratteri Unicode inclusa tra virgolette. Ad esempio, `"i-1234567890abcdef0"`. Utilizza barre rovesciate come caratteri di escape.

I parametri di stringa possono includere un campo di `interpolationType` opzionale con il valore `ENV_VAR`, per abilitare l'interpolazione delle variabili di ambiente per una maggiore sicurezza.

## YAML

```

InstanceId:
 type: String
 description: "(Optional) The target EC2 instance ID."
 interpolationType: ENV_VAR
```

## JSON

```
"InstanceId":{
 "type":"String",
 "description":"(Optional) The target EC2 instance ID.",
 "interpolationType": "ENV_VAR"
}
```

## StringList

Un elenco di elementi String separati da virgole. Ad esempio, ["cd ~", "pwd"].

## YAML

```

commands:
 type: StringList
 description: "(Required) Specify a shell script or a command to run."
 default: ""
 minItems: 1
 displayType: textarea
```

## JSON

```
"commands":{
 "type":"StringList",
 "description":"(Required) Specify a shell script or a command to run.",
 "minItems":1,
 "displayType":"textarea"
}
```

## Booleano

Accetta solo true o false. Non accetta "true" o 0.



## YAML

```

canRun:
 type: Boolean
 description: ''
 default: true
```

## JSON

```
"canRun": {
 "type": "Boolean",
 "description": "",
 "default": true
}
```

## Numero intero

Numeri interi. Non accetta numeri decimali, ad esempio 3,14159, o numeri inclusi tra virgolette, ad esempio "3".

## YAML

```

timeout:
 type: Integer
 description: The type of action to perform.
 default: 100
```

## JSON

```
"timeout": {
 "type": "Integer",
 "description": "The type of action to perform.",
 "default": 100
}
```

## StringMap

Mappatura di chiavi a valori. Le chiavi e i valori devono essere stringhe. Ad esempio, {"Env": "Prod"}.

## YAML

```

notificationConfig:
 type: StringMap
 description: The configuration for events to be notified about
 default:
 NotificationType: 'Command'
 NotificationEvents:
 - 'Failed'
 NotificationArn: "$dependency.topicArn"
 maxChars: 150
```

## JSON

```
"notificationConfig" : {
 "type" : "StringMap",
 "description" : "The configuration for events to be notified about",
 "default" : {
 "NotificationType" : "Command",
 "NotificationEvents" : ["Failed"],
 "NotificationArn" : "$dependency.topicArn"
 },
 "maxChars" : 150
}
```

## MapList

Un elenco di oggetti. StringMap

## YAML

```
blockDeviceMappings:
 type: MapList
 description: The mappings for the create image inputs
 default:
 - DeviceName: "/dev/sda1"
 Ebs:
 VolumeSize: "50"
 - DeviceName: "/dev/sdm"
 Ebs:
 VolumeSize: "100"
 maxItems: 2
```

## JSON

```
"blockDeviceMappings":{
 "type":"MapList",
 "description":"The mappings for the create image inputs",
 "default":[
 {
 "DeviceName":"/dev/sda1",
 "Ebs":{"
 "VolumeSize":"50"
 }
 },
 {
 "DeviceName":"/dev/sdm",
 "Ebs":{"
 "VolumeSize":"100"
 }
 }
],
 "maxItems":2
}
```

### Visualizzazione del contenuto del documento Command SSM

Per visualizzare in anteprima i parametri obbligatori e facoltativi di un documento AWS Systems Manager (SSM) Command, oltre alle azioni eseguite dal documento, è possibile visualizzare il contenuto del documento nella console di Systems Manager.

Per visualizzare il contenuto del documento Command SSM

1. Aprire la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Documenti.
3. Nella casella di ricerca selezionare Document type (Tipo di documento) e quindi selezionare Command (Comando).
4. Scegli il nome di un documento, quindi la scheda Contenuto.
5. Nel campo del contenuto esaminare i parametri e i passaggi delle operazioni disponibili per il documento.

Ad esempio, l'immagine seguente mostra che (1) `version` e (2) `allowDowngrades` sono parametri opzionali per il documento `AWS-UpdateSSMAgent` e che la prima operazione eseguita dal documento è (3) `aws:updateSsmAgent`.



## Documentazione di riferimento del plugin per i documenti di comando

Questo riferimento descrive i plugin che è possibile specificare in un documento di tipo Command AWS Systems Manager (SSM). Questi plugin non possono essere utilizzati nei runbook Automation SSM che usano operazioni di Automation. Per informazioni sulle azioni di AWS Systems Manager automazione, consulta [Riferimento alle operazioni del servizio di automazione di Systems Manager](#)

Systems Manager determina le operazioni da eseguire su un'istanza gestita mediante la lettura dei contenuti di un documento SSM. Ogni documento include una sezione di esecuzione di codice. A seconda della versione dello schema del documento, questa sezione di esecuzione di codice può includere uno o più plugin o fasi. Ai fini di questo argomento della Guida, i plugin e le fasi sono chiamati plugin. Questa sezione include informazioni su ciascun plugin di Systems Manager. Per ulteriori informazioni sui documenti, incluse informazioni sulla creazione di documenti e sulle differenze tra le versioni dello schema, consulta [AWS Systems Manager Documenti di](#).

Per i plugin che accettano parametri String, come `aws:runShellScript` e `aws:runPowerShellScript`, il parametro `interpolationType` è utilizzabile per migliorare la sicurezza trattando gli input dei parametri come stringhe letterali, invece di comandi potenzialmente eseguibili. Ad esempio:

```
{
```

```
"schemaVersion": "2.2",
"description": "runShellScript with command strings stored as Parameter Store
parameter",
"parameters": {
 "commands": {
 "type": "StringList",
 "description": "(Required) The commands to run on the instance.",
 "default": ["{{ ssm:myShellCommands }}"],
 "interpolationType" : "ENV_VAR"
 }
},
//truncated
}
```

#### Note

Alcuni dei plugin illustrati in questa sezione possono essere eseguiti soltanto su istanze Windows Server o Linux. Sono riportate le dipendenze della piattaforma per ogni plugin. I seguenti plugin di documenti sono supportati nelle istanze di Amazon Elastic Compute Cloud (Amazon EC2) per macOS:

- `aws:refreshAssociation`
- `aws:runShellScript`
- `aws:runPowerShellScript`
- `aws:softwareInventory`
- `aws:updateSsmAgent`

## Indice

- [Input condivisi](#)
- [aws:applications](#)
- [aws:cloudWatch](#)
- [aws:configureDocker](#)
- [aws:configurePackage](#)
- [aws:domainJoin](#)
- [aws:downloadContent](#)

- [aws:psModule](#)
- [aws:refreshAssociation](#)
- [aws:run DockerAction](#)
- [aws:runDocument](#)
- [aws: esegui PowerShellScript](#)
- [aws: run ShellScript](#)
- [aws:softwareInventory](#)
- [aws:updateAgent](#)
- [aws: aggiornamento SsmAgent](#)

## Input condivisi

Solo con la versione 3.0.502 e successive di SSM Agent tutti i plugin possono utilizzare i seguenti input:

### finallyStep

L'ultimo passaggio è l'esecuzione del documento. Se questo input è definito per un passaggio, ha la precedenza su un valore `exit` specificato negli input `onFailure` o `onSuccess`. Affinché un passaggio con questo input venga eseguito come previsto, deve essere `mainSteps`ultimo definito nel documento.

Tipo: Booleano

Valori validi: `true` | `false`

Obbligatorio: no

### onFailure

Se si specifica questo input per un plugin con il valore `exit` e il passaggio non riesce, lo stato del passaggio riflette l'errore e il documento non esegue i passaggi rimanenti a meno che non sia stato definito un `finallyStep`. Se si specifica questo input per un plugin con il valore `successAndExit` e il passaggio non riesce, lo stato del passaggio riflette l'errore e il documento non esegue i passaggi rimanenti a meno che non sia stato definito un `finallyStep`.

Tipo: stringa

Valori validi: `exit` | `successAndExit`

Obbligatorio: no

## onSuccess

Se si specifica questo input per un plugin e il passaggio viene eseguito correttamente, il documento non esegue i passaggi rimanenti a meno che non sia stato definito un `finallyStep`.

Tipo: stringa

Valori validi: `exit`

Campo obbligatorio: no

## YAML

```

schemaVersion: '2.2'
description: Shared inputs example
parameters:
 customDocumentParameter:
 type: String
 description: Example parameter for a custom Command-type document.
mainSteps:
- action: aws:runDocument
 name: runCustomConfiguration
 inputs:
 documentType: SSMDocument
 documentPath: "yourCustomDocument"
 documentParameters: '"documentParameter":{{customDocumentParameter}}'
 onSuccess: exit
- action: aws:runDocument
 name: ifConfigurationFailure
 inputs:
 documentType: SSMDocument
 documentPath: "yourCustomRepairDocument"
 onFailure: exit
- action: aws:runDocument
 name: finalConfiguration
 inputs:
 documentType: SSMDocument
 documentPath: "yourCustomFinalDocument"
```

```
finallyStep: true
```

## JSON

```
{
 "schemaVersion": "2.2",
 "description": "Shared inputs example",
 "parameters": {
 "customDocumentParameter": {
 "type": "String",
 "description": "Example parameter for a custom Command-type document."
 }
 },
 "mainSteps": [
 {
 "action": "aws:runDocument",
 "name": "runCustomConfiguration",
 "inputs": {
 "documentType": "SSMDocument",
 "documentPath": "yourCustomDocument",
 "documentParameters": "\"documentParameter\": {{customDocumentParameter}}",
 "onSuccess": "exit"
 }
 },
 {
 "action": "aws:runDocument",
 "name": "ifConfigurationFailure",
 "inputs": {
 "documentType": "SSMDocument",
 "documentPath": "yourCustomRepairDocument",
 "onFailure": "exit"
 }
 },
 {
 "action": "aws:runDocument",
 "name": "finalConfiguration",
 "inputs": {
 "documentType": "SSMDocument",
 "documentPath": "yourCustomFinalDocument",
 "finallyStep": true
 }
 }
]
}
```



```
]
}
```

## aws:applications

Installa, ripara o disinstalla applicazioni su un'istanza EC2. Questo plugin può essere eseguito solo su sistemi operativi Windows Server.

### Sintassi

### Schema 2.2

### YAML

```

schemaVersion: '2.2'
description: aws:applications plugin
parameters:
 source:
 description: "(Required) Source of msi."
 type: String
mainSteps:
- action: aws:applications
 name: example
 inputs:
 action: Install
 source: "{{ source }}"
```

### JSON

```
{
 "schemaVersion": "2.2",
 "description": "aws:applications",
 "parameters": {
 "source": {
 "description": "(Required) Source of msi.",
 "type": "String"
 }
 },
 "mainSteps": [
 {
 "action": "aws:applications",
```

```
 "name": "example",
 "inputs": {
 "action": "Install",
 "source": "{{ source }}"
 }
 }
]
```

## Schema 1.2

### YAML

```

runtimeConfig:
 aws:applications:
 properties:
 - id: 0.aws:applications
 action: "{{ action }}"
 parameters: "{{ parameters }}"
 source: "{{ source }}"
 sourceHash: "{{ sourceHash }}"
```

### JSON

```
{
 "runtimeConfig": {
 "aws:applications": {
 "properties": [
 {
 "id": "0.aws:applications",
 "action": "{{ action }}",
 "parameters": "{{ parameters }}",
 "source": "{{ source }}",
 "sourceHash": "{{ sourceHash }}"
 }
]
 }
 }
}
```

## Properties

### operazione

L'operazione da eseguire.

Tipo: Enum

Valori validi: Install | Repair | Uninstall

Obbligatorio: sì

### parametri

I parametri per il programma di installazione.

Tipo: stringa

Obbligatorio: no

### origine

L'URL del file .msi per l'applicazione.

Tipo: stringa

Obbligatorio: sì

### sourceHash

L'hash SHA256 del file .msi.

■Tipo: stringa

Obbligatorio: no

## aws:cloudWatch

Esporta dati Windows Server da Amazon CloudWatch o Amazon CloudWatch Logs e monitora i dati utilizzando CloudWatch metriche. Questo plugin può essere eseguito solo su sistemi operativi Windows Server. Per ulteriori informazioni sulla configurazione CloudWatch dell'integrazione con Amazon Elastic Compute Cloud (Amazon EC2), consulta [Collecting metrics, logs and trace with the CloudWatch agent](#) nella Amazon User Guide. CloudWatch

 Important

L' CloudWatch agente unificato è stato sostituito SSM Agent come strumento per l'invio di dati di log ad Amazon Logs. CloudWatch Il plugin aws:cloudWatch SSM Agent non è supportato. Ti consigliamo di utilizzare solo l' CloudWatch agente unificato per i processi di raccolta dei log. Per ulteriori informazioni, consulta i seguenti argomenti:

- [Invio dei log dei nodi a CloudWatch registri unificati \(CloudWatch agente\)](#)
- [Esegui la migrazione della raccolta di log dei nodi di Windows Server all'agente CloudWatch](#)
- [Raccolta di metriche, log e tracce con l' CloudWatch agente](#) nella Amazon CloudWatch User Guide.

Puoi esportare e monitorare i seguenti tipi di dati:

#### ApplicationEventLog

Invia i dati del registro degli eventi dell'applicazione a CloudWatch Logs.

#### CustomLogs

Invia qualsiasi file di registro basato su testo ad Amazon CloudWatch Logs. Il CloudWatch plugin crea un'impronta digitale per i file di registro. Quindi, il sistema associa un offset dei dati con ciascun ID digitale. Il plugin carica i file quando sono presenti modifiche, registra l'offset e lo associa a un ID digitale. Questo metodo viene utilizzato per evitare una situazione in cui un utente attiva il plugin, associa il servizio a una directory che contiene un numero elevato di file e il sistema carica tutti i file.

 Warning

Se l'applicazione tronca o tenta di eliminare i log durante il polling, qualsiasi log specificato per LogDirectoryPath può perdere voci. Se, ad esempio, desideri limitare le dimensioni del file di log, devi creare un nuovo file di log quando viene raggiunto il limite, quindi devi continuare a scrivere i dati sul nuovo file.

#### ETW

Invia i dati di Event Tracing for Windows (ETW) ai registri. CloudWatch

## IIS

Invia i dati di registro IIS ai CloudWatch registri.

## PerformanceCounter

Invia i contatori delle prestazioni di Windows a CloudWatch. Puoi selezionare diverse categorie in cui caricare CloudWatch come metriche. Per ogni contatore delle prestazioni che desideri caricare, crea una PerformanceCounter sezione con un ID univoco (ad esempio "PerformanceCounter2", "PerformanceCounter 3" e così via) e configurane le proprietà.

### Note

Se il AWS Systems Manager SSM Agent CloudWatch plug-in viene interrotto, i dati del contatore delle prestazioni non vengono registrati. CloudWatch Questo comportamento è diverso rispetto ai log personalizzati o ai log di eventi di Windows. I registri personalizzati e i registri degli eventi di Windows conservano i dati dei contatori delle prestazioni e li caricano su CloudWatch dopo SSM Agent che il CloudWatch plug-in è disponibile.

## SecurityEventLog

Invia i dati del registro degli eventi di sicurezza ai CloudWatch registri.

## SystemEventLog

Invia i dati del registro degli eventi di sistema a CloudWatch Logs.

Puoi definire le seguenti destinazioni per i dati:

### CloudWatch

La destinazione in cui vengono inviati i dati dei parametri del contatore delle prestazioni. Puoi aggiungere altre sezioni con ID univoci (ad esempio, "CloudWatch2", "CloudWatch 3" e così via) e specificare una regione diversa per ogni nuovo ID per inviare gli stessi dati a località diverse.

### CloudWatchLogs

La destinazione in cui vengono inviati i dati di log. Puoi aggiungere altre sezioni con ID univoci (ad esempio "CloudWatchLogs2", "CloudWatchLogs3" e così via) e specificare una regione diversa per ogni nuovo ID per inviare gli stessi dati a località diverse.

## Sintassi

```
"runtimeConfig":{
 "aws:cloudWatch":{
 "settings":{
 "startType":"{{ status }}"
 },
 "properties":"{{ properties }}"
 }
}
```

## Impostazioni e proprietà

### AccessKey

L'ID chiave di accesso . Questa proprietà è obbligatoria, a meno che l'utente non abbia avviato l'istanza usando un ruolo IAM. Questa proprietà non può essere utilizzata con SSM.

─Tipo: stringa

Obbligatorio: no

### CategoryName

La categoria del contatore delle prestazioni da Performance Monitor.

Tipo: stringa

Obbligatorio: sì

### CounterName

Il nome del contatore delle prestazioni da Performance Monitor.

Tipo: stringa

Obbligatorio: sì

### CultureName

L'impostazione locale in cui viene registrato il timestamp. Se `CultureName` è vuoto, per impostazione predefinita viene utilizzata la stessa lingua utilizzata dall'istanza. Windows Server

Tipo: stringa

Valori validi: per un elenco dei valori supportati, consulta [National Language Support \(NLS\)](#) sul sito Web Microsoft. I valori div, div-MV, hu e hu-HU non sono supportati.

Obbligatorio: no

### DimensionName

Una dimensione per la tua metrica Amazon CloudWatch . Se specifichi DimensionName, devi specificare DimensionValue. Questi parametri forniscono un'altra vista al momento della creazione di elenchi di parametri. Puoi utilizzare la stessa dimensione per più parametri per poter visualizzare tutti i parametri appartenenti a una dimensione specifica.

─Tipo: stringa

Obbligatorio: no

### DimensionValue

Un valore di dimensione per la tua CloudWatch metrica Amazon.

─Tipo: stringa

Obbligatorio: no

### Encoding

La codifica del file da utilizzare (ad esempio, UTF-8). Utilizza il nome di codifica, non il nome di visualizzazione.

Tipo: stringa

Valori validi: per un elenco dei valori supportati, consulta l'argomento relativo alla [classe di codifica](#) nella libreria di Microsoft Learn.

Obbligatorio: sì

### Filtro

Il prefisso dei nomi di log. Lascia questo parametro bianco per monitorare tutti i file.

Tipo: stringa

Valori validi: per un elenco dei valori supportati, vedere la [FileSystemWatcherFilter proprietà](#) nella libreria MSDN.

Obbligatorio: no

## Flussi

Ogni tipo di dati da caricare, insieme alla destinazione dei dati (CloudWatch o CloudWatch registri). Ad esempio, per inviare un contatore delle prestazioni definito in "Id": "PerformanceCounter" alla CloudWatch destinazione definita in "Id": "CloudWatch", inserisci "PerformanceCounter". Analogamente, per inviare il log personalizzato, il log ETW e il log di sistema alla destinazione CloudWatch Logs definita in "Id": "ETW", inserisci «(ETW),CloudWatchLogs». Inoltre, puoi inviare lo stesso contatore delle prestazioni o file di log a più destinazioni. Ad esempio, per inviare il log dell'applicazione a due diverse destinazioni definite in "Id": "CloudWatchLogs" e "Id": "CloudWatchLogs2", inserisci "(ApplicationEventLogCloudWatchLogs, CloudWatchLogs2)".

Tipo: stringa

Valori validi (origine): ApplicationEventLog | CustomLogs | ETW | PerformanceCounter | SystemEventLog | SecurityEventLog

Valori validi (destinazione): CloudWatch | CloudWatchLogs | CloudWatch *n* | CloudWatchLogs *n*

Obbligatorio: sì

### FullName

Il nome completo del componente.

Tipo: stringa

Obbligatorio: sì

### Id

Identifica l'origine o la destinazione dei dati. Questo identificatore deve essere univoco all'interno del file di configurazione.

Tipo: stringa

Obbligatorio: sì

### InstanceName

Il nome dell'istanza del contatore delle prestazioni. Non utilizzare un asterisco (\*) per indicare tutte le istanze perché ciascun componente del contatore delle prestazioni supporta solo un parametro. Tuttavia, puoi utilizzare \_Total.



Tipo: stringa

Obbligatorio: sì

## Levels

I tipi di messaggi da inviare ad Amazon CloudWatch.

Tipo: stringa

Valori validi:

- 1: solo i messaggi di errore caricati.
- 2: solo i messaggi di avviso caricati.
- 4: solo i messaggi informativi caricati.

È possibile aggiungere valori per includere più di un tipo di messaggio. Ad esempio, 3 indica che i messaggi di errore (1) e i messaggi di avviso (2) sono inclusi. Un valore pari a 7 indica che i messaggi di errore (1), i messaggi di avviso (2) e i messaggi informativi (4) sono inclusi.

Obbligatorio: sì

### Note

I log di sicurezza di Windows dovrebbero impostare livelli fino a 7.

## LineCount

Il numero di righe dell'intestazione per identificare il file di log. Ad esempio, i file di log IIS dispongono di intestazioni praticamente identiche. Puoi inserire 3, che può leggere le prime tre righe dell'intestazione del file di log per identificarlo. Nei file di log IIS, la terza riga è costituita dalla data e dal timestamp, che è diverso tra i file di log.

Tipo: Integer

Obbligatorio: no

## LogDirectoryPath

Per CustomLogs, il percorso in cui sono archiviati i log sulla tua istanza EC2. Per i log IIS, la cartella in cui sono archiviati i log IIS per un singolo sito (ad esempio, C:\inetpub\logs\LogFiles\W3SVC). **n** Per i log di IIS, è supportato solo il formato di log W3C. I formati IIS, NCSA e quelli personalizzati non sono supportati.

Tipo: stringa

Obbligatorio: sì

## LogGroup

Nome del gruppo di log. Questo nome viene visualizzato sulla schermata Log Groups (Gruppi di log) nella console CloudWatch.

Tipo: stringa

Obbligatorio: sì

## LogName

Nome del file di log.

1. Per individuare il nome del log, in Visualizzatore eventi, nel riquadro di navigazione, scegli Log di applicazioni e servizi.
2. Nell'elenco dei registri, apri il menu contestuale del registro che desideri caricare (ad esempio, Microsoft > > Windows Backup > Operational), quindi seleziona Crea visualizzazione personalizzata.
3. Nella finestra di dialogo Crea visualizzazione personalizzata, scegli la scheda XML. LogNameÈ contenuto nel tag <Select Path=> (ad esempio,). Microsoft-Windows-Backup Copia questo testo nel parametro. LogName

Tipo: stringa

Valori validi: Application| Security| System| Microsoft-Windows-WinINet/Analytic

Obbligatorio: sì

## LogStream

Il flusso di log di destinazione. Se utilizzi {instance\_id}, il valore predefinito, l'ID di questa istanza viene utilizzato come nome del flusso di log.

Tipo: stringa

Valori validi: {instance\_id} | {hostname} | {ip\_address} *<log\_stream\_name>*

Se inserisci un nome di log stream che non esiste già, CloudWatch Logs lo crea automaticamente per te. Puoi utilizzare una stringa letterale o variabili predefinite ({instance\_id}, {hostname}, {ip\_address}) o una combinazione di tutte e tre per definire un nome di flusso di log.

Il nome del flusso di log specificato in questo parametro viene visualizzato nella *<YourLogStream>* schermata Log Groups > Streams for della CloudWatch console.

Obbligatorio: sì

#### MetricName

La CloudWatch metrica in cui desideri includere i dati sulle prestazioni.

##### Note

Non utilizzare caratteri speciali nel nome. In caso contrario, il parametro e gli allarmi associati potrebbero non funzionare.

Tipo: stringa

Obbligatorio: sì

#### NameSpace

Il namespace parametro in cui desideri che vengano scritti i dati dei contatori delle prestazioni.

Tipo: stringa

Obbligatorio: sì

#### PollInterval

Il numero di secondi che devono trascorrere prima che un nuovo contatore delle prestazioni e i dati di log vengano caricati.

Tipo: numero intero

Valori validi: imposta questo valore su 5 o più secondi. Quindici secondi (00:00:15) è il valore consigliato.

Obbligatorio: sì

#### Region

La Regione AWS posizione in cui desideri inviare i dati di registro. Sebbene possa inviare contatori delle prestazioni a una regione diversa rispetto a quella a cui invii i dati di log, è consigliabile impostare questo parametro sulla stessa regione in cui l'istanza è in esecuzione.

Tipo: stringa

Valori validi: ID delle regioni AWS supportati sia da Systems Manager che da CloudWatch Logs - east-2, ad esempio eu-west-1, eap-southeast-1. Per gli elenchi degli endpoint AWS supportati da ciascun servizio, consulta [Amazon CloudWatch Logs Service Endpoints](#) and [Systems Manager](#) nel. Riferimenti generali di Amazon Web Services

Obbligatorio: sì

SecretKey

La chiave di accesso segreta. Questa proprietà è obbligatoria, a meno che l'utente non abbia avviato l'istanza usando un ruolo IAM.

■Tipo: stringa

Obbligatorio: no

startType

Attiva o disattiva l' CloudWatch istanza.

Tipo: stringa

Valori validi: Enabled | Disabled

Obbligatorio: sì

TimestampFormat

Il formato del timestamp che desideri utilizzare. Per un elenco dei valori supportati, consulta l'argomento [Stringhe di formato di data e ora personalizzato](#) nella libreria MSDN.

Tipo: stringa

Obbligatorio: sì

TimeZoneKind

Fornisce le informazioni sul fuso orario se non sono incluse nel timestamp del log. Se questo parametro viene lasciato vuoto e se il timestamp non include informazioni sul fuso orario, CloudWatch Logs utilizza per impostazione predefinita il fuso orario locale. Questo parametro viene ignorato se il timestamp contiene già informazioni sul fuso orario.

Tipo: stringa

Valori validi: Local | UTC

Obbligatorio: no

## Unità

L'unità di misura appropriata per il parametro.

Tipo: stringa

Valori validi: Secondi | Microsecondi | Millisecondi | Byte | Kilobyte | Megabyte | Gigabyte | Terabyte | Terabyte | Bit | Kilobit | Kilobit | Megabit | Gigabit | | | | | | | | | | Nessuno Bytes/Second Kilobytes/Second Megabytes/Second Gigabytes/Second Terabytes/Second Bits/Second Kilobits/Second Megabits/Second Gigabits/Second Terabits/Second Count/Second

Obbligatorio: sì

## aws:configureDocker

(Versione dello schema 2.0 o successiva) Configura un'istanza da utilizzare con contenitori e Docker. Questo plug-in è supportato su gran parte delle versioni di Linux e sui sistemi operativi Windows Server.

## Sintassi

### Schema 2.2

## YAML

```

schemaVersion: '2.2'
description: aws:configureDocker
parameters:
 action:
 description: "(Required) The type of action to perform."
 type: String
 default: Install
 allowedValues:
 - Install
 - Uninstall
 mainSteps:
 - action: aws:configureDocker
```

```
name: configureDocker
inputs:
 action: "{{ action }}"
```

## JSON

```
{
 "schemaVersion": "2.2",
 "description": "aws:configureDocker plugin",
 "parameters": {
 "action": {
 "description": "(Required) The type of action to perform.",
 "type": "String",
 "default": "Install",
 "allowedValues": [
 "Install",
 "Uninstall"
]
 }
 },
 "mainSteps": [
 {
 "action": "aws:configureDocker",
 "name": "configureDocker",
 "inputs": {
 "action": "{{ action }}"
 }
 }
]
}
```

## Input

### operazione

Il tipo di operazione da eseguire.

Tipo: Enum

Valori validi: Install | Uninstall

Obbligatorio: sì

## aws:configurePackage

(Schema versione AWS Systems Manager Distributor 2.0 o successiva) Installa o disinstalla un pacchetto. Puoi installare la versione più recente, la versione predefinita o una versione del pacchetto specificata. Sono supportati anche AWS i pacchetti forniti da. Questo plugin viene eseguito sui sistemi operativi Windows Server e Linux, ma non tutti i pacchetti disponibili sono supportati sui sistemi operativi Linux.

AWS I pacchetti disponibili per Windows Server includono quanto segue: AWSPVDriver, AWSNVMeAwsEnaNetworkDriver, AwsVssComponents, AmazonCloudWatchAgent, CodeDeployAgent, e AWSSupport-EC2Rescue.

AWS I pacchetti disponibili per i sistemi operativi Linux includono: AmazonCloudWatchAgent, CodeDeployAgent, e AWSSupport-EC2Rescue.

### Sintassi

### Schema 2.2

### YAML

```

schemaVersion: '2.2'
description: aws:configurePackage
parameters:
 name:
 description: "(Required) The name of the AWS package to install or uninstall."
 type: String
 action:
 description: "(Required) The type of action to perform."
 type: String
 default: Install
 allowedValues:
 - Install
 - Uninstall
 ssmParameter:
 description: "(Required) Argument stored in Parameter Store."
 type: String
 default: "{{ ssm:parameter_store_arg }}"
mainSteps:
- action: aws:configurePackage
 name: configurePackage
```

```
inputs:
 name: "{{ name }}"
 action: "{{ action }}"
 additionalArguments:
 "\"SSM_parameter_store_arg\": \"{{ ssmParameter }}\", \"SSM_custom_arg\":
 \"myValue\""
```

## JSON

```
{
 "schemaVersion": "2.2",
 "description": "aws:configurePackage",
 "parameters": {
 "name": {
 "description": "(Required) The name of the AWS package to install or
uninstall.",
 "type": "String"
 },
 "action": {
 "description": "(Required) The type of action to perform.",
 "type": "String",
 "default": "Install",
 "allowedValues": [
 "Install",
 "Uninstall"
]
 },
 "ssmParameter": {
 "description": "(Required) Argument stored in Parameter Store.",
 "type": "String",
 "default": "{{ ssm:parameter_store_arg }}"
 }
 },
 "mainSteps": [
 {
 "action": "aws:configurePackage",
 "name": "configurePackage",
 "inputs": {
 "name": "{{ name }}",
 "action": "{{ action }}",
 "additionalArguments": "\"SSM_parameter_store_arg\":
 \"{{ ssmParameter }}\", \"SSM_custom_arg\": \"myValue\""
 }
 }
]
}
```



```
}
]
}
```

## Input

### nome

Il nome del AWS pacchetto da installare o disinstallare. I pacchetti disponibili includono: `AWSPVDriver`, `AwsEnaNetworkDriver`, `AwsVssComponents` e `AmazonCloudWatchAgent`.

Tipo: stringa

Obbligatorio: sì

### operazione

Installa o disinstalla un pacchetto.

Tipo: Enum

Valori validi: `Install` | `Uninstall`

Obbligatorio: sì

### Tipo di installazione

Il tipo di installazione da eseguire. Se si specifica `Uninstall` and `reinstall`, il pacchetto viene completamente disinstallato e quindi reinstallato. L'applicazione non è disponibile fino al completamento della reinstallazione. Se si specifica `In-place update`, solo i file nuovi o modificati vengono aggiunti all'installazione esistente in base alle istruzioni fornite in uno script di aggiornamento. L'applicazione rimane disponibile durante tutto il processo di aggiornamento. L'`In-place update` opzione non è supportata per AWS i pacchetti pubblicati. `Uninstall` and `reinstall` è il valore predefinito.

Tipo: Enum

Valori validi: `Uninstall` and `reinstall` | `In-place update`

Obbligatorio: no

## additionalArguments

Una stringa JSON di parametri aggiuntivi da fornire agli script di installazione, disinstallazione o aggiornamento. Ogni parametro deve essere preceduto da `SSM_`. È possibile fare riferimento a un parametro Parameter Store negli argomenti aggiuntivi utilizzando la convenzione `{{ssm:parameter-name}}`. Per utilizzare il parametro aggiuntivo nello script di installazione, disinstallazione o aggiornamento, è necessario fare riferimento al parametro come variabile di ambiente utilizzando la sintassi appropriata per il sistema operativo. Ad esempio, in PowerShell, si fa riferimento all'`SSM_arg` argomento come `$Env:SSM_arg`. Non vi è alcun limite al numero di argomenti definiti, ma l'input dell'argomento aggiuntivo ha un limite di 4096 caratteri. Questo limite include tutte le chiavi e i valori definiti.

Tipo: StringMap

Obbligatorio: no

## version

Una versione specifica del pacchetto da installare o disinstallare. In caso di installazione, il sistema installa per impostazione predefinita l'ultima versione pubblicata. In caso di disinstallazione, il sistema disinstalla per impostazione predefinita la versione attualmente installata. Se non viene trovata nessuna versione installata, viene scaricata l'ultima versione pubblicata e viene eseguita l'operazione di disinstallazione.

─Tipo: stringa

Obbligatorio: no

## aws:domainJoin

Aggiungi un'istanza EC2 a un dominio. Questo plugin funziona su Linux e sistemi operativi Windows Server. Questo plugin cambia il nome host per le istanze Linux nel formato EC2AMAZ-*XXXXXXXX*. Per ulteriori informazioni sull'aggiunta di istanze EC2, consulta [Aggiungere un'istanza EC2 alla directory Microsoft AD AWS gestita nella Guida all'amministrazione](#). Servizio di directory AWS

## Sintassi

## Schema 2.2

## YAML

```

```

```

schemaVersion: '2.2'
description: aws:domainJoin
parameters:
 directoryId:
 description: "(Required) The ID of the directory."
 type: String
 directoryName:
 description: "(Required) The name of the domain."
 type: String
 directoryOU:
 description: "(Optional) The organizational unit to assign the computer object to."
 type: String
 dnsIpAddresses:
 description: "(Required) The IP addresses of the DNS servers for your directory."
 type: StringList
 hostname:
 description: "(Optional) The hostname you want to assign to the node."
 type: String
mainSteps:
- action: aws:domainJoin
 name: domainJoin
 inputs:
 directoryId: "{{ directoryId }}"
 directoryName: "{{ directoryName }}"
 directoryOU: "{{ directoryOU }}"
 dnsIpAddresses: "{{ dnsIpAddresses }}"
 hostname: "{{ hostname }}"

```

## JSON

```

{
 "schemaVersion": "2.2",
 "description": "aws:domainJoin",
 "parameters": {
 "directoryId": {
 "description": "(Required) The ID of the directory.",
 "type": "String"
 },
 "directoryName": {
 "description": "(Required) The name of the domain.",
 "type": "String"
 }
 }
}

```

```

 },
 "directoryOU": {
 "description": "(Optional) The organizational unit to assign the computer
object to.",
 "type": "String"
 },
 "dnsIpAddresses": {
 "description": "(Required) The IP addresses of the DNS servers for your
directory.",
 "type": "StringList"
 },
 "hostname": {
 "description": "(Optional) The hostname you want to assign to the node.",
 "type": "String"
 }
 },
 "mainSteps": [
 {
 "action": "aws:domainJoin",
 "name": "domainJoin",
 "inputs": {
 "directoryId": "{{ directoryId }}",
 "directoryName": "{{ directoryName }}",
 "directoryOU": "{{ directoryOU }}",
 "dnsIpAddresses": "{{ dnsIpAddresses }}",
 "hostname": "{{ hostname }}"
 }
 }
]
}

```

## Schema 1.2

### YAML

```

runtimeConfig:
 aws:domainJoin:
 properties:
 directoryId: "{{ directoryId }}"
 directoryName: "{{ directoryName }}"
 directoryOU: "{{ directoryOU }}"

```

```
dnsIpAddresses: "{{ dnsIpAddresses }}"
```

## JSON

```
{
 "runtimeConfig":{
 "aws:domainJoin":{
 "properties":{
 "directoryId":"{{ directoryId }}",
 "directoryName":"{{ directoryName }}",
 "directoryOU":"{{ directoryOU }}",
 "dnsIpAddresses":"{{ dnsIpAddresses }}"
 }
 }
 }
}
```

## Properties

### directoryId

L'ID della directory.

Tipo: stringa

Obbligatorio: sì

Esempio: "directoryId": "d-1234567890"

### directoryName

Il nome del dominio.

Tipo: stringa

Obbligatorio: sì

Esempio: "directoryName": "example.com"

### directoryOU

L'unità organizzativa (UO).

─Tipo: stringa

Obbligatorio: no

Esempio: "directoryOU": "OU=test,DC=example,DC=com"

## dns IpAddresses

Gli indirizzi IP dei server DNS.

Tipo: StringList

Obbligatorio: sì

Esempio: «dns IpAddresses «: [" 198.51.100.1", "198.51.100.2"]

## hostname

Il nome host che si desidera assegnare al nodo. Se non viene fornito, non viene effettuata alcuna modifica del nome per le istanze Windows Server, mentre le istanze Linux utilizzeranno lo schema di denominazione predefinito. Se fornito, le istanze Windows Server utilizzeranno l'esatto valore fornito, mentre per le istanze Linux fungerà da prefisso (a meno che non keepHostName sia impostato su "true").

─Tipo: stringa

Obbligatorio: no

## mantieni HostName

Determina se il nome host viene modificato per le istanze Linux quando vengono aggiunte al dominio. Questo è un Linux-only parametro. Per impostazione predefinita (senza input per hostname e con keepHostName «false»), gli host Linux verranno rinominati in base allo schema. hostnameNumAppendDigits EC2AMAZ-XXXXXX Se impostato su "true", mantiene il nome host originale e ignora gli input verso hostname e hostnameNumAppendDigits.

Tipo: Booleano

Obbligatorio: no

## nome host NumAppendDigits

Definisce il numero di cifre numeriche casuali da aggiungere dopo il valore del nome host. Questo è un Linux-only parametro e viene utilizzato insieme al hostname parametro. Se hostname non viene fornito, viene ignorato.

Tipo: stringa

Valori validi: da 1 a 5

Obbligatorio: no

## Esempi

Per alcuni esempi, consulta la sezione [Unire un'istanza Amazon EC2 a AWS Managed Microsoft AD](#) nella Servizio di directory AWS Guida per gli amministratori di .

## aws:downloadContent

(Versione dello schema 2.0 o successiva) Scaricare documenti e script SSM da posizioni remote. I repository di GitHub Enterprise non sono supportati. Questo plugin è supportato su Linux e dai sistemi operativi Windows Server.

## Sintassi

### Schema 2.2

### YAML

```

schemaVersion: '2.2'
description: aws:downloadContent
parameters:
 sourceType:
 description: "(Required) The download source."
 type: String
 sourceInfo:
 description: "(Required) The information required to retrieve the content from the required source."
 type: StringMap
mainSteps:
- action: aws:downloadContent
 name: downloadContent
 inputs:
 sourceType: "{{ sourceType }}"
 sourceInfo: "{{ sourceInfo }}"
```

### JSON

```
{
 "schemaVersion": "2.2",
```

```
"description": "aws:downloadContent",
"parameters": {
 "sourceType": {
 "description": "(Required) The download source.",
 "type": "String"
 },
 "sourceInfo": {
 "description": "(Required) The information required to retrieve the content from the required source.",
 "type": "StringMap"
 }
},
"mainSteps": [
 {
 "action": "aws:downloadContent",
 "name": "downloadContent",
 "inputs": {
 "sourceType": "{{ sourceType }}",
 "sourceInfo": "{{ sourceInfo }}"
 }
 }
]
}
```

## Input

### sourceType

Origine del download Systems Manager supporta i seguenti tipi di origine per il download di script e di documenti SSM: GitHub, Git, HTTP, S3 e SSMDocument.

Tipo: stringa

Obbligatorio: sì

### sourceInfo

Le informazioni necessarie per recuperare il contenuto dall'origine richiesta.

Tipo: StringMap

Obbligatorio: sì

Per sourceType **GitHub**, , specificare quanto segue:



- **owner**: il proprietario del repository.
- **repository**: il nome del repository.
- **path**: il percorso del file o della directory che desideri scaricare.
- **getOptions**: opzioni aggiuntive per recuperare il contenuto da un ramo diverso dal master o da un commit specifico nel repository. **getOptions** può essere omesso se si utilizza l'ultimo commit nel ramo master. Se il repository è stato creato dopo il 1° ottobre 2020, il ramo predefinito potrebbe essere denominato **main** anziché **master**. In questo caso, è necessario specificare i valori per il parametro **getOptions**.

Questo parametro utilizza il seguente formato:

- ramo:/refs/heads`branch_name`

Il valore predefinito è `master`.

Per specificare un ramo non predefinito, utilizza il formato seguente:

filiale:refs/heads/`branch_name`

- ID commit: `commitID`

Il valore predefinito è `head`.

Per utilizzare la versione del documento SSM in un commit diverso da quello più recente, specificare l'ID di commit completo. Ad esempio:

```
"getOptions": "commitID:bbc1ddb94...b76d3bEXAMPLE",
```

- **tokenInfo**: il parametro Systems Manager (un `SecureString` parametro) in cui vengono archiviate le informazioni del token di GitHub accesso, nel formato. `{ssm-secure:secure-string-token-name}`

#### Note

Questo **tokenInfo** campo è l'unico campo del plugin per documenti SSM che supporta un parametro. `SecureString` i parametri non sono supportati per nessun altro campo, né per altri plug-in di documenti SSM.

```
{
 "owner": "TestUser",
```

```
"repository": "GitHubTest",
"path": "scripts/python/test-script",
"getOptions": "branch:master",
"tokenInfo": "{ssm-secure:secure-string-token}"
}
```

Per sourceType **Git**, si deve specificare quanto segue:

- repository

L'URL del repository Git relativo al file o alla directory che si desidera scaricare.

Tipo: stringa

Inoltre, è possibile specificare i seguenti parametri facoltativi:

- getOptions

Opzioni aggiuntive per recuperare il contenuto da un ramo diverso dal master o da un commit specifico nel repository. getOptions può essere omesso se si utilizza l'ultimo commit nel ramo master.

Tipo: stringa

Questo parametro utilizza il seguente formato:

- filiale:/refs/heads*branch\_name*

Il valore predefinito è master.

"branch" è necessario solo se il documento SSM è memorizzato in un ramo diverso da master. Ad esempio:

```
"getOptions": "branch:refs/heads/main"
```

- ID commit: *commitID*

Il valore predefinito è head.

Per utilizzare la versione del documento SSM in un commit diverso da quello più recente, specificare l'ID di commit completo. Ad esempio:

```
"getOptions": "commitID:bbc1ddb94...b76d3bEXAMPLE",
```

- PrivateShkey

La chiave SSH da usare durante la connessione al repository specificato. È possibile utilizzare il formato seguente per riferirsi a un parametro SecureString per il valore della chiave SSH: `{{ssm-secure:your-secure-string-parameter}}`.

Tipo: stringa

- salta HostKeyChecking

Determina il valore dell' StrictHostKeyCheckingopzione quando ci si connette a quella repository specificata. Il valore predefinito è false.

Tipo: Booleano

- username

Il nome utente da usare durante la connessione al repositoryspecificato utilizzando HTTP. È possibile utilizzare il formato seguente per riferirsi a un parametro SecureString per il valore del nome utente: `{{ssm-secure:your-secure-string-parameter}}`.

Tipo: stringa

- password

La password da usare durante la connessione al repositoryspecificato utilizzando HTTP. È possibile utilizzare il formato seguente per riferirsi a un parametro SecureString per il valore della password: `{{ssm-secure:your-secure-string-parameter}}`.

Tipo: stringa

Per sourceType **HTTP**, si deve specificare quanto segue:

- url

L'URL del file o della directory che si desidera scaricare.

Tipo: stringa

Inoltre, è possibile specificare i seguenti parametri facoltativi:

- consentire InsecureDownload

Determina se è possibile eseguire un download tramite una connessione non crittografata con Secure Socket Layer (SSL) o Transport Layer Security (TLS). Il valore predefinito è false. Si

sconsiglia l'esecuzione di download senza crittografia. Se scegli di farlo, ti assumi tutti i rischi associati. SSM Agent segue i reindirizzamenti HTTP, il che significa che un URL HTTPS può essere reindirizzato a un URL HTTP. La sicurezza è una responsabilità condivisa tra AWS e te. Questo è descritto come il modello di responsabilità condivisa. Per ulteriori informazioni, consulta il [modello di responsabilità condivisa](#).

Tipo: Booleano

- `authMethod`

Determina se un nome utente e una password vengono utilizzati per l'autenticazione durante la connessione all'`url` specificato. Se si specifica `Basic` o `Digest`, è necessario fornire valori per i parametri `username` e `password`. Per utilizzare il metodo `Digest`, deve essere installata nell'istanza la versione di SSM Agent 3.0.1181.0 o successiva. Il metodo `Digest` supporta la crittografia MD5 e SHA256.

Tipo: stringa

Valori validi: `None` | `Basic` | `Digest`

- `username`

Il nome utente da usare durante la connessione all'`url` specificato utilizzando l'autenticazione `Basic`. È possibile utilizzare il formato seguente per riferirsi a un parametro `SecureString` per il valore del nome utente: `{{ssm-secure:your-secure-string-parameter}}`.

Tipo: stringa

- `password`

La password da usare durante la connessione all'`url` specificato utilizzando l'autenticazione `Basic`. È possibile utilizzare il formato seguente per riferirsi a un parametro `SecureString` per il valore della password: `{{ssm-secure:your-secure-string-parameter}}`.

Tipo: stringa

Per `sourceType` **S3**, specificare quanto segue:

- `path`: l'URL del file o della directory che si desidera scaricare da Amazon S3.

**Note**

Quando si scarica un file da un bucket S3, i file .etag vengono generati nella directory di download.

```
{
 "path": "https://s3.amazonaws.com/amzn-s3-demo-bucket/powershell/
helloPowershell.ps1"
}
```

Per `sourceType` **SSMDocument**, specificare uno dei seguenti valori:

- `name`: il nome e la versione del documento nel formato seguente: `name:version`. La versione è facoltativa.

```
{
 "name": "Example-RunPowerShellScript:3"
}
```

- `name`: l'ARN del documento nel seguente formato:  
`arn:aws:ssm:region:account_id:document/document_name`

```
{
 "name": "arn:aws:ssm:us-east-2:3344556677:document/MySharedDoc"
}
```

**destinationPath**

Un percorso locale facoltativo nell'istanza in cui desideri scaricare il file. Se non specifichi un percorso, i contenuti vengono scaricati in un percorso relativo al tuo ID comando.

─Tipo: stringa

Obbligatorio: no

**aws:psModule**

Installa PowerShell i moduli su un'istanza Amazon EC2. Questo plugin può essere eseguito solo su sistemi operativi Windows Server.

## Sintassi

### Schema 2.2

#### YAML

```

schemaVersion: '2.2'
description: aws:psModule
parameters:
 source:
 description: "(Required) The URL or local path on the instance to the
application
.zip file."
 type: String
mainSteps:
- action: aws:psModule
 name: psModule
 inputs:
 source: "{{ source }}"
```

#### JSON

```
{
 "schemaVersion": "2.2",
 "description": "aws:psModule",
 "parameters": {
 "source": {
 "description": "(Required) The URL or local path on the instance to the
application .zip file.",
 "type": "String"
 }
 },
 "mainSteps": [
 {
 "action": "aws:psModule",
 "name": "psModule",
 "inputs": {
 "source": "{{ source }}"
 }
 }
]
}
```

## Schema 1.2

### YAML

```

runtimeConfig:
 aws:psModule:
 properties:
 - runCommand: "{{ commands }}"
 source: "{{ source }}"
 sourceHash: "{{ sourceHash }}"
 workingDirectory: "{{ workingDirectory }}"
 timeoutSeconds: "{{ executionTimeout }}"
```

### JSON

```
{
 "runtimeConfig": {
 "aws:psModule": {
 "properties": [
 {
 "runCommand": "{{ commands }}",
 "source": "{{ source }}",
 "sourceHash": "{{ sourceHash }}",
 "workingDirectory": "{{ workingDirectory }}",
 "timeoutSeconds": "{{ executionTimeout }}"
 }
]
 }
 }
}
```

### Properties

#### runCommand

Il PowerShell comando da eseguire dopo l'installazione del modulo.

Tipo: StringList

Obbligatorio: no

## origine

L'URL o il percorso locale nell'istanza al file .zip dell'applicazione.

Tipo: stringa

Obbligatorio: sì

## sourceHash

L'hash SHA256 del file .zip.

─Tipo: stringa

Obbligatorio: no

## timeoutSeconds

Il tempo in secondi entro cui un comando deve essere portato a termine prima di essere considerato non riuscito.

─Tipo: stringa

Obbligatorio: no

## workingDirectory

Il percorso alla directory di lavoro nell'istanza.

─Tipo: stringa

Obbligatorio: no

## **aws:refreshAssociation**

(Versione dello schema 2.0 o successiva) Aggiorna (applicazione di forza) un'associazione on demand. Questa operazione modificherà lo stato del sistema in base a quanto definito nell'associazione selezionata o in tutte le associazioni dei target. Questo plugin funziona su sistemi operativi Linux e Microsoft Windows Server.



## Sintassi

### Schema 2.2

#### YAML

```

schemaVersion: '2.2'
description: aws:refreshAssociation
parameters:
 associationIds:
 description: "(Optional) List of association IDs. If empty, all associations
bound
 to the specified target are applied."
 type: StringList
mainSteps:
- action: aws:refreshAssociation
 name: refreshAssociation
 inputs:
 associationIds:
 - "{{ associationIds }}"
```

#### JSON

```
{
 "schemaVersion": "2.2",
 "description": "aws:refreshAssociation",
 "parameters": {
 "associationIds": {
 "description": "(Optional) List of association IDs. If empty, all associations
bound to the specified target are applied.",
 "type": "StringList"
 }
 },
 "mainSteps": [
 {
 "action": "aws:refreshAssociation",
 "name": "refreshAssociation",
 "inputs": {
 "associationIds": [
 "{{ associationIds }}"
]
 }
 }
]
}
```

```
}
]
}
```

## Input

### associationIds

Elenco di ID di associazione. Se vuoto, vengono applicate tutte le associazioni ai target specificati.

Tipo: StringList

Obbligatorio: no

## aws:run DockerAction

(Versione dello schema 2.0 o successiva) Esegui operazioni Docker sui contenitori. Questo plugin funziona su sistemi operativi Linux e Microsoft Windows Server.

## Sintassi

### Schema 2.2

## YAML

```

mainSteps:
- action: aws:runDockerAction
 name: RunDockerAction
 inputs:
 action: "{{ action }}"
 container: "{{ container }}"
 image: "{{ image }}"
 memory: "{{ memory }}"
 cpuShares: "{{ cpuShares }}"
 volume: "{{ volume }}"
 cmd: "{{ cmd }}"
 env: "{{ env }}"
 user: "{{ user }}"
 publish: "{{ publish }}"
 workingDirectory: "{{ workingDirectory }}"
```

```
timeoutSeconds: "{{ timeoutSeconds }}"
```

## JSON

```
{
 "mainSteps":[
 {
 "action":"aws:runDockerAction",
 "name":"RunDockerAction",
 "inputs:{
 "action":"{{ action }}",
 "container":"{{ container }}",
 "image":"{{ image }}",
 "memory":"{{ memory }}",
 "cpuShares":"{{ cpuShares }}",
 "volume":"{{ volume }}",
 "cmd":"{{ cmd }}",
 "env":"{{ env }}",
 "user":"{{ user }}",
 "publish":"{{ publish }}",
 "workingDirectory": "{{ workingDirectory }}",
 "timeoutSeconds": "{{ timeoutSeconds }}"
 }
 }
]
}
```

### Input

#### operazione

Il tipo di operazione da eseguire.

Tipo: stringa

Obbligatorio: sì

#### container

L'ID del container Docker.

─Tipo: stringa

Obbligatorio: no

image

Il nome dell'immagine Docker.

─Tipo: stringa

Obbligatorio: no

cmd

Il comando del container.

─Tipo: stringa

Obbligatorio: no

memory

Il limite di memoria del container.

─Tipo: stringa

Obbligatorio: no

cpuShares

Le condivisioni di CPU del container (peso relativo).

─Tipo: stringa

Obbligatorio: no

volume

I montaggi dei volumi del container.

Tipo: StringList

Obbligatorio: no

env

Le variabili di ambiente del container.

─Tipo: stringa

Obbligatorio: no

user

Il nome dell'utente del container.

─Tipo: stringa

Obbligatorio: no

pubblicazione

Le porte pubblicate del container.

─Tipo: stringa

Obbligatorio: no

workingDirectory

Il percorso verso la directory di lavoro nel nodo gestito dall'utente.

─Tipo: stringa

Obbligatorio: no

timeoutSeconds

Il tempo in secondi entro cui un comando deve essere portato a termine prima di essere considerato non riuscito.

─Tipo: stringa

Obbligatorio: no

## **aws:runDocument**

(Versione dello schema 2.0 o successiva) Esegue documenti SSM archiviati in Systems Manager o in una condivisione locale. È possibile utilizzare questo plugin con il plugin [aws:downloadContent](#) per scaricare un documento SSM da una posizione remota a una condivisione locale, quindi eseguirlo. Questo plugin è supportato su Linux e dai sistemi operativi Windows Server. Questo plugin non supporta l'esecuzione del documento AWS-UpdateSSMAgent o qualsiasi documento che utilizza il plugin aws:updateSsmAgent.

## Sintassi

### Schema 2.2

#### YAML

```

schemaVersion: '2.2'
description: aws:runDocument
parameters:
 documentType:
 description: "(Required) The document type to run."
 type: String
 allowedValues:
 - LocalPath
 - SSMDocument
mainSteps:
- action: aws:runDocument
 name: runDocument
 inputs:
 documentType: "{{ documentType }}"
```

#### JSON

```
{
 "schemaVersion": "2.2",
 "description": "aws:runDocument",
 "parameters": {
 "documentType": {
 "description": "(Required) The document type to run.",
 "type": "String",
 "allowedValues": [
 "LocalPath",
 "SSMDocument"
]
 }
 },
 "mainSteps": [
 {
 "action": "aws:runDocument",
 "name": "runDocument",
 "inputs": {
 "documentType": "{{ documentType }}"
 }
 }
]
}
```

```
}
 }
] }
}
```

## Input

### documentType

Il tipo di documento da eseguire. È possibile eseguire documenti locali (LocalPath) o documenti archiviati in Systems Manager (SSMDocument).

Tipo: stringa

Obbligatorio: sì

### documentPath

Il percorso del documento. Se documentType è LocalPath, specifica il percorso al documento nella condivisione locale. Se documentType è SSMDocument, specifica il nome del documento.

─Tipo: stringa

Obbligatorio: no

### documentParameters

I parametri per il documento.

Tipo: StringMap

Obbligatorio: no

## **aws: esegui PowerShellScript**

Esegui PowerShell script o specifica il percorso di uno script da eseguire. Questo plugin può essere eseguito su sistemi operativi Microsoft Windows Server e Linux.

## Sintassi

### Schema 2.2

#### YAML

```

schemaVersion: '2.2'
description: aws:runPowerShellScript
parameters:
 commands:
 type: String
 description: "(Required) The commands to run or the path to an existing script
 on the instance."
 default: Write-Host "Hello World"
mainSteps:
- action: aws:runPowerShellScript
 name: runPowerShellScript
 inputs:
 timeoutSeconds: '60'
 runCommand:
 - "{{ commands }}"
```

#### JSON

```
{
 "schemaVersion": "2.2",
 "description": "aws:runPowerShellScript",
 "parameters": {
 "commands": {
 "type": "String",
 "description": "(Required) The commands to run or the path to an existing
script on the instance.",
 "default": "Write-Host \"Hello World\""
 }
 },
 "mainSteps": [
 {
 "action": "aws:runPowerShellScript",
 "name": "runPowerShellScript",
 "inputs": {
 "timeoutSeconds": "60",
 "runCommand": [
```



```
 "{{ commands }}"
]
}
]
```

## Schema 1.2

### YAML

```

runtimeConfig:
 aws:runPowerShellScript:
 properties:
 - id: 0.aws:runPowerShellScript
 runCommand: "{{ commands }}"
 workingDirectory: "{{ workingDirectory }}"
 timeoutSeconds: "{{ executionTimeout }}"
```

### JSON

```
{
 "runtimeConfig": {
 "aws:runPowerShellScript": {
 "properties": [
 {
 "id": "0.aws:runPowerShellScript",
 "runCommand": "{{ commands }}",
 "workingDirectory": "{{ workingDirectory }}",
 "timeoutSeconds": "{{ executionTimeout }}"
 }
]
 }
 }
}
```

## Properties

### runCommand

Specifica i comandi da eseguire o il percorso a uno script esistente nell'istanza.

Tipo: StringList

Obbligatorio: sì

### timeoutSeconds

Il tempo in secondi entro cui un comando deve essere portato a termine prima di essere considerato non riuscito. Quando viene raggiunto il timeout, Systems Manager interrompe l'esecuzione del comando.

─Tipo: stringa

Obbligatorio: no

### workingDirectory

Il percorso alla directory di lavoro nell'istanza.

─Tipo: stringa

Obbligatorio: no

## aws: run ShellScript

Esegui script di shell Linux o specifica il percorso a uno script da eseguire. Questo plugin può essere eseguito solo su sistemi operativi Linux.

### Sintassi

### Schema 2.2

### YAML

```

schemaVersion: '2.2'
description: aws:runShellScript
```

```
parameters:
 commands:
 type: String
 description: "(Required) The commands to run or the path to an existing script
 on the instance."
 default: echo Hello World
mainSteps:
- action: aws:runShellScript
 name: runShellScript
 inputs:
 timeoutSeconds: '60'
 runCommand:
 - "{{ commands }}"
```

## JSON

```
{
 "schemaVersion": "2.2",
 "description": "aws:runShellScript",
 "parameters": {
 "commands": {
 "type": "String",
 "description": "(Required) The commands to run or the path to an existing
script on the instance.",
 "default": "echo Hello World"
 }
 },
 "mainSteps": [
 {
 "action": "aws:runShellScript",
 "name": "runShellScript",
 "inputs": {
 "timeoutSeconds": "60",
 "runCommand": [
 "{{ commands }}"
]
 }
 }
]
}
```

## Schema 1.2

### YAML

```

runtimeConfig:
 aws:runShellScript:
 properties:
 - runCommand: "{{ commands }}"
 workingDirectory: "{{ workingDirectory }}"
 timeoutSeconds: "{{ executionTimeout }}"
```

### JSON

```
{
 "runtimeConfig": {
 "aws:runShellScript": {
 "properties": [
 {
 "runCommand": "{{ commands }}",
 "workingDirectory": "{{ workingDirectory }}",
 "timeoutSeconds": "{{ executionTimeout }}"
 }
]
 }
 }
}
```

### Properties

#### runCommand

Specifica i comandi da eseguire o il percorso a uno script esistente nell'istanza.

Tipo: StringList

Obbligatorio: sì

#### timeoutSeconds

Il tempo in secondi entro cui un comando deve essere portato a termine prima di essere considerato non riuscito. Quando viene raggiunto il timeout, Systems Manager interrompe l'esecuzione del comando.

■Tipo: stringa

Obbligatorio: no

workingDirectory

Il percorso alla directory di lavoro nell'istanza.

■Tipo: stringa

Obbligatorio: no

## **aws:softwareInventory**

(Versione dello schema 2.0 o successiva) è possibile ottenere i metadati su applicazioni, file e configurazioni sulle istanze gestite. Questo plugin funziona su sistemi operativi Linux e Microsoft Windows Server. Quando configuri la raccolta dell'inventario, inizi creando un' AWS Systems Manager State Manager associazione. Systems Manager raccoglie i dati dell'inventario quando viene eseguita l'associazione. Se non si crea prima l'associazione e si tenta di richiamare il plugin `aws:softwareInventory`, il sistema restituisce il seguente errore:

The `aws:softwareInventory` plugin can only be invoked through `ssm-associate`.

Un'istanza può avere una sola associazione di Inventory configurata alla volta. Se configuri un'istanza con due o più associazioni, l'associazione di Inventory non viene eseguita e non viene raccolto alcun dato dell'inventario. Per ulteriori informazioni sulla raccolta dell'inventario, consulta [AWS Systems Manager Inventory](#).

Sintassi

Schema 2.2

YAML

```

mainSteps:
- action: aws:softwareInventory
 name: collectSoftwareInventoryItems
 inputs:
 applications: "{{ applications }}"
```

```
awsComponents: "{{ awsComponents }}"
networkConfig: "{{ networkConfig }}"
files: "{{ files }}"
services: "{{ services }}"
windowsRoles: "{{ windowsRoles }}"
windowsRegistry: "{{ windowsRegistry }}"
windowsUpdates: "{{ windowsUpdates }}"
instanceDetailedInformation: "{{ instanceDetailedInformation }}"
customInventory: "{{ customInventory }}"
```

## JSON

```
{
 "mainSteps":[
 {
 "action":"aws:softwareInventory",
 "name":"collectSoftwareInventoryItems",
 "inputs:{
 "applications":"{{ applications }}",
 "awsComponents":"{{ awsComponents }}",
 "networkConfig":"{{ networkConfig }}",
 "files":"{{ files }}",
 "services":"{{ services }}",
 "windowsRoles":"{{ windowsRoles }}",
 "windowsRegistry":"{{ windowsRegistry }}",
 "windowsUpdates":"{{ windowsUpdates }}",
 "instanceDetailedInformation":"{{ instanceDetailedInformation }}",
 "customInventory":"{{ customInventory }}"
 }
 }
]
}
```

## Inputs

### applications

(Facoltativo) Consente di raccogliere i metadati per le applicazioni installate.

─Tipo: stringa

Obbligatorio: no

## awsComponents

(Facoltativo) Raccogli i metadati per AWS componenti come amazon-ssm-agent.

─Tipo: stringa

Obbligatorio: no

## files

(Facoltativo, richiede la versione di SSM Agent 2.2.64.0 o successiva) Consente di raccogliere i metadati dei file, tra cui nomi, data e ora di creazione, data e ora dell'ultimo accesso e aggiornamento, e dimensioni, per citarne alcuni. Per ulteriori informazioni sulla raccolta dell'inventario dei file, consulta [Utilizzo dell'inventario dei file e del registro di sistema di Windows](#).

─Tipo: stringa

Obbligatorio: no

## networkConfig

(Facoltativo) Consente di raccogliere i metadati relativi alle configurazioni di rete.

─Tipo: stringa

Obbligatorio: no

## billingInfo

(Facoltativo) Raccogli i metadati per i dettagli della piattaforma associati al codice di fatturazione di AMI.

─Tipo: stringa

Obbligatorio: no

## windowsUpdates

(Facoltativo) Consente di raccogliere i metadati per tutti gli aggiornamenti di Windows.

─Tipo: stringa

Obbligatorio: no

## istanza DetailedInformation

(Facoltativo) Consente di raccogliere ulteriori informazioni sulle istanze rispetto a quelle fornite dal plugin dell'inventario predefinito (`aws:instanceInformation`), tra cui ad esempio il modello della CPU, la velocità e il numero di core.

─Tipo: stringa

Obbligatorio: no

## services

(Facoltativo, solo sistema operativo Windows, richiede SSM Agent versione 2.2.64.0 o successiva) Consente di raccogliere i metadati per le configurazioni dei servizi.

─Tipo: stringa

Obbligatorio: no

## windowsRegistry

(Facoltativo, solo sistema operativo Windows, richiede SSM Agent versione 2.2.64.0 o successiva) Consente di raccogliere chiavi e valori del registro di Windows. È possibile scegliere un percorso chiave e raccogliere tutte le chiavi e i valori in modo ricorsivo. È possibile inoltre raccogliere una determinata chiave di registro e il relativo valore per un percorso specifico. Inventory raccoglie il percorso, il nome, il tipo e il valore delle chiavi. Per ulteriori informazioni sulla raccolta dell'inventario del Registro di sistema di Windows, consulta [Utilizzo dell'inventario dei file e del registro di sistema di Windows](#).

─Tipo: stringa

Obbligatorio: no

## windowsRoles

(Facoltativo, solo sistema operativo Windows, richiede SSM Agent versione 2.2.64.0 o successiva) Consente di raccogliere i metadati per le configurazioni dei ruoli Microsoft Windows.

─Tipo: stringa

Obbligatorio: no

## customInventory

(Facoltativo) Consente di raccogliere i dati dell'inventario personalizzato. Per ulteriori informazioni sull'inventario personalizzato, consulta [Utilizzo di inventari personalizzati](#)



▪Tipo: stringa

Obbligatorio: no

personalizzato InventoryDirectory

(Facoltativo) Raccogli dati di inventario personalizzati dalla directory specificata. Per ulteriori informazioni sull'inventario personalizzato, consulta [Utilizzo di inventari personalizzati](#)

▪Tipo: stringa

Obbligatorio: no

## aws:updateAgent

Aggiorna il servizio EC2Config alla versione più recente o specifica una versione precedente. Questo plugin funziona solo sui sistemi operativi Microsoft Windows Server. Per ulteriori informazioni sul servizio EC2Config, consulta la sezione [Configurazione di un'istanza Windows utilizzando il servizio EC2Config \(legacy\)](#) nella Guida per l'utente di Amazon EC2.

Sintassi

Schema 2.2

YAML

```

schemaVersion: '2.2'
description: aws:updateAgent
mainSteps:
- action: aws:updateAgent
 name: updateAgent
 inputs:
 agentName: Ec2Config
 source: https://s3.{Region}.amazonaws.com/aws-ssm-{Region}/manifest.json
```

JSON

```
{
 "schemaVersion": "2.2",
 "description": "aws:updateAgent",
```

```
"mainSteps": [
 {
 "action": "aws:updateAgent",
 "name": "updateAgent",
 "inputs": {
 "agentName": "Ec2Config",
 "source": "https://s3.{Region}.amazonaws.com/aws-ssm-{Region}/manifest.json"
 }
 }
]
}
```

## Schema 1.2

### YAML

```

runtimeConfig:
 aws:updateAgent:
 properties:
 agentName: Ec2Config
 source: https://s3.{Region}.amazonaws.com/aws-ssm-{Region}/manifest.json
 allowDowngrade: "{{ allowDowngrade }}"
 targetVersion: "{{ version }}"
```

### JSON

```
{
 "runtimeConfig": {
 "aws:updateAgent": {
 "properties": {
 "agentName": "Ec2Config",
 "source": "https://s3.{Region}.amazonaws.com/aws-ssm-{Region}/
manifest.json",
 "allowDowngrade": "{{ allowDowngrade }}",
 "targetVersion": "{{ version }}"
 }
 }
 }
}
```

## Properties

### agentName

EC2Config. Questo è il nome dell'agente che esegue il servizio EC2Config.

Tipo: stringa

Obbligatorio: sì

### allowDowngrade

Consenti il downgrade del servizio EC2Config a una versione precedente. Se impostato su "false", il servizio può essere aggiornato solo a versioni più recenti (impostazione predefinita). Se impostato su "true", specifica la versione precedente.

Tipo: Booleano

Obbligatorio: no

### origine

La posizione in cui Systems Manager copia la versione di EC2Config da installare. Non puoi modificare questa posizione.

Tipo: stringa

Obbligatorio: sì

### targetVersion

Una versione specifica del servizio EC2Config da installare. Se non è specificata, il servizio verrà aggiornato alla versione più recente.

─Tipo: stringa

Obbligatorio: no

## aws: aggiornamento SsmAgent

Aggiorna SSM Agent alla versione più recente o specifica una versione precedente. Questo plugin funziona su Linux e sistemi operativi Windows Server. Per ulteriori informazioni, consulta [Lavorare con Agente SSM](#).

## Sintassi

### Schema 2.2

#### YAML

```

schemaVersion: '2.2'
description: aws:updateSsmAgent
parameters:
 allowDowngrade:
 default: 'false'
 description: "(Optional) Allow the Amazon SSM Agent service to be downgraded to
 an earlier version. If set to false, the service can be upgraded to newer
 versions
 only (default). If set to true, specify the earlier version."
 type: String
 allowedValues:
 - 'true'
 - 'false'
mainSteps:
- action: aws:updateSsmAgent
 name: updateSSMAgent
 inputs:
 agentName: amazon-ssm-agent
 source: https://s3.{Region}.amazonaws.com/amazon-ssm-{Region}/ssm-agent-
manifest.json
 allowDowngrade: "{{ allowDowngrade }}"
```

#### JSON

```
{
 "schemaVersion": "2.2",
 "description": "aws:updateSsmAgent",
 "parameters": {
 "allowDowngrade": {
 "default": "false",
 "description": "(Required) Allow the Amazon SSM Agent service to be downgraded
to an earlier version. If set to false, the service can be upgraded to newer
versions only (default). If set to true, specify the earlier version.",
 "type": "String",
 "allowedValues": [
 "true",
```

```

 "false"
]
 }
 },
 "mainSteps": [
 {
 "action": "aws:updateSsmAgent",
 "name": "awsupdateSsmAgent",
 "inputs": {
 "agentName": "amazon-ssm-agent",
 "source": "https://s3.{Region}.amazonaws.com/amazon-ssm-{Region}/ssm-agent-
manifest.json",
 "allowDowngrade": "{{ allowDowngrade }}"
 }
 }
]
}

```

## Schema 1.2

### YAML

```

runtimeConfig:
 aws:updateSsmAgent:
 properties:
 - agentName: amazon-ssm-agent
 source: https://s3.{Region}.amazonaws.com/aws-ssm-{Region}/manifest.json
 allowDowngrade: "{{ allowDowngrade }}"

```

### JSON

```

{
 "runtimeConfig": {
 "aws:updateSsmAgent": {
 "properties": [
 {
 "agentName": "amazon-ssm-agent",
 "source": "https://s3.{Region}.amazonaws.com/aws-ssm-{Region}/
manifest.json",
 "allowDowngrade": "{{ allowDowngrade }}"
 }
]
 }
 }
}

```

```
]
 }
}
}
```

## Properties

### agentName

amazon-ssm-agent. Questo è il nome dell'agente Systems Manager che elabora le richieste ed esegue i comandi nell'istanza.

Tipo: stringa

Obbligatorio: sì

### allowDowngrade

Consenti il downgrade di SSM Agent a una versione precedente. Se impostato su "false", l'agente può essere aggiornato solo a versioni più recenti (impostazione predefinita). Se impostato su "true", specifica la versione precedente.

Tipo: Booleano

Obbligatorio: sì

### origine

La posizione in cui Systems Manager copia la versione di SSM Agent da installare. Non puoi modificare questa posizione.

Tipo: stringa

Obbligatorio: sì

### targetVersion

Una versione specifica di SSM Agent da installare. Se non è specificata, l'agente verrà aggiornato alla versione più recente.

▪Tipo: stringa

Obbligatorio: no

## Creazione del contenuto del documento SSM

Se i documenti AWS Systems Manager pubblici non eseguono tutte le azioni che desideri eseguire sulle tue AWS risorse, puoi creare i tuoi documenti SSM. È inoltre possibile clonare documenti SSM tramite la console. La clonazione copia il contenuto da un documento esistente in un nuovo documento che è possibile modificare. Il contenuto del documento non deve superare i 64 KB, incluso il contenuto specificato per i parametri di input in fase di esecuzione. Per i nuovi Command o Policy i documenti, consigliamo la versione dello schema 2.2 o successiva. Questa versione supporta la modifica dei documenti, il controllo automatico delle versioni, il sequenziamento e altro ancora.

### Scrittura del contenuto del documento SSM

Per creare il proprio contenuto del documento SSM, è importante comprendere i diversi schemi, plugin, le diverse funzionalità e la diversa sintassi disponibili per i documenti SSM. Si consiglia di acquisire familiarità con le seguenti risorse.

- [Scrivere i propri documenti AWS Systems Manager](#)
- [Elementi di dati e parametri](#)
- [Schemi, funzionalità ed esempi](#)
- [Documentazione di riferimento del plugin per i documenti di comando](#)
- [Riferimento alle operazioni del servizio di automazione di Systems Manager](#)
- [Variabili di sistema del servizio di automazione](#)
- [Ulteriori esempi di runbook](#)
- [Utilizzo dei runbook Automation di Systems Manager](#) tramite il AWS Toolkit for Visual Studio Code
- [Esperienza di progettazione visiva per i runbook Automation](#)
- [Utilizzo di script nei runbook](#)

AWS i documenti SSM predefiniti potrebbero eseguire alcune delle azioni richieste. È possibile richiamare questi documenti utilizzando i plugin `aws:runDocument`, `aws:runCommand` o `aws:executeAutomation` all'interno del documento SSM personalizzato, a seconda del tipo di documento. È inoltre possibile copiare parti di tali documenti in un documento SSM personalizzato e modificare il contenuto in base alle proprie esigenze.

 Tip

Durante la creazione del contenuto del documento SSM, è possibile modificare il contenuto e aggiornare il documento più volte durante il test. I comandi seguenti aggiornano il documento SSM con il contenuto più recente e aggiornano la versione predefinita del documento alla versione più recente.

 Note

I comandi Linux e Windows utilizzano lo strumento a riga di comando `jq` per filtrare i dati di risposta JSON.

## Linux &amp; macOS

```
latestDocVersion=$(aws ssm update-document \
 --content file://path/to/file/documentContent.json \
 --name "ExampleDocument" \
 --document-format JSON \
 --document-version '$LATEST' \
 | jq -r '.DocumentDescription.LatestVersion')

aws ssm update-document-default-version \
 --name "ExampleDocument" \
 --document-version $latestDocVersion
```

## Windows

```
latestDocVersion=$(aws ssm update-document ^
 --content file://C:\path\to\file\documentContent.json ^
 --name "ExampleDocument" ^
 --document-format JSON ^
 --document-version "$LATEST" ^
 | jq -r '.DocumentDescription.LatestVersion')

aws ssm update-document-default-version ^
 --name "ExampleDocument" ^
 --document-version $latestDocVersion
```



## PowerShell

```
$content = Get-Content -Path "C:\path\to\file\documentContent.json" | Out-String
$latestDocVersion = Update-SSMDocument `
 -Content $content `
 -Name "ExampleDocument" `
 -DocumentFormat "JSON" `
 -DocumentVersion '$LATEST' `
 | Select-Object -ExpandProperty LatestVersion

Update-SSMDocumentDefaultVersion `
 -Name "ExampleDocument" `
 -DocumentVersion $latestDocVersion
```

### Best practice per la sicurezza dei documenti SSM

Durante la creazione di documenti SSM, segui queste best practice per la sicurezza, per evitare l'iniezione di comandi e garantire una gestione sicura dei parametri:

- Utilizza l'interpolazione delle variabili di ambiente per i parametri di stringa che verranno utilizzati nei comandi o negli script. Aggiungi la proprietà di `interpolationType` con valore `ENV_VAR` ai tuoi parametri di stringa:

```
{
 "command": {
 "type": "String",
 "description": "Command to execute",
 "interpolationType": "ENV_VAR"
 }
}
```

Puoi migliorare ulteriormente la sicurezza dei tuoi documenti SSM specificando che le virgolette doppie non sono accettate nei valori forniti per interpolazione:

```
{
 "command": {
 "type": "String",
 "description": "Command to execute",
```

```

 "interpolationType": "ENV_VAR",
 "allowedPattern": "^[^"]*$"
 }
}

```

- Quando si utilizzano linguaggi interpretati come Python, Ruby o Node.js, si fa riferimento ai parametri utilizzando la sintassi della variabile di ambiente appropriata:

```

Python example
import os
command = os.environ['SSM_Message']

```

- Per la compatibilità retroattiva con le versioni SSM Agent precedenti (precedenti alla versione 3.3.2746.0), includi la logica di fallback per le variabili di ambiente:

```

if [-z "${SSM_command+x}"]; then
 export SSM_command="{{command}}"
fi

```

- Combina l'interpolazione delle variabili di ambiente con `allowedPattern` per una convalida aggiuntiva degli input. Nell'esempio seguente, il valore di `allowedPattern` `^[^"]*$` impedisce specificamente le virgolette doppie nel valore della stringa:

```

{
 "command": {
 "type": "String",
 "interpolationType": "ENV_VAR",
 "allowedPattern": "^[a-zA-Z0-9_-]+$"
 }
}

```

- Prima di implementare il documento SSM, verifica le seguenti considerazioni sulla sicurezza:
  - Tutti i parametri di stringa che accettano l'input dell'utente utilizzano l'interpolazione delle variabili di ambiente, quando appropriato.
  - La convalida dell'input viene implementata utilizzando `allowedPattern`, ove possibile.
  - Il documento include la gestione appropriata degli errori per l'elaborazione dei parametri.
  - La compatibilità retroattiva viene mantenuta per gli ambienti che utilizzano versioni SSM Agent precedenti.

Per informazioni sulle risorse di AWS proprietà del servizio a cui accede Systems Manager e su come configurare le politiche perimetrali dei dati, vedere. [Perimetri di dati in AWS Systems Manager](#)

## Clonazione di un documento SSM

È possibile clonare AWS Systems Manager i documenti utilizzando la console Systems Manager Documents per creare documenti SSM. La clonazione di documenti SSM consente di copiare il contenuto da un documento esistente in un nuovo documento che è possibile modificare. Non puoi clonare un documento di dimensioni superiori a 64 KB.

### Per clonare un documento SSM

1. Aprire la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Documenti.
3. Nella casella di ricerca, inserire il nome del documento che si desidera clonare.
4. Scegliere il nome del documento che si desidera clonare, quindi scegliere Clone document (Clona documento) nel menu a tendina Actions (Operazioni).
5. Modificare il documento come si preferisce, quindi scegliere Create document (Crea documento) per salvare il documento.

Dopo aver scritto il contenuto del documento SSM, è possibile utilizzarlo per creare un documento SSM tramite uno dei seguenti metodi.

### Creare documenti SSM

- [Creazione di documenti compositi](#)

### Creazione di documenti compositi

Un documento composito AWS Systems Manager (SSM) è un documento personalizzato che esegue una serie di azioni eseguendo uno o più documenti SSM secondari. I documenti compositi promuovono l'Infrastructure as Code consentendo di creare un set standard di documenti SSM per attività comuni, come processi di bootstrap di software o l'aggiunta di domini a istanze. È quindi possibile condividere questi documenti Account AWS in un unico documento Regione AWS per ridurre la manutenzione dei documenti SSM e garantire la coerenza.

Ad esempio, puoi creare un documento composito che esegue le seguenti operazioni:

1. Installa tutte le patch nell'elenco Consenti.
2. Installa il software antivirus.
3. Scarica script da GitHub e li esegue.

In questo esempio, il documento SSM personalizzato include i seguenti plugin per effettuare le operazioni riportate di seguito:

1. Il plug-in `aws:runDocument` per eseguire il documento `AWS-RunPatchBaseline`, che installa tutte le patch consentite elencate.
2. Il plugin `aws:runDocument` per eseguire il documento `AWS-InstallApplication`, che installa il software antivirus.
3. Il plug-in `aws:downloadContent` per scaricare script da GitHub ed eseguirli.

I documenti compositi e secondari possono essere archiviati in Systems Manager, GitHub (repository pubblici e privati) o Amazon S3. I documenti compositi e secondari possono essere create in formato JSON o YAML.

#### Note

I documenti compositi possono essere eseguiti solo a una profondità massima di tre documenti. Ciò significa che un documento composito può chiamare un documento figlio e che questo documento figlio può chiamare un ultimo documento.

Per creare un documento composito, aggiungere il plug-in [aws:runDocument](#) in un documento SSM personalizzato e specificare gli input necessari. L'esempio qui sotto mostra un documento composito che effettua le seguenti operazioni:

1. Esegue il plug-in [aws:downloadContent](#) per scaricare un documento SSM da un repository GitHub pubblico in una directory locale denominata `bootstrap`. Il documento SSM si chiama `StateManagerBootstrap.yml` (un documento YAML).
2. Esegue il `aws:runDocument` plugin per eseguire il documento. `StateManagerBootstrap.yml` Non è specificato alcun parametro.
3. Esegue il plugin `aws:runDocument` per eseguire il documento SSM di `AWS-ConfigureDocker` pre-defined. I parametri specificati installano Docker sull'istanza.

```
{
 "schemaVersion": "2.2",
 "description": "My composite document for bootstrapping software and installing Docker.",
 "parameters": {
 },
 "mainSteps": [
 {
 "action": "aws:downloadContent",
 "name": "downloadContent",
 "inputs": {
 "sourceType": "GitHub",
 "sourceInfo": "{\"owner\":\"TestUser1\",\"repository\":\"TestPublic\", \"path\": \"documents/bootstrap/StateManagerBootstrap.yml\"}",
 "destinationPath": "bootstrap"
 }
 },
 {
 "action": "aws:runDocument",
 "name": "runDocument",
 "inputs": {
 "documentType": "LocalPath",
 "documentPath": "bootstrap",
 "documentParameters": "{}"
 }
 },
 {
 "action": "aws:runDocument",
 "name": "configureDocker",
 "inputs": {
 "documentType": "SSMDocument",
 "documentPath": "AWS-ConfigureDocker",
 "documentParameters": "{\"action\":\"Install\"}"
 }
 }
]
}
```

## Ulteriori informazioni

- Per ulteriori informazioni sul riavvio dei server e delle istanze quando usi Run Command per chiamare gli script, consulta [Gestione di riavvii durante l'esecuzione dei comandi](#).

- Per ulteriori informazioni sui plugin che è possibile aggiungere a un documento SSM personalizzato, consultare [Documentazione di riferimento del plugin per i documenti di comando](#).
- Se desideri eseguire un documento da una posizione remota (senza creare un documento composito), consulta [Esecuzione di documenti da posizioni remote](#).

## Utilizzo dei documenti

Questa sezione include informazioni su come utilizzare e gestire i documenti SSM.

### Argomenti

- [Confronta le versioni del documento SSM](#)
- [Crea un documento SSM](#)
- [Eliminazione di documenti SSM personalizzati](#)
- [Esecuzione di documenti da posizioni remote](#)
- [Condivisione di documenti SSM](#)
- [Ricerca di documenti SSM](#)

### Confronta le versioni del documento SSM

È possibile confrontare le differenze di contenuto tra le versioni dei documenti AWS Systems Manager (SSM) nella console Systems Manager Documents. Quando si confrontano le versioni di un documento SSM, vengono evidenziate le differenze di contenuto delle versioni.

Per confrontare il contenuto del documento SSM (console)

1. Aprire la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Documenti.
3. Nell'elenco dei documenti, scegliere il documento di cui si desidera confrontare il contenuto.
4. Sulla scheda Contenuti, seleziona Confronta versioni e scegli la versione del documento con cui si desidera confrontare il contenuto.

## Crea un documento SSM

Dopo aver creato il contenuto per il documento SSM personalizzato, come descritto in [Scrittura del contenuto del documento SSM](#), è possibile utilizzare la console di Systems Manager per creare un documento SSM tramite il contenuto.

Per creare un documento SSM

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Documenti.
3. Scegli Crea comando o sessione.
4. Inserisci un nome descrittivo per il documento.
5. (Facoltativo) Per Tipo di destinazione, specifica il tipo di risorse su cui è possibile eseguire il documento.
6. Nell'elenco Tipo di documento, scegli il tipo di documento che desideri creare.
7. Elimina le parentesi nel campo Contenuto, quindi incolla il documento creato in precedenza.
8. (Facoltativo) Nella sezione Tag del documento, applicate una o più name/value coppie di chiavi di tag al documento.

I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Ad esempio, è possibile assegnare un tag a un documento per identificare il tipo di attività che esegue, il tipo di sistemi operativi di destinazione e l'ambiente in cui viene eseguito. In questo caso, è possibile specificare le seguenti name/value coppie di chiavi:

- Key=TaskType, Value=MyConfigurationUpdate
- Key=OS, Value=AMAZON\_LINUX\_2
- Key=Environment, Value=Production

9. Scegli Crea documento per salvare il documento.

## Eliminazione di documenti SSM personalizzati

Se non si desidera più utilizzare un documento SSM personalizzato, è possibile eliminarlo utilizzando la console AWS Systems Manager .

## Per eliminare un documento SSM

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Documenti.
3. Selezionare il documento che si desidera eliminare.
4. Seleziona Elimina. Quando viene richiesto di eliminare il documento, seleziona Elimina.

Per esempi di utilizzo di strumenti da riga di comando o SDK per eliminare documenti SSM, consulta la sezione [Usare DeleteDocument con un AWS SDK o CLI](#).

## Esecuzione di documenti da posizioni remote

È possibile eseguire documenti AWS Systems Manager (SSM) da postazioni remote utilizzando il documento SSM AWS-RunDocument predefinito. Questo documento supporta l'esecuzione di documenti SSM memorizzati nelle seguenti posizioni:

- Repository GitHub pubblici e privati (GitHub Enterprise non è supportato)
- Bucket Amazon S3
- Systems Manager

Sebbene sia possibile eseguire documenti remoti anche utilizzando State Manager o Automation, tools in AWS Systems Manager, la procedura seguente descrive solo come eseguire documenti SSM remoti utilizzando la console di Systems AWS Systems Manager Run Command Manager.

### Note

AWS-RunDocument può essere utilizzato per eseguire solo documenti SSM di tipo comando, non altri tipi come i runbook di Automation. AWS-RunDocument utilizza il plugin `aws:downloadContent`. Per ulteriori informazioni sui plugin `aws:downloadContent`, consultare [aws:downloadContent](#).

### Warning

AWS-RunDocument può eseguire il contenuto dei documenti da varie fonti (documenti SSM, S3 GitHub, URL). Quando si eseguono documenti remoti, le autorizzazioni IAM valutate si



riferiscono al documento remoto e sono attive. `ssm:GetDocument` `ssm:SendCommand` `AWS-RunDocument` Se disponi di policy IAM che negano l'accesso a documenti SSM specifici, gli utenti con `AWS-RunDocument` autorizzazioni possono comunque eseguire quei documenti negati passando il contenuto del documento come parametro, che potrebbero non essere soggetti alle stesse restrizioni IAM specifiche del documento.

Per limitare correttamente l'esecuzione dei documenti, utilizza uno di questi approcci:

- Consenti l'accesso alle fonti approvate: se devi utilizzare l'esecuzione di documenti annidati, limita l'accesso solo alle fonti approvate. Usa le policy IAM `ssm:GetDocument` per controllare le fonti dei documenti SSM. Usa le policy dei bucket IAM e Amazon S3 per i sorgenti Amazon S3. Utilizza le impostazioni di rete (come endpoint VPC o gruppi di sicurezza) per le fonti Internet pubbliche.
- Limita l'accesso a `AWS-RunDocument`: Deny `ssm:SendCommand` on `AWS-RunDocument` e a qualsiasi altro documento che utilizza il `aws:runDocument` plug-in nelle tue policy IAM per impedire l'esecuzione di documenti annidati.
- Usa i limiti delle autorizzazioni: implementa i limiti delle autorizzazioni IAM per impostare le autorizzazioni massime per gli utenti, impedendo loro di eseguire documenti non autorizzati indipendentemente dal metodo di esecuzione.

Per ulteriori informazioni sulle best practice IAM e sui limiti delle autorizzazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'AWS Identity and Access Management utente.

## Prima di iniziare

Prima di eseguire un documento remoto devi completare le attività seguenti.

- Creare un documento SSM e salvarlo in una posizione remota. Per ulteriori informazioni, consulta [Creazione del contenuto del documento SSM](#)
- Se si decide di eseguire un documento remoto archiviato in un repository GitHub privato, è necessario creare un parametro `SecureString` di Systems Manager per il token di accesso di sicurezza a GitHub. Non è possibile accedere a un documento remoto in un repository GitHub privato trasferendo manualmente il token su SSH. Il token di accesso deve essere trasferito come parametro `SecureString` di Systems Manager. Per ulteriori informazioni sulla creazione di un parametro `SecureString`, consulta [Creazione in corso Parameter Store parametri in Systems Manager](#).

## Esecuzione di un documento remoto (console remota)

Per eseguire un documento remoto

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Run Command.
3. Seleziona Esegui comando.
4. Nell'elenco Document (Documento) scegliere **AWS-RunDocument**.
5. In Command parameters (Parametri di comando), per Source Type (Tipo di origine), scegliere un'opzione.
  - Se si sceglie GitHub, specificare le Source Info (Informazioni origine) nel formato seguente:

```
{
 "owner": "owner_name",
 "repository": "repository_name",
 "path": "path_to_document",
 "getOptions": "branch:branch_name",
 "tokenInfo": "{{ssm-secure:secure-string-token}}"
}
```

Ad esempio:

```
{
 "owner": "TestUser",
 "repository": "GitHubTestExamples",
 "path": "scripts/python/test-script",
 "getOptions": "branch:exampleBranch",
 "tokenInfo": "{{ssm-secure:my-secure-string-token}}"
}
```

### Note

getOptions sono opzioni aggiuntive per recuperare il contenuto da un ramo diverso dal master o da un commit specifico nel repository. getOptions può essere omissso se si utilizza l'ultimo commit nel ramo master. Il parametro branch è necessario solo se il documento SSM è memorizzato in un ramo diverso da master.

Per utilizzare la versione del documento SSM in un particolare commit nel repository, usare `commitID` con `getOptions` invece di `branch`. Ad esempio:

```
"getOptions": "commitID:bbc1ddb94...b76d3bEXAMPLE",
```

- Se si sceglie S3, specificare le Source Info (Informazioni origine) nel formato seguente:

```
{"path": "URL_to_document_in_S3"}
```

Ad esempio:

```
{"path": "https://s3.amazonaws.com/amzn-s3-demo-bucket/scripts/ruby/mySSMdoc.json"}
```

- Se si sceglie SSM Document, specificare le Source Info (Informazioni origine) nel formato seguente:

```
{"name": "document_name"}
```

Ad esempio:

```
{"name": "mySSMdoc"}
```

6. Nel campo Document Parameters (Parametri documento), inserire i parametri per il documento SSM remoto. Ad esempio, se si esegue il documento `AWS-RunPowerShell`, è possibile specificare:

```
{"commands": ["date", "echo \"Hello World\""]}
```

Se si esegue il documento `AWS-ConfigureAWSPack`, è possibile specificare:

```
{
 "action": "Install",
 "name": "AWSPVDriver"
}
```

7. Nella sezione Targets (Destinazioni), identificare i nodi in cui si desidera eseguire questa operazione specificando i tag, selezionando manualmente le istanze, i dispositivi edge o indicando un gruppo di risorse.

 Tip

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

8. In Altri parametri:

- In Commento, digita le informazioni su questo comando.
- In Timeout (secondi), specifica il numero di secondi che il sistema dovrà attendere prima di generare un errore per l'intera esecuzione del comando.

9. Per Controllo velocità:

- In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti presi di mira, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.
10. (Facoltativo) Nella sezione Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Scrivi l'output del comando in un bucket S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

 Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

11. Se vuoi che vengano inviate notifiche sullo stato dell'esecuzione del comando, nella sezione Notifiche SNS selezionare la casella di controllo Abilita notifiche SNS.

Per ulteriori informazioni sulla configurazione delle notifiche Amazon SNS per Run Command, consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

12. Scegli Esegui.

 Note

Per ulteriori informazioni sul riavvio dei server e delle istanze quando usi Run Command per chiamare gli script, consulta [Gestione di riavvii durante l'esecuzione dei comandi](#).

## Condivisione di documenti SSM

Puoi condividere documenti AWS Systems Manager (SSM) con altri account nello stesso modo Regione AWS in due modi. Per la condivisione di nuovi documenti, consigliamo di utilizzare AWS Resource Access Manager (AWS RAM). Con la AWS RAM, puoi condividere un documento con un'intera organizzazione o unità organizzativa (OU) in AWS Organizzazioni o con singoli individui Account AWS. Puoi anche gestire tutte le tue condivisioni dalla console AWS RAM. Per ulteriori informazioni, consulta [Condividi un documento SSM utilizzando AWS RAM](#).

Puoi condividere un documento anche utilizzando le autorizzazioni dell'account, il meccanismo di condivisione originale. Con le autorizzazioni dell'account, puoi modificare direttamente le

autorizzazioni del documento per condividerlo privatamente con Account AWS ID specifici o pubblicamente con tutti. Account-permission la condivisione rimane supportata. Per ulteriori informazioni, consulta [Condividi un documento SSM utilizzando le autorizzazioni dell'account](#).

Se condividi già documenti utilizzando le autorizzazioni dell'account, puoi migrare tali condivisioni nella RAM. AWS Per ulteriori informazioni, consulta [Esegui la migrazione di un documento condiviso esistente su AWS RAM](#).

Non puoi condividere un documento pubblicamente e privatamente allo stesso tempo. Inoltre, non puoi utilizzare la condivisione della AWS RAM e la condivisione delle autorizzazioni dell'account (ModifyDocumentPermission) sullo stesso documento contemporaneamente.

#### Warning

Utilizzare documenti SSM condivisi solo se provengono da fonti attendibili. Quando utilizzi un documento condiviso, verificane attentamente i contenuti prima di utilizzarlo per comprendere come modificherà la configurazione dell'istanza. Per ulteriori informazioni sulle best practice per i documenti condivisi, consulta [Best practice per documenti SSM condivisi](#).

## Limitazioni

Quando si iniziano a utilizzare documenti SSM, tenere presente le seguenti restrizioni.

- Soltanto il proprietario può condividere un documento.
- I documenti possono essere condivisi con altri account solo nello stesso Regione AWS account. Cross-Region la condivisione non è supportata.

#### Important

In Systems Manager, un documento Amazon-owned SSM è un documento creato e gestito da Amazon Web Services stesso. Amazon-ownedi documenti includono un prefisso come AWS-\* nel nome del documento. Il proprietario del documento è considerato Amazon, non un account utente specifico al suo interno AWS. Questi documenti sono disponibili al pubblico e possono essere utilizzati da tutti.

## Indice

- [Best practice per documenti SSM condivisi](#)
- [Bloccare la condivisione pubblica per i documenti SSM](#)
- [Condividi un documento SSM utilizzando AWS RAM](#)
- [Condividi un documento SSM utilizzando le autorizzazioni dell'account](#)
- [Utilizzo di documenti SSM condivisi](#)

## Best practice per documenti SSM condivisi

Consulta le seguenti linee guida prima di condividere o utilizzare un documento condiviso.

### Usa la AWS RAM per condividere documenti (consigliato)

Per la condivisione di nuovi documenti, consigliamo di utilizzare AWS Resource Access Manager (AWS RAM) anziché l'operazione `ModifyDocumentPermission` API. Quando condividi tramite AWS RAM, puoi condividere un documento con un'intera organizzazione o unità organizzativa (OU) in AWS Organizations invece di elencare Account AWS i singoli ID. Puoi anche gestire l'accesso con una policy basata sulle risorse e visualizzare e controllare tutte le tue condivisioni in un unico posto nella AWS console RAM. Per le fasi, consulta [Condividi un documento SSM utilizzando AWS RAM](#). I documenti che condividi con Account AWS ID individuali utilizzando `ModifyDocumentPermission` sono ancora supportati. Per spostare un documento che già condividi AWS nella RAM, consulta [Esegui la migrazione di un documento condiviso esistente su AWS RAM](#).

### Rimuovi le informazioni sensibili

Rivedi attentamente il tuo documento AWS Systems Manager (SSM) e rimuovi tutte le informazioni sensibili. Ad esempio, verifica che il documento non includa AWS le tue credenziali. Se condividi un documento con utenti specifici, questi possono visualizzare le informazioni contenute nel documento. Se condividi un documento pubblicamente, tutti possono visualizzare le informazioni contenute nel documento.

### Bloccare la condivisione pubblica per i documenti

Controlla tutti i documenti SSM condivisi pubblicamente nel tuo account e conferma se desideri continuare a condividerli. Per interrompere la condivisione di un documento con il pubblico, è necessario modificare l'impostazione delle autorizzazioni del documento come descritto nella sezione [Modifica delle autorizzazioni per un documento condiviso](#) di questo argomento. L'attivazione dell'impostazione di blocco della condivisione pubblica non ha effetto sui documenti che stai attualmente condividendo con il pubblico. A meno che il caso d'uso non richieda la

condivisione pubblica, si consiglia di attivare l'impostazione Blocca condivisione pubblica per i documenti SSM nella sezione Preferenze della console Documenti di Systems Manager. L'attivazione di questa impostazione impedisce l'accesso indesiderato ai documenti SSM. L'impostazione Blocca condivisione pubblica è un'impostazione a livello di account che può differire per ogni Regione AWS.

### Limitazione delle operazioni Run Command utilizzando una policy di attendibilità IAM

Crea una policy restrittiva AWS Identity and Access Management (IAM) per gli utenti che avranno accesso al documento. La policy IAM determina quali documenti SSM un utente può visualizzare nella console Amazon Elastic Compute Cloud (Amazon EC2) o chiamando `ListDocuments` utilizzando () o. AWS Command Line Interface AWS CLI AWS Tools for Windows PowerShell. La policy limita inoltre le operazioni che l'utente può eseguire con i documenti SSM. Puoi creare una policy restrittiva in modo che un utente possa utilizzare solo documenti specifici. Per ulteriori informazioni, consulta [Esempi di policy gestite dal cliente](#).

### Fare attenzione quando si utilizzano documenti SSM condivisi

È importante verificare i contenuti di ogni documento condiviso, soprattutto nel caso di documenti pubblici, per comprendere i comandi che verranno eseguiti sulle istanze. L'esecuzione di un documento potrebbe avere ripercussioni negative, anche in modo non intenzionale. Se il documento fa riferimento a una rete esterna, verifica quest'ultima prima di utilizzare il documento.

### Invia comandi utilizzando l'hash del documento

Quando condividi un documento, il sistema crea un Sha-256 hash e lo assegna al documento. Il sistema salva inoltre uno snapshot del contenuto del documento. Quando inviate un comando utilizzando un documento condiviso, potete specificare l'hash nel comando per assicurarvi che le seguenti condizioni siano vere:

- Si sta eseguendo un comando dal documento di Systems Manager corretto
- Il contenuto del documento non è stato modificato da quando è stato condiviso con l'utente.

Se l'hash non corrisponde al documento specificato o se il contenuto del documento condiviso è stato modificato, il comando restituisce un'eccezione `InvalidDocument` (Documento non valido). L'hash non è in grado di verificare il contenuto di un documento da percorsi esterni.

### Utilizzare il parametro di interpolazione per migliorare la sicurezza

Per i parametri di tipo `String` nei documenti SSM, utilizza il parametro e il valore `interpolationType": "ENV_VAR`, per migliorare la sicurezza contro gli attacchi di iniezione di comandi trattando gli input dei parametri come stringhe letterali, invece di comandi potenzialmente



eseguibili. In questo caso, l'agente crea una variabile di ambiente denominata `SSM_parameter-name`, che contiene il valore del parametro. Si consiglia di aggiornare tutti i documenti SSM esistenti che includono i parametri di tipo `String`, per includere `"interpolationType": "ENV_VAR"`. Per ulteriori informazioni, consulta [the section called "Scrittura del contenuto del documento SSM"](#).

## Bloccare la condivisione pubblica per i documenti SSM

Prima di iniziare, esamina tutti i documenti SSM condivisi pubblicamente in Account AWS e conferma se desideri continuare a condividerli. Per interrompere la condivisione di un documento SSM con il pubblico, è necessario modificare l'impostazione delle autorizzazioni del documento come descritto nella sezione [Modifica delle autorizzazioni per un documento condiviso](#) di questo argomento.

L'attivazione dell'impostazione di blocco della condivisione pubblica non influisce sui documenti SSM che stai attualmente condividendo con il pubblico. Con l'impostazione di blocco della condivisione pubblica abilitata, non sarai in grado di condividere altri documenti SSM con il pubblico.

A meno che il caso d'uso non richieda l'attivazione della condivisione pubblica, consigliamo di attivare l'impostazione Blocca condivisione pubblica per i documenti SSM. L'attivazione di questa impostazione impedisce l'accesso indesiderato ai documenti SSM. L'impostazione di blocco della condivisione pubblica è un'impostazione a livello di account che può differire per ciascuno Regione AWS. Completare le seguenti attività per bloccare la condivisione pubblica di qualsiasi documento SSM attualmente in condivisione.

### Blocca condivisione pubblica (console)

#### Bloccare la condivisione pubblica dei documenti SSM

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Documenti.
3. Scegli Preferenze, quindi scegli Modifica nella sezione Blocca condivisione pubblica.
4. Selezionare la casella Blocca condivisione pubblica, quindi scegli Salva.

### Blocca condivisione pubblica (riga di comando)

Apri AWS Command Line Interface (AWS CLI) o AWS Tools for Windows PowerShell sul tuo computer locale ed esegui il seguente comando per bloccare la condivisione pubblica dei tuoi documenti SSM.

## Linux & macOS

```
aws ssm update-service-setting \
 --setting-id /ssm/documents/console/public-sharing-permission \
 --setting-value Disable \
 --region 'The Regione AWS you want to block public sharing in'
```

## Windows

```
aws ssm update-service-setting ^
 --setting-id /ssm/documents/console/public-sharing-permission ^
 --setting-value Disable ^
 --region "The Regione AWS you want to block public sharing in"
```

## PowerShell

```
Update-SSMServiceSetting `
 -SettingId /ssm/documents/console/public-sharing-permission `
 -SettingValue Disable `
 -Region The Regione AWS you want to block public sharing in
```

Confermare che il valore dell'impostazione sia stato aggiornato utilizzando il seguente comando.

## Linux & macOS

```
aws ssm get-service-setting \
 --setting-id /ssm/documents/console/public-sharing-permission \
 --region The Regione AWS you blocked public sharing in
```

## Windows

```
aws ssm get-service-setting ^
 --setting-id /ssm/documents/console/public-sharing-permission ^
 --region "The Regione AWS you blocked public sharing in"
```

## PowerShell

```
Get-SSMServiceSetting `
 -SettingId /ssm/documents/console/public-sharing-permission `
 -Region The Regione AWS you blocked public sharing in
```

## Limitazione dell'accesso per bloccare la condivisione pubblica con IAM

È possibile creare policy AWS Identity and Access Management (IAM) che impediscano agli utenti di modificare l'impostazione di blocco della condivisione pubblica. Ciò impedisce agli utenti di consentire l'accesso indesiderato ai documenti SSM.

Di seguito è riportato un esempio di policy IAM che impedisce agli utenti di aggiornare l'impostazione di blocco della condivisione pubblica. Per utilizzare questo esempio, è necessario sostituire l'ID dell'account Amazon Web Services di esempio con il proprio ID dell'account.

### JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Deny",
 "Action": "ssm:UpdateServiceSetting",
 "Resource": "arn:aws:ssm:*:444455556666:servicesetting/ssm/documents/
console/public-sharing-permission"
 }
]
}
```

## Condividi un documento SSM utilizzando AWS RAM

AWS Resource Access Manager (AWS RAM) è il metodo consigliato per condividere documenti AWS Systems Manager (SSM). Con AWS RAM, si crea una condivisione di risorse che consente l'accesso al documento e si gestiscono tutte le condivisioni dalla console AWS RAM. Puoi condividere un documento SSM con i seguenti tre tipi di committenti:

- Un'intera organizzazione in AWS Organizzazioni.
- Un'unità organizzativa (OU) in AWS Organizzazioni.
- Individuale Account AWS.

È possibile condividere un documento solo con account appartenenti allo stesso Regione AWS e solo il proprietario del documento può condividere un documento. Per ulteriori informazioni sulla

condivisione con la AWS RAM, vedere Guida [introduttiva alla AWS RAM](#) nella Guida per l'utente di AWS Resource Access Manager.

 Important

Quando condividete un documento SSM utilizzando la AWS RAM, condividete tutte le versioni del documento, non solo la versione predefinita.

 Note

AWS La RAM supporta solo la condivisione privata. Per condividere un documento pubblicamente, utilizza [Condividi un documento SSM utilizzando le autorizzazioni dell'account](#) invece la procedura in.

 Note

Quando condividi un documento con un Account AWS utente esterno all'organizzazione, il consumatore deve accettare l'invito alla condivisione delle risorse nella AWS RAM prima di poter accedere al documento. Quando condividi all'interno di un'organizzazione in cui è abilitata la condivisione della AWS RAM, non è richiesto alcun invito e AWS RAM concede l'accesso automaticamente.

AWS Le quote di servizio RAM si applicano quando si condividono documenti SSM tramite RAM. AWS Per ulteriori informazioni, consulta Quote [di servizio per la AWS RAM](#) nella Guida per l'utente di AWS Resource Access Manager.

Per gestire una condivisione esistente (ad esempio, per aggiornare i principali o interrompere la condivisione di un documento condiviso tramite AWS RAM), vedi [Utilizzo AWS delle risorse condivise](#) nella Guida per l'utente di AWS Resource Access Manager.

Condividi un documento utilizzando AWS RAM (console)

Per condividere un documento utilizzando AWS RAM

1. Apri la console AWS RAM all'indirizzo <https://console.aws.amazon.com/ram/>.

2. Nel pannello di navigazione, scegli Condivisioni di risorse, quindi scegli Crea condivisione di risorse.
3. In Nome, inserisci un nome per la condivisione delle risorse.
4. In Risorse, scegli il tipo di risorsa SSM Documents, quindi seleziona il documento che desideri condividere.
5. (Facoltativo) In Autorizzazioni gestite, esamina l'autorizzazione gestita che AWS RAM applica al documento condiviso.
6. Scegli Avanti. In Principi, aggiungi l'organizzazione, le unità organizzative o con Account AWS cui desideri condividere. Per condividere con la tua organizzazione o un'unità organizzativa, devi abilitare la condivisione all'interno AWS delle organizzazioni.
7. Scegli Avanti, rivedi le tue scelte, quindi scegli Crea condivisione di risorse.

Condividi un documento usando AWS RAM (riga di comando)

Apri AWS Command Line Interface (AWS CLI) o AWS Tools for Windows PowerShell sul tuo computer locale ed esegui il seguente comando per condividere un documento creando una condivisione di risorse AWS RAM. Per il `--principals` parametro, specificate un ARN dell'organizzazione, un ARN dell'unità organizzativa o un Account AWS ID.

## Linux & macOS

```
aws ram create-resource-share \
 --name MyDocumentShare \
 --resource-arns arn:aws:ssm:region:account-id:document/document-name \
 --principals principal
```

## Windows

```
aws ram create-resource-share ^
 --name MyDocumentShare ^
 --resource-arns arn:aws:ssm:region:account-id:document/document-name ^
 --principals principal
```

 Note

Dopo aver creato una condivisione, la AWS RAM potrebbe impiegare alcuni minuti per propagare la modifica prima che gli account di consumo possano vederla.

## Esegui la migrazione di un documento condiviso esistente su AWS RAM

Se attualmente condividi un documento utilizzando le autorizzazioni dell'account (operazione `ModifyDocumentPermission` API), puoi migrarlo su una condivisione di risorse AWS RAM eseguendo il runbook `AWS-MigrateSSMDocumentSharingToRAM`. Questo runbook AWS di AWS Systems Manager Automation di proprietà migra un documento dalla condivisione delle autorizzazioni dell'account a una condivisione di risorse AWS RAM preservando i consumatori esistenti del documento.

 Note

L'esecuzione del `AWS-MigrateSSMDocumentSharingToRAM` runbook utilizza l'automazione, che comporta dei costi. AWS Systems Manager Per ulteriori informazioni, consulta [Prezzi di AWS Systems Manager](#).

 Note

Non puoi migrare un documento condiviso pubblicamente, perché la AWS RAM supporta solo la condivisione privata. Se si specifica un documento condiviso pubblicamente, il runbook ha esito negativo. Se esegui la migrazione di tutti i documenti dell'account, il runbook salta i documenti condivisi pubblicamente. Per migrare un documento condiviso pubblicamente, interrompi prima la condivisione pubblica e poi condividilo con gli account, le unità organizzative (OU) o l'organizzazione che desideri.

 Important

Dopo aver eseguito la migrazione di un documento, è possibile gestirne la condivisione tramite AWS RAM. Le operazioni `ModifyDocumentPermission` e `DescribeDocumentPermission` API restituiscono un errore 4xx per un documento

migrato. Se la migrazione fallisce o viene annullata, il runbook annulla automaticamente la modifica.

Per migrare un documento dalla relativa vista Autorizzazioni (console)

1. Apri la AWS Systems Manager console e, nel riquadro di navigazione, scegli Documenti.
2. Scegli il documento che desideri migrare.
3. Seleziona la scheda Details (Dettagli).
4. Nella sezione Autorizzazioni, scegli Migrate to RAM. Systems Manager apre la pagina Migrate to RAM, che consente di avviare la migrazione.
5. Per la migrazione dei documenti, seleziona i documenti da migrare. Seleziona singoli documenti o scegli Tutti i documenti per migrare tutti i documenti dell'account che utilizza la condivisione delle autorizzazioni dell'account.
6. Per AutomationAssumeRole, scegli il ruolo IAM che Systems Manager Automation assume per eseguire la migrazione.
7. (Facoltativo) Per le unità organizzative, aggiungi un ID dell'organizzazione o un ID dell'unità organizzativa (OU) con cui condividere i documenti.
8. Scegli Avvia migrazione.

Per l'elenco completo dei parametri, le autorizzazioni IAM richieste per il AutomationAssumeRole ruolo e le istruzioni dettagliate per l'esecuzione del runbook, consulta [AWS-MigrateSSMDocumentSharingToRAM](#) la guida di riferimento al runbook di Automation. AWS Systems Manager

Condividi un documento SSM utilizzando le autorizzazioni dell'account

Puoi condividere documenti AWS Systems Manager (SSM) modificando le autorizzazioni del documento per concedere l'accesso a Account AWS ID specifici (condivisione privata) o a tutti (condivisione pubblica). È possibile condividere documenti dalla console di Systems Manager o a livello di codice richiamando l'operazione ModifyDocumentPermission API utilizzando AWS Command Line Interface (AWS CLI) o l'SDK. AWS Tools for Windows PowerShell AWS Quando si condividono documenti dalla console, è possibile condividere solo la versione predefinita del documento. Prima di condividere un documento, recupera gli Account AWS ID degli account con cui desideri dividerlo. Specifica questi ID account quando condividi il documento.

 Note

Per la condivisione di nuovi documenti, consigliamo invece di utilizzare AWS Resource Access Manager (AWS RAM). Con la AWS RAM, puoi condividere con un'intera organizzazione o unità organizzativa e gestire tutte le tue condivisioni in un unico posto. Per ulteriori informazioni, consulta [Condividi un documento SSM utilizzando AWS RAM](#).

## Limitazioni

Tieni presente le seguenti limitazioni quando condividi un documento utilizzando le autorizzazioni dell'account.

- Devi interrompere la condivisione di un documento prima di poterlo eliminare. Per ulteriori informazioni, consulta [Modifica delle autorizzazioni per un documento condiviso](#).
- Puoi condividere un documento con un massimo di 1.000 Account AWS. È possibile richiedere un aumento di questo limite nel [Supporto Center](#). Per Limit type (Tipo di limite), scegliere EC2 Systems Manager e descrivere il motivo della richiesta.
- È possibile condividere pubblicamente un massimo di cinque documenti SSM. È possibile richiedere un aumento di questo limite nel [Supporto Center](#). Per Limit type (Tipo di limite), scegliere EC2 Systems Manager e descrivere il motivo della richiesta.

Per ulteriori informazioni sulle service quotas di Systems Manager, consulta [AWS Systems Manager Service Quotas](#).

## Condivisione di un documento (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Documenti.
3. Nell'elenco dei documenti, scegliere il documento che si desidera condividere, quindi selezionare View details (Visualizza dettagli). Nella scheda Permissions (Autorizzazioni), verificare di essere il proprietario del documento. Soltanto il proprietario di un documento può dividerlo.
4. Scegli Modifica.
5. Per condividere il comando pubblicamente, scegliere Public (Pubblico), quindi selezionare Save (Salva). Per condividere il comando privatamente, scegliere Private (Privato), inserire l'ID dell'Account AWS, selezionare Add permission (Aggiungi autorizzazione) e scegliere Save (Salva).



## Condivisione di un documento (riga di comando)

La procedura seguente richiede di specificare una Regione AWS per la sessione a riga di comando.

1. Aprire AWS CLI o AWS Tools for Windows PowerShell sul computer locale ed eseguire il comando seguente per specificare le credenziali.

Nel comando seguente, sostituisci *region* con le tue informazioni. Per un elenco dei *region* valori supportati, vedere la colonna Regione negli endpoint del servizio [Systems Manager](#) in. Riferimenti generali di Amazon Web Services

### Linux & macOS

```
aws config

AWS Access Key ID: [your key]
AWS Secret Access Key: [your key]
Default region name: region
Default output format [None]:
```

### Windows

```
aws config

AWS Access Key ID: [your key]
AWS Secret Access Key: [your key]
Default region name: region
Default output format [None]:
```

### PowerShell

```
Set-AWSCredentials -AccessKey your key -SecretKey your key
Set-DefaultAWSRegion -Region region
```

2. Utilizzare il comando seguente per visualizzare le autorizzazioni per il documento.

### Linux & macOS

```
aws ssm describe-document-permission \
 --name document name \
 --permission-type Share
```

## Windows

```
aws ssm describe-document-permission ^
 --name document name ^
 --permission-type Share
```

## PowerShell

```
Get-SSMDocumentPermission `
 -Name document name `
 -PermissionType Share
```

3. Utilizzare il comando seguente per modificare le autorizzazioni per il documento e condividerlo. È necessario essere il proprietario del documento per modificare le autorizzazioni. Facoltativamente, per documenti condivisi con specifici ID Account AWS , è possibile specificare una versione del documento da condividere utilizzando il parametro `--shared-document-version`. Se non specifichi una versione, il sistema condivide la versione Default del documento. Se condividi un documento pubblicamente (con `all`), tutte le versioni del documento specificato vengono condivise per impostazione predefinita. Il seguente comando di esempio condivide privatamente il documento con una persona specifica, in base all'ID di Account AWS quella persona.

## Linux & macOS

```
aws ssm modify-document-permission \
 --name document name \
 --permission-type Share \
 --account-ids-to-add Account AWS ID
```

## Windows

```
aws ssm modify-document-permission ^
 --name document name ^
 --permission-type Share ^
 --account-ids-to-add Account AWS ID
```

## PowerShell

```
Edit-SSMDocumentPermission `
```

```
-Name document name \
-PermissionType Share \
-AccountIdsToAdd Account AWS ID
```

4. Utilizzare il comando seguente per condividere un documento pubblicamente.

#### Note

Se condividi un documento pubblicamente (con `all`), tutte le versioni del documento specificato vengono condivise per impostazione predefinita.

## Linux & macOS

```
aws ssm modify-document-permission \
 --name document name \
 --permission-type Share \
 --account-ids-to-add 'all'
```

## Windows

```
aws ssm modify-document-permission ^
 --name document name ^
 --permission-type Share ^
 --account-ids-to-add "all"
```

## PowerShell

```
Edit-SSMDocumentPermission \
 -Name document name \
 -PermissionType Share \
 -AccountIdsToAdd ('all')
```

## Modifica delle autorizzazioni per un documento condiviso

Se condividi un comando, gli utenti possono visualizzarlo e utilizzarlo finché non rimuovi l'accesso al documento AWS Systems Manager (SSM) o elimini il documento SSM. Tuttavia, non è possibile eliminare un documento finché è condiviso. Devi interrompere la condivisione prima di poterlo eliminare.

 Note

Questa sezione si applica ai documenti che hai condiviso utilizzando le autorizzazioni dell'account. Per gestire un documento che hai condiviso tramite AWS RAM, consulta [Condividi un documento SSM utilizzando AWS RAM](#).

## Interruzione della condivisione di un documento (console)

## Interrompere la condivisione di un documento

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Documenti.
3. Nell'elenco dei documenti, scegliere il documento di cui si desidera interrompere la condivisione, quindi selezionare Details (dettagli). Nella sezione Permissions (Autorizzazioni), verificare di essere il proprietario del documento. Soltanto il proprietario del documento può interromperne la condivisione.
4. Scegli Modifica.
5. Scegli **X** per eliminare l' Account AWS ID che non dovrebbe più avere accesso al comando, quindi scegli Salva.

## Interruzione della condivisione di un documento (riga di comando)

Apri AWS CLI o AWS Tools for Windows PowerShell sul tuo computer locale ed esegui il comando seguente per interrompere la condivisione di un documento.

## Linux &amp; macOS

```
aws ssm modify-document-permission \
 --name document name \
 --permission-type Share \
 --account-ids-to-remove 'Account AWS ID'
```

## Windows

```
aws ssm modify-document-permission ^
 --name document name ^
```

```
--permission-type Share ^
--account-ids-to-remove "Account AWS ID"
```

## PowerShell

```
Edit-SSMDocumentPermission `
-Name document name `
-PermissionType Share `
-AccountIdsToRemove Account AWS ID
```

## Utilizzo di documenti SSM condivisi

Quando condividi un documento AWS Systems Manager (SSM), il sistema genera un Amazon Resource Name (ARN) e lo assegna al comando. Se si seleziona e si esegue un documento condiviso dalla console di Systems Manager, non si visualizza l'ARN. Tuttavia, se si desidera eseguire un documento SSM condiviso utilizzando un metodo diverso dalla console di Systems Manager, è necessario specificare l'ARN completo del documento per il parametro di richiesta `DocumentName`. L'ARN completo per un documento SSM viene mostrato quando si esegue il comando per elencare i documenti.

### Note

Non è necessario specificare gli ARN per i documenti AWS pubblici (documenti che iniziano con `AWS-`) o i documenti di tua proprietà.

## Utilizzare un documento SSM condiviso (riga di comando)

### Per elencare tutti i documenti SSM pubblici

## Linux & macOS

```
aws ssm list-documents \
--filters Key=Owner,Values=Public
```

## Windows

```
aws ssm list-documents ^
--filters Key=Owner,Values=Public
```

## PowerShell

```
$filter = New-Object Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter
$filter.Key = "Owner"
$filter.Values = "Public"

Get-SSMDocumentList `
 -Filters @($filter)
```

Per elencare i documenti SSM privati che sono stati condivisi con l'utente

## Linux & macOS

```
aws ssm list-documents \
 --filters Key=Owner,Values=Private
```

## Windows

```
aws ssm list-documents ^
 --filters Key=Owner,Values=Private
```

## PowerShell

```
$filter = New-Object Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter
$filter.Key = "Owner"
$filter.Values = "Private"

Get-SSMDocumentList `
 -Filters @($filter)
```

Per elencare tutti i documenti SSM disponibili per l'utente

## Linux & macOS

```
aws ssm list-documents
```

## Windows

```
aws ssm list-documents
```

## PowerShell

```
Get-SSMDocumentList
```

Per ottenere informazioni su un documento SSM che è stato condiviso con l'utente

## Linux & macOS

```
aws ssm describe-document \
 --name arn:aws:ssm:us-east-2:12345678912:document/documentName
```

## Windows

```
aws ssm describe-document ^
 --name arn:aws:ssm:us-east-2:12345678912:document/documentName
```

## PowerShell

```
Get-SSMDocumentDescription `
 -Name arn:aws:ssm:us-east-2:12345678912:document/documentName
```

Per eseguire un documento SSM condiviso

## Linux & macOS

```
aws ssm send-command \
 --document-name arn:aws:ssm:us-east-2:12345678912:document/documentName \
 --instance-ids ID
```

## Windows

```
aws ssm send-command ^
 --document-name arn:aws:ssm:us-east-2:12345678912:document/documentName ^
 --instance-ids ID
```

## PowerShell

```
Send-SSMCommand `
```

```
-DocumentName arn:aws:ssm:us-east-2:12345678912:document/documentName `
-InstanceIds ID
```

## Ricerca di documenti SSM

È possibile cercare documenti SSM nell'archivio documenti AWS Systems Manager (SSM) utilizzando la ricerca a testo libero o una ricerca basata su filtri. Per trovare più facilmente i documenti SSM usati di frequente, puoi aggiungerli ai tuoi preferiti. Le sezioni seguenti descrivono come utilizzare queste funzionalità.

### Utilizzo della ricerca a testo libero

La casella di ricerca nella pagina Documenti di Systems Manager supporta la ricerca a testo libero. La ricerca a testo libero confronta il termine o i termini di ricerca immessi con il nome del documento in ogni documento SSM. Se si immette un singolo termine di ricerca, ad esempio **ansible**, Systems Manager restituisce tutti i documenti SSM in cui è stato trovato questo termine. Se si immettono più termini di ricerca, Systems Manager esegue la ricerca utilizzando un'istruzione OR. Ad esempio, se si specifica **ansible** e **linux**, la ricerca restituisce tutti i documenti con una delle parole chiave nel nome.

Se si immette un termine di ricerca a testo libero e si sceglie un'opzione di ricerca, ad esempio Tipo di piattaforma, la ricerca utilizza un'istruzione AND e restituisce tutti i documenti con la parola chiave nel nome e il tipo di piattaforma specificato.

#### Note

Notare i seguenti dettagli relativi alla ricerca a testo libero.

- La ricerca a testo libero non fa distinzione tra maiuscole e minuscole.
- I termini di ricerca devono avere un minimo di tre caratteri e un massimo di 20 caratteri
- La ricerca a testo libero accetta fino a cinque termini di ricerca.
- Se si immette uno spazio fra i termini di ricerca, il sistema include lo spazio durante la ricerca.
- È possibile combinare la ricerca a testo libero con altre opzioni di ricerca, ad esempio Tipo di documento o Tipo di piattaforma.
- Il filtro relativo al Prefisso del nome del documento e la ricerca a testo libero non possono essere utilizzati insieme. Si escludono a vicenda.



## Per cercare un documento SSM

1. Apri la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Documenti.
3. Inserire i termini di ricerca nella casella di ricerca e premere Invio.

## Esecuzione della ricerca di documenti a testo libero utilizzando il AWS CLI

### Eseguire una ricerca di documenti a testo libero utilizzando il CLI

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Per effettuare la ricerca di documenti a testo libero con un singolo termine, eseguire il comando seguente. In questo comando, *search\_term* sostituisco con le tue informazioni.

```
aws ssm list-documents --filters Key="SearchKeyword",Values="search_term"
```

Ecco un esempio:

```
aws ssm list-documents --filters Key="SearchKeyword",Values="aws-asg" --region us-east-2
```

Per eseguire ricerche utilizzando più termini che creano un'istruzione AND, eseguire il comando seguente. In questo comando, sostituisci *search\_term\_1* e *search\_term\_2* con le tue informazioni.

```
aws ssm list-documents --filters
Key="SearchKeyword",Values="search_term_1","search_term_2","search_term_3" --
region us-east-2
```

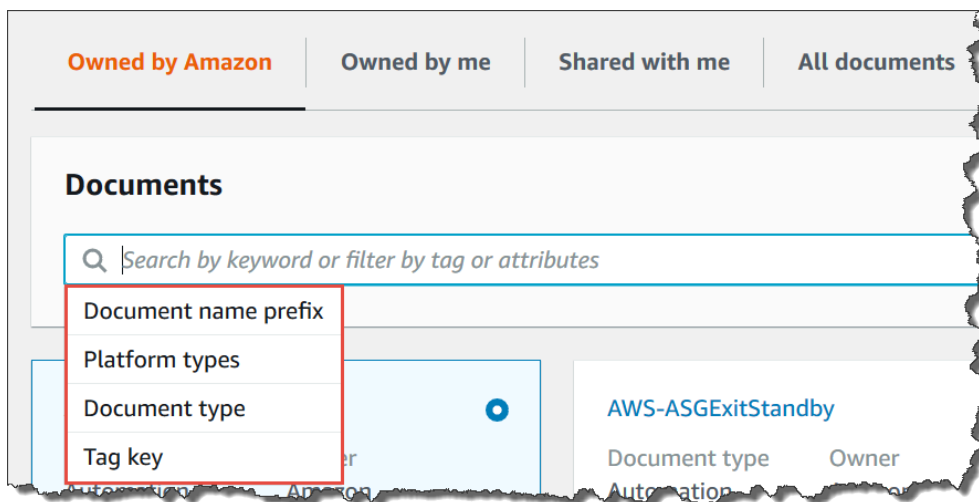
Ecco un esempio:

```
aws ssm list-documents --filters Key="SearchKeyword",Values="aws-asg","aws-ec2","restart" --region us-east-2
```

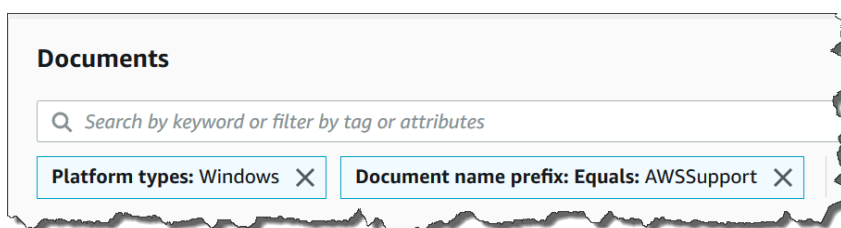
## Utilizzo dei filtri

La pagina Documenti di Systems Manager visualizza automaticamente i seguenti filtri quando si sceglie la casella di ricerca.

- Prefisso del nome del documento
- Tipi di piattaforma
- Tipo di documento
- Chiave tag



È possibile cercare documenti SSM utilizzando un singolo filtro. Se si desidera restituire un insieme più specifico di documenti SSM, è possibile applicare più filtri. Di seguito è riportato un esempio di ricerca che utilizza i filtri Tipi di piattaforma e Prefisso del nome del documento.



Se si applicano più filtri, Systems Manager crea istruzioni di ricerca diverse in base ai filtri scelti:

- Se si applica lo stesso filtro più volte, ad esempio Prefisso del nome del documento, Systems Manager esegue la ricerca utilizzando un'istruzione OR. Ad esempio, se si specifica un filtro di Prefisso del nome del documento=**AWS** e un secondo filtro di Prefisso del nome del

documento=**Lambda**, la ricerca restituisce tutti i documenti con il prefisso "AWS" e tutti i documenti con il prefisso "Lambda".

- Se applichi filtri diversi, ad esempio Prefisso del nome del documento e Tipi di piattaforma, Systems Manager esegue la ricerca utilizzando un'istruzione AND. Ad esempio, se specifichi un filtro Prefisso del nome del documento=**AWS** (=) e un filtro Tipi di piattaforma=**Linux** (=), la ricerca restituirà tutti i documenti con il prefisso "AWS" specifici per la piattaforma Linux.

#### Note

Le ricerche che utilizzano i filtri fanno distinzione tra maiuscole e minuscole.

### Aggiunta di documenti ai preferiti

Per trovare più facilmente i documenti SSM usati di frequente, aggiungili ai tuoi preferiti. Puoi aggiungere ai preferiti fino a 20 documenti per tipo di documento, per Account AWS e Regione AWS. Puoi scegliere, modificare e visualizzare i tuoi preferiti dalla Console di gestione AWS Documenti. Le procedure seguenti descrivono come scegliere, modificare e visualizzare i preferiti.

#### Aggiunta di un documento SSM ai preferiti

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Documenti.
3. Seleziona l'icona a forma di stella accanto al nome del documento che desideri aggiungere ai preferiti.

#### Rimozione di un documento SSM dai preferiti

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Documenti.
3. Deseleziona l'icona a forma di stella accanto al nome del documento che desideri rimuovere dai preferiti.

Per visualizzare i preferiti dai documenti Console di gestione AWS

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Documenti.
3. Seleziona la scheda Preferiti.

## Risoluzione dei problemi di gestione dei parametri

### Problemi comuni di gestione dei parametri

#### Variabili di ambiente non disponibili durante l'esecuzione

Problema: i comandi fanno errore, perché le variabili di ambiente (SSM\_*parameter-name*) non vengono trovate.

Possibili cause:

- La versione dell'SSM Agent non supporta l'interpolazione delle variabili di ambiente
- `interpolationType` non è impostato su `ENV_VAR`
- Il nome del parametro non corrisponde a quello della variabile di ambiente previsto

Soluzione::

- Verifica che la versione dell'SSM Agent sia 3.3.2746.0 o successiva
- Aggiungi la logica di fallback per le versioni precedenti dell'agente:

```
if [-z "${SSM_parameterName+x}"]; then
 export SSM_parameterName="{{parameterName}}"
fi
```

#### Valori di parametri contenenti caratteri speciali

Problema: i comandi fanno errore, quando i valori dei parametri contengono spazi, virgolette o altri caratteri speciali.

Soluzione::

- Usa le virgolette corrette, quando fai riferimento alle variabili di ambiente:

```
Correct
```

```
echo "$SSM_parameter-name"

Incorrect
echo $SSM_parameter-name
```

- Aggiungi la convalida dell'input utilizzando `allowedPattern` per limitare i caratteri speciali

Comportamento incoerente tra le piattaforme

Problema: la gestione dei parametri funziona in modo diverso su Linux e sui sistemi Windows Server.

Soluzione::

- Utilizza la sintassi delle variabili di ambiente specifica della piattaforma:

```
PowerShell
$env:SSM_parameter-name

Bash
$SSM_parameter-name
```

- Utilizza i controlli delle precondizioni specifici della piattaforma nel tuo documento

I valori dei parametri non sono stati correttamente esposti a escape

Problema: vulnerabilità di iniezione di comandi nonostante l'utilizzo dell'interpolazione delle variabili di ambiente.

Soluzione::

- Usa sempre l'escape corretto, quando includi i valori dei parametri nei comandi:

```
Correct
mysql_command="mysql -u \"\$SSM_username\" -p\"\$SSM_password\""

Incorrect
mysql_command="mysql -u $SSM_username -p$SSM_password"
```

Consigli per la convalida dei parametri

Usa queste tecniche per convalidare la gestione dei parametri:

1. Testa la disponibilità delle variabili di ambiente:

```
#!/bin/bash
Print all SSM_ environment variables
env | grep ^SSM_

Test specific parameter
if [-n "$SSM_parameter"]; then
 echo "Parameter is available"
else
 echo "Parameter is not available"
fi
```

## 2. Verifica i modelli dei parametri:

```
parameters:
 myParameter:
 type: String
 allowedPattern: "^[a-zA-Z0-9_-]+$"
 description: "Test this pattern with sample inputs"
```

## 3. Includi la gestione degli errori:

```
if [[! "$SSM_parameter" =~ ^[a-zA-Z0-9_-]+$]]; then
 echo "Parameter validation failed"
 exit 1
fi
```

# AWS Systems Manager Intervallo di manutenzione

Maintenance Windowsconsente di definire una pianificazione per l'esecuzione di azioni potenzialmente dannose sui nodi, ad esempio l'applicazione di patch a un sistema operativo, l'aggiornamento dei driver o l'installazione di software o patch.

### Note

State Manager e Maintenance Windows sono in grado di eseguire alcuni tipi di aggiornamenti simili sui nodi gestiti. La scelta dipende dalla necessità di automatizzare la conformità del sistema o di eseguire attività ad alta priorità e sensibili al tempo durante i periodi specificati. Per ulteriori informazioni, consulta [Scelta tra State Manager and Intervallo di manutenzione](#).

Con Maintenance Windows, puoi pianificare azioni su numerosi altri tipi di AWS risorse, come bucket Amazon Simple Storage Service (Amazon S3), code Amazon Simple Queue Service (Amazon SQS), chiavi () e molte altre. AWS Key Management Service AWS KMS

Per un elenco completo dei tipi di risorse supportati che puoi includere in una finestra di manutenzione, consulta [Risorse utilizzabili con AWS Resource Groups e Tag Editor nella Guida per l'utente](#). AWS Resource Groups Per cominciare a utilizzare Maintenance Windows, apri la [console di Systems Manager](#). Nel pannello di navigazione, scegli Maintenance Windows.

Ogni finestra di manutenzione ha una pianificazione, una durata massima, una serie di obiettivi registrati (i nodi gestiti o altre AWS risorse su cui si interviene) e una serie di attività registrate. È possibile aggiungere tag alle finestre di manutenzione quando vengono create o aggiornate. I tag sono chiavi che consentono di identificare e ordinare le risorse all'interno della tua organizzazione. Puoi anche indicare delle date prima o dopo le quali la finestra di manutenzione non deve essere eseguita, nonché specificare il fuso orario internazionale su cui basare la pianificazione della finestra di manutenzione.

Per una spiegazione di come le diverse opzioni relative alla pianificazione per le finestre di manutenzione siano tra loro correlate, consulta [Opzioni di pianificazione e periodo attivo per la finestra di manutenzione](#).

Per ulteriori informazioni sull'utilizzo dell'opzione `--schedule`, consulta [Riferimento: espressioni Cron e della frequenza per Systems Manager](#).

## Tipi di processi supportati

Con le finestre di manutenzione è possibile eseguire quattro tipi di attività:

- Comandi in Run Command, uno strumento di Systems Manager

Per ulteriori informazioni su Run Command, consultare [AWS Systems Manager Run Command](#).

- Flussi di lavoro in Automazione, uno strumento di Systems Manager

Per ulteriori informazioni sui flussi di lavoro di automazione, consulta [AWS Systems Manager Automazione di](#).

- Funziona in AWS Lambda

Per ulteriori informazioni sulle funzioni Lambda, consulta [Nozioni di base su Lambda](#) nella Guida per gli sviluppatori di AWS Lambda .

- Compiti in AWS Step Functions

 Note

Le attività della finestra di manutenzione supportano solo i flussi di lavoro delle macchine a stati standard di Step Functions. Non supportano i flussi di lavoro delle macchine a stati express. Per informazioni sui tipi di flusso di lavoro delle macchine a stati, consulta [Standard vs. Express Workflows](#) (Differenze flussi di lavoro standard ed express) nella Guida per gli sviluppatori di AWS Step Functions .

Per ulteriori informazioni su Step Functions, consulta la [Guida per sviluppatori di AWS Step Functions](#).

Questo significa che è possibile utilizzare le finestre di manutenzione per eseguire attività quali le seguenti sulle destinazioni selezionate.

- Installazione o aggiornamento di applicazioni.
- Applicazione di patch.
- Installazione o aggiornamento dell'SSM Agent.
- Esegui PowerShell comandi e script di shell Linux utilizzando un'Run Commandattività di Systems Manager.
- Creazione di Amazon Machine Images (AMIs), bootstrap di software e configurazione di nodi utilizzando l'attività di automazione Systems Manager.
- Esegui AWS Lambda funzioni che richiamano azioni aggiuntive, come la scansione dei nodi per gli aggiornamenti delle patch.
- Esegui macchine a AWS Step Functions stati per eseguire attività come rimuovere un nodo da un ambiente Elastic Load Balancing, applicare patch al nodo e quindi aggiungere nuovamente il nodo all'ambiente Elastic Load Balancing.
- Scegli come target i nodi che sono offline specificando un gruppo di AWS risorse come destinazione.

 Note

È necessario specificare uno o più oggetti per le attività di tipo Run Command della finestra di manutenzione. A seconda dell'attività, le destinazioni sono opzionali per altri tipi di attività



della finestra di manutenzione (Automazione e AWS Step Functions). AWS Lambda Per ulteriori informazioni sull'esecuzione di attività che non specificano destinazioni, consulta [Registrazione delle attività della finestra di manutenzione senza destinazioni](#).

## EventBridge supporto

Questo strumento Systems Manager è supportato come tipo di evento nelle EventBridge regole di Amazon. Per informazioni, consulta [Monitoraggio degli eventi di Systems Manager con Amazon EventBridge](#) e [Riferimento: modelli e tipi di EventBridge eventi Amazon per Systems Manager](#).

## Indice

- [Configurazione Intervallo di manutenzione](#)
- [Crea e gestisci finestre di manutenzione utilizzando la console](#)
- [Esercitazioni](#)
- [Utilizzo degli pseudo parametri durante la registrazione delle attività della finestra di manutenzione](#)
- [Opzioni di pianificazione e periodo attivo per la finestra di manutenzione](#)
- [Registrazione delle attività della finestra di manutenzione senza destinazioni](#)
- [Risoluzione dei problemi di finestre di manutenzione](#)

## Configurazione Intervallo di manutenzione

Prima che gli utenti del tuo account Account AWS possano creare e pianificare le attività della finestra di manutenzione utilizzando Maintenance Windows, devono disporre delle autorizzazioni necessarie. Inoltre, è necessario creare un ruolo di servizio IAM per le finestre di manutenzione e la policy IAM da allegare ad esso.

### Prima di iniziare

Oltre alle autorizzazioni configurate in questa sezione, è necessario che le entità IAM (utenti, ruoli o gruppi) che funzioneranno con le finestre di manutenzione dispongano già delle autorizzazioni generali relative alle finestre di manutenzione. È possibile concedere queste autorizzazioni assegnando la policy IAM AmazonSSMFullAccess alle Entità, oppure assegnando un'altra policy IAM personalizzata che fornisce un insieme più piccolo di autorizzazioni di accesso per Systems Manager che copre le attività delle finestre di manutenzione.

## Argomenti

- [Controllo degli accessi alle finestre di manutenzione tramite la console](#)
- [Controlla l'accesso alle finestre di manutenzione utilizzando il AWS CLI](#)

## Controllo degli accessi alle finestre di manutenzione tramite la console

Le procedure seguenti descrivono come utilizzare la AWS Systems Manager console per creare le autorizzazioni e i ruoli richiesti per le finestre di manutenzione.

### Argomenti

- [Attività 1: crea una policy personalizzata per il ruolo di servizio della finestra di manutenzione tramite la console](#)
- [Attività 2: crea un ruolo di servizio personalizzato per le finestre di manutenzione tramite la console](#)
- [Attività 3: concedi le autorizzazioni per l'uso del ruolo di servizio agli utenti che registrano le attività della finestra di manutenzione tramite la console](#)
- [Attività 4: impedisce agli utenti specificati di registrare le attività della finestra di manutenzione tramite la console](#)

### Attività 1: crea una policy personalizzata per il ruolo di servizio della finestra di manutenzione tramite la console

Le attività della finestra di manutenzione richiedono un ruolo IAM per concedere le autorizzazioni necessarie per l'esecuzione sulle risorse di destinazione. Le autorizzazioni vengono fornite tramite una policy IAM collegata al ruolo. I tipi di attività eseguite e gli altri requisiti operativi determinano il contenuto di questa policy. Forniamo una policy di base da poter adattare alle proprie esigenze. A seconda delle attività e dei tipi di attività eseguite dalle finestre di manutenzione, è possibile che non tutte le autorizzazioni in questa policy siano necessarie, mentre potrebbe rendersi necessario includere autorizzazioni aggiuntive. Dovrai collegare questa policy al ruolo che creerai successivamente in [Attività 2: crea un ruolo di servizio personalizzato per le finestre di manutenzione tramite la console](#).

Per creare una policy personalizzata tramite la console

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, scegli Policy e Crea policy.
3. Nella sezione Editor di policy, scegli l'opzione JSON.
4. Sostituisci i contenuti di default con il seguente:

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:SendCommand",
 "ssm:CancelCommand",
 "ssm:ListCommands",
 "ssm:ListCommandInvocations",
 "ssm:GetCommandInvocation",
 "ssm:GetAutomationExecution",
 "ssm:StartAutomationExecution",
 "ssm:ListTagsForResource",
 "ssm:DescribeInstanceInformation",
 "ssm:GetParameters"
],
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "states:DescribeExecution",
 "states:StartExecution"
],
 "Resource": [
 "arn:aws:states:::execution:*:*",
 "arn:aws:states:::stateMachine:*"
]
 },
 {
 "Effect": "Allow",
 "Action": [
 "lambda:InvokeFunction"
],
 "Resource": [
 "arn:aws:lambda:::function:*"
]
 }
]
}
```

```

 "Effect": "Allow",
 "Action": [
 "resource-groups:ListGroupResources"
],
 "Resource": [
 "*"
]
 },
 {
 "Effect": "Allow",
 "Action": [
 "tag:GetResources"
],
 "Resource": [
 "*"
]
 },
 {
 "Effect": "Allow",
 "Action": "iam:PassRole",
 "Resource": "arn:aws:iam::111122223333:role/maintenance-window-
role-name",
 "Condition": {
 "StringEquals": {
 "iam:PassedToService": [
 "ssm.amazonaws.com"
]
 }
 }
 }
]
}

```

5. Modifica il contenuto JSON secondo necessità per le attività di manutenzione eseguite nel tuo account. Le modifiche apportate sono specifiche per le operazioni pianificate.

Ad esempio:

- Puoi fornire nomi della risorsa Amazon (ARN) per funzioni specifiche e macchine a stati invece di utilizzare i qualificatori jolly (\*).
- Se non hai intenzione di eseguire AWS Step Functions attività, puoi rimuovere le states autorizzazioni e gli ARN.

- Se non hai intenzione di eseguire AWS Lambda attività, puoi rimuovere le lambda autorizzazioni e gli ARN.
- Se non prevedi l'esecuzione di attività di automazione, puoi rimuovere le autorizzazioni `ssm:GetAutomationExecution` e `ssm:StartAutomationExecution`.
- Aggiungi le autorizzazioni supplementari che potrebbero essere necessarie per l'esecuzione delle attività. Ad esempio, alcune operazioni di automazione utilizzano gli stack di AWS CloudFormation . Pertanto, servono le autorizzazioni `cloudformation:CreateStack`, `cloudformation:DescribeStacks` e `cloudformation>DeleteStack`.

Un altro esempio: il runbook Automation AWS-CopySnapshot richiede le autorizzazioni per creare uno snapshot Amazon Elastic Block Store (Amazon EBS). Pertanto, il ruolo di servizio richiede l'autorizzazione `ec2:CreateSnapshot`.

Per informazioni sulle autorizzazioni di ruolo necessarie per i runbook di automazione, consulta le descrizioni dei runbook nella [Documentazione di riferimento ai runbook di automazione AWS Systems Manager](#).

6. Dopo aver completato le revisioni delle policy, scegli Successivo.
7. Alla voce Nome policy, inserisci un nome che la identifichi come la policy utilizzata dal ruolo di servizio che crei. Ad esempio: **my-maintenance-window-role-policy**.
8. (Facoltativo) Nella sezione Aggiungi tag, aggiungi una o più coppie tag chiave-valore per organizzare, monitorare o controllare l'accesso per questa policy.
9. Scegli Crea policy.

Prendi nota del nome specificato per la policy. Vi farai riferimento nella procedura successiva, [Attività 2: crea un ruolo di servizio personalizzato per le finestre di manutenzione tramite la console](#).

Attività 2: crea un ruolo di servizio personalizzato per le finestre di manutenzione tramite la console

La policy che hai creato nell'attività precedente è associata al ruolo di servizio della finestra di manutenzione che crei in questa attività. Quando gli utenti registrano un'attività della finestra di manutenzione, specificano questo ruolo IAM come parte della configurazione dell'attività. Le autorizzazioni in questo ruolo consentono a Systems Manager di eseguire attività nelle finestre di manutenzione per conto tuo.

 Important

In precedenza, la console di Systems Manager offriva la possibilità di scegliere il ruolo AWS gestito collegato ai servizi IAM `AWSServiceRoleForAmazonSSM` da utilizzare come ruolo di manutenzione per le attività. Non è più consigliato utilizzare questo ruolo e la relativa policy associata, `AmazonSSMServiceRolePolicy`, per le attività della finestra di manutenzione. Se stai ancora utilizzando questo ruolo per le attività della finestra di manutenzione, ti invitiamo a interromperne l'utilizzo. È invece possibile creare un ruolo IAM personalizzato che consenta la comunicazione tra Systems Manager e altri utenti Servizi AWS durante l'esecuzione delle attività della finestra di manutenzione.

Utilizza la seguente procedura per creare un ruolo di servizio personalizzato per Maintenance Windows in modo che Systems Manager possa eseguire le attività Maintenance Windows per tuo conto. Collegherai la policy che hai creato nell'attività precedente al ruolo di servizio personalizzato che andrai a creare.

Per creare un ruolo di servizio personalizzato per le finestre di manutenzione tramite la console

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, scegli Ruoli e quindi Crea ruolo.
3. Per Seleziona un'entità attendibile, effettua le seguenti selezioni:
  1. Per Tipo di entità attendibile, scegli Servizio AWS .
  2. Alla voce Caso d'uso, scegli Systems Manager
  3. Scegli Systems Manager.

L'immagine seguente evidenzia la posizione dell'opzione Systems Manager.

## Service or use case

Systems Manager ▼

Choose a use case for the specified service.

## Use case

- ☒ **Systems Manager**  
Allows SSM to call AWS services on your behalf
- ☐ **Systems Manager - Inventory and Maintenance Windows**  
Allow AWS Systems Manager to call AWS resources on your behalf.

4. Scegli Successivo.
5. Nella sezione Policy di autorizzazione, nella barra di ricerca, inserisci il nome della policy creata in [Attività 1: crea una policy personalizzata per il ruolo di servizio della finestra di manutenzione tramite la console](#), seleziona il campo accanto al suo nome, quindi scegli Successivo.
6. In Nome ruolo, inserisci un nome che identifichi questo ruolo come un ruolo Maintenance Windows. Ad esempio: **my-maintenance-window-role**.
7. (Facoltativo) Modificare la descrizione predefinita del ruolo per rispecchiarne lo scopo. Ad esempio: **Performs maintenance window tasks on your behalf**.
8. Per il passaggio 1: seleziona le entità attendibili, verifica che la seguente policy sia visualizzata nel campo Politica attendibile.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "",
 "Effect": "Allow",
 "Principal": {
 "Service": "ssm.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
]
}
```

9. Per il passaggio 2: aggiungi le autorizzazioni, verifica che la politica creata in [Attività 1: crea una policy personalizzata per il ruolo di servizio della finestra di manutenzione tramite la console](#) sia presente.
10. (Facoltativo) Nel passaggio 3: aggiungi tag, aggiungi una o più coppie tag chiave-valore per organizzare, monitorare o controllare l'accesso per questo ruolo.
11. Scegli Crea ruolo. Il sistema visualizza di nuovo la pagina Ruoli.
12. Scegli il nome del ruolo IAM appena creato.
13. Copia o annota il nome del ruolo e il valore ARN nell'area Riepilogo. Gli utenti nel tuo account specificano queste informazioni quando creano finestre di manutenzione.

Attività 3: concedi le autorizzazioni per l'uso del ruolo di servizio agli utenti che registrano le attività della finestra di manutenzione tramite la console

La concessione agli utenti delle autorizzazioni di accesso al ruolo di servizio personalizzato per la finestra di manutenzione consente loro di utilizzarlo con le attività delle finestre di manutenzione. Si tratta di un'aggiunta alle autorizzazioni già concesse agli utenti per lavorare con i comandi dell'API di Systems Manager dello strumento Maintenance Windows. Questo ruolo IAM trasmette le autorizzazioni necessarie per eseguire un'attività della finestra di manutenzione. Di conseguenza, un utente non può registrare le attività con una finestra di manutenzione utilizzando il ruolo di servizio personalizzato senza la possibilità di passare queste autorizzazioni IAM.

Quando registri un'attività con una finestra di manutenzione, devi specificare un ruolo di servizio per eseguire le operazioni dell'attività effettiva. È il ruolo che assume il servizio durante l'esecuzione di attività per conto dell'utente. Prima di ciò, per registrare l'attività stessa, assegna la policy IAM `PassRole` a un'entità IAM (come un utente o un gruppo). Ciò consente all'entità IAM di specificare, nell'ambito della registrazione di tali attività nella finestra di manutenzione, il ruolo da utilizzare durante l'esecuzione delle attività. Per informazioni, consulta [Concedi autorizzazioni utente per il passaggio di un ruolo a Servizio AWS](#) nella Guida per l'utente IAM.

Per configurare le autorizzazioni per gli utenti che registrano le attività della finestra di manutenzione

Se a un'entità IAM (utente, ruolo o gruppo) vengono assegnate le autorizzazioni di amministratore, l'utente o il ruolo IAM ha accesso alle funzionalità delle finestre di manutenzione. Per le entità IAM senza autorizzazioni di amministratore, un amministratore deve concedere le seguenti autorizzazioni all'entità IAM. Queste sono le autorizzazioni minime necessarie per registrare le attività con una finestra di manutenzione:

- La policy gestita `AmazonSSMFullAccess` o una policy che fornisce autorizzazioni analoghe.



- Le seguenti autorizzazioni `iam:PassRole` e `iam:ListRoles`.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "iam:PassRole",
 "Resource": "arn:aws:iam::111122223333:role/my-maintenance-window-
role"
 },
 {
 "Effect": "Allow",
 "Action": "iam:ListRoles",
 "Resource": "arn:aws:iam::111122223333:role/"
 },
 {
 "Effect": "Allow",
 "Action": "iam:ListRoles",
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/
ssm.amazonaws.com/"
 }
]
}
```

*my-maintenance-window-role* rappresenta il nome del ruolo personalizzato del servizio della finestra di manutenzione creato in precedenza.

*account-id* rappresenta l'ID del tuo Account AWS. L'aggiunta di questa autorizzazione per la risorsa `arn:aws:iam::account-id:role/` consente a un utente di visualizzare e scegliere tra i ruoli del cliente nella console quando crea un'attività della finestra di manutenzione. L'aggiunta di questa autorizzazione per `arn:aws:iam::account-id:role/aws-service-role/ssm.amazonaws.com/` consente a un utente di scegliere il ruolo collegato ai servizi di Systems Manager nella console quando crea un'attività della finestra di manutenzione.

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 configurare le autorizzazioni per i gruppi autorizzati a registrare le attività della finestra di manutenzione tramite la console

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, seleziona Gruppi di utenti.
3. Nell'elenco dei gruppi, seleziona il nome del gruppo desiderato a cui assegnare l'autorizzazione `iam:PassRole` oppure, se necessario, crea un nuovo gruppo
4. Nella scheda Autorizzazioni, scegli Aggiungi autorizzazioni, Crea policy in linea.
5. Nella sezione Editor di policy, scegli l'opzione JSON e sostituisci i contenuti di default del campo con quanto segue.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "iam:PassRole",
 "Resource": "arn:aws:iam::111122223333:role/my-maintenance-
window-role"
 },
 {
```

```
 "Effect": "Allow",
 "Action": "iam:ListRoles",
 "Resource": "arn:aws:iam::111122223333:role/"
 },
 {
 "Effect": "Allow",
 "Action": "iam:ListRoles",
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/
ssm.amazonaws.com/"
 }
]
```

*my-maintenance-window-role* rappresenta il nome del ruolo personalizzato della finestra di manutenzione creato in precedenza.

*account-id* rappresenta l'ID del tuo Account AWS. L'aggiunta di questa autorizzazione per la risorsa `arn:aws:iam::account-id:role/` consente a un utente di visualizzare e scegliere tra i ruoli del cliente nella console quando crea un'attività della finestra di manutenzione. L'aggiunta di questa autorizzazione per `arn:aws:iam::account-id:role/aws-service-role/ssm.amazonaws.com/` consente a un utente di scegliere il ruolo collegato ai servizi di Systems Manager nella console quando crea un'attività della finestra di manutenzione.

6. Scegli Avanti.
7. Alla pagina Esamina e crea, inserisci un nome nel campo Nome policy per identificare questa policy `PassRole`, ad esempio **my-group-iam-passrole-policy**, quindi scegli Crea policy.

Attività 4: impedisci agli utenti specificati di registrare le attività della finestra di manutenzione tramite la console

Puoi negare l'`ssm:RegisterTaskWithMaintenanceWindow` autorizzazione agli utenti del tuo Account AWS account a cui non desideri registrare le attività nelle finestre di manutenzione. Ciò fornisce un ulteriore livello di prevenzione per gli utenti che non devono registrare le attività della finestra di manutenzione.

Per configurare le autorizzazioni per i gruppi non autorizzati a registrare le attività della finestra di manutenzione tramite la console

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.

2. Nel pannello di navigazione, seleziona Gruppi di utenti.
3. Nell'elenco dei gruppi, seleziona il nome del gruppo a cui desideri negare l'autorizzazione `ssm:RegisterTaskWithMaintenanceWindow` oppure, se necessario, crea un nuovo gruppo.
4. Nella scheda Autorizzazioni, scegli Aggiungi autorizzazioni, Crea policy in linea.
5. Nella sezione Editor di policy, scegli l'opzione JSON e successivamente sostituisci i contenuti di default del campo con quanto segue.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Deny",
 "Action": "ssm:RegisterTaskWithMaintenanceWindow",
 "Resource": "*"
 }
]
}
```

6. Scegli Avanti.
7. Alla pagina Esamina e crea, alla voce Nome policy, inserisci un nome per identificare questa policy, ad esempio **my-groups-deny-mw-tasks-policy**, quindi scegli Crea policy.

Controlla l'accesso alle finestre di manutenzione utilizzando il AWS CLI

Le procedure seguenti descrivono come utilizzare AWS Command Line Interface (AWS CLI) per creare le autorizzazioni e i ruoli richiesti per Maintenance Windows

## Argomenti

- [Attività 1: crea file di policy di fiducia e di policy gestita dal cliente in formato JSON](#)
- [Attività 2: Creare e verificare un ruolo di servizio personalizzato per le finestre di manutenzione utilizzando il AWS CLI](#)
- [Attività 3: concedi le autorizzazioni agli utenti specificati per registrare le attività della finestra di manutenzione utilizzando il AWS CLI](#)
- [Attività 4: Impedire agli utenti specificati di registrare le attività della finestra di manutenzione utilizzando il AWS CLI](#)

## Attività 1: crea file di policy di fiducia e di policy gestita dal cliente in formato JSON

Le attività della finestra di manutenzione richiedono un ruolo IAM per concedere le autorizzazioni necessarie per l'esecuzione sulle risorse di destinazione. Le autorizzazioni vengono fornite tramite una policy IAM collegata al ruolo. I tipi di attività eseguite e gli altri requisiti operativi determinano il contenuto di questa policy. Forniamo una policy di base da poter adattare alle proprie esigenze. A seconda delle attività e dei tipi di attività eseguite dalle finestre di manutenzione, è possibile che non tutte le autorizzazioni in questa policy siano necessarie, mentre potrebbe rendersi necessario includere autorizzazioni aggiuntive.

In questa attività, specificherai le autorizzazioni necessarie per il ruolo della finestra di manutenzione personalizzata in un paio di file JSON. Dovrai collegare questa policy al ruolo che creerai successivamente in [Attività 2: Creare e verificare un ruolo di servizio personalizzato per le finestre di manutenzione utilizzando il AWS CLI](#).

Per creare file di policy di fiducia e di policy gestita dal cliente

1. Copiare e incollare la seguente policy di attendibilità in un file di testo. Salva il file con il nome ed estensione seguenti: **mw-role-trust-policy.json**.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "ssm.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
]
}
```

2. Copia e incolla la seguente policy JSON in un file di testo diverso. Nella stessa directory in cui hai creato il primo file, salva questo file con il nome e l'estensione seguenti: **mw-role-custom-policy.json**.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:SendCommand",
 "ssm:CancelCommand",
 "ssm:ListCommands",
 "ssm:ListCommandInvocations",
 "ssm:GetCommandInvocation",
 "ssm:GetAutomationExecution",
 "ssm:StartAutomationExecution",
 "ssm:ListTagsForResource",
 "ssm:GetParameters"
],
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "states:DescribeExecution",
 "states:StartExecution"
],
 "Resource": [
 "arn:aws:states:::execution:*:*",
 "arn:aws:states:::stateMachine:*"
]
 },
 {
 "Effect": "Allow",
 "Action": [
 "lambda:InvokeFunction"
],
 "Resource": [
 "arn:aws:lambda:::function:*"
]
 },
 {
 "Effect": "Allow",
```

```

 "Action": [
 "resource-groups:ListGroup",
 "resource-groups:ListGroupResources"
],
 "Resource": [
 "*"
]
 },
 {
 "Effect": "Allow",
 "Action": [
 "tag:GetResources"
],
 "Resource": [
 "*"
]
 },
 {
 "Effect": "Allow",
 "Action": "iam:PassRole",
 "Resource": "arn:aws:iam::111122223333:role/maintenance-window-
role-name",
 "Condition": {
 "StringEquals": {
 "iam:PassedToService": [
 "ssm.amazonaws.com"
]
 }
 }
 }
]
}

```

3. Modifica il contenuto di `mw-role-custom-policy.json` in base alle necessità per le attività di manutenzione eseguite nel tuo account. Le modifiche apportate sono specifiche per le operazioni pianificate.

Ad esempio:

- Puoi fornire nomi della risorsa Amazon (ARN) per funzioni specifiche e macchine a stati invece di utilizzare i qualificatori jolly (\*).
- Se non intendi eseguire AWS Step Functions attività, puoi rimuovere le `states` autorizzazioni e gli ARN.

- Se non hai intenzione di eseguire AWS Lambda attività, puoi rimuovere le lambda autorizzazioni e gli ARN.
- Se non prevedi l'esecuzione di attività di automazione, puoi rimuovere le autorizzazioni `ssm:GetAutomationExecution` e `ssm:StartAutomationExecution`.
- Aggiungi le autorizzazioni supplementari che potrebbero essere necessarie per l'esecuzione delle attività. Ad esempio, alcune operazioni di automazione utilizzano gli stack di AWS CloudFormation . Pertanto, servono le autorizzazioni `cloudformation:CreateStack`, `cloudformation:DescribeStacks` e `cloudformation>DeleteStack`.

Un altro esempio: il runbook Automation AWS-CopySnapshot richiede le autorizzazioni per creare uno snapshot Amazon Elastic Block Store (Amazon EBS). Pertanto, il ruolo di servizio richiede l'autorizzazione `ec2:CreateSnapshot`.

Per informazioni sulle autorizzazioni di ruolo necessarie per i runbook di automazione, consulta le descrizioni dei runbook nella [Documentazione di riferimento ai runbook di automazione AWS Systems Manager](#).

Salva nuovamente il file dopo aver apportato le modifiche necessarie.

**Attività 2:** Creare e verificare un ruolo di servizio personalizzato per le finestre di manutenzione utilizzando il AWS CLI

La policy che hai creato nell'attività precedente è associata al ruolo di servizio della finestra di manutenzione che crei in questa attività. Quando gli utenti registrano un'attività della finestra di manutenzione, specificano questo ruolo IAM come parte della configurazione dell'attività. Le autorizzazioni in questo ruolo consentono a Systems Manager di eseguire attività nelle finestre di manutenzione per conto tuo.

#### Important

In precedenza, la console di Systems Manager offriva la possibilità di scegliere il ruolo AWS gestito collegato al servizio IAM `AWSServiceRoleForAmazonSSM` da utilizzare come ruolo di manutenzione per le attività. Non è più consigliato utilizzare questo ruolo e la relativa policy associata, `AmazonSSMServiceRolePolicy`, per le attività della finestra di manutenzione. Se stai ancora utilizzando questo ruolo per le attività della finestra di manutenzione, ti invitiamo a interromperne l'utilizzo. È invece possibile creare un ruolo IAM personalizzato



che consenta la comunicazione tra Systems Manager e altri utenti Servizi AWS durante l'esecuzione delle attività della finestra di manutenzione.

In questa attività, eseguirai i comandi CLI per creare il ruolo di servizio delle finestre di manutenzione, aggiungendo il contenuto della policy dai file JSON che hai creato.

Crea un ruolo di servizio personalizzato per le finestre di manutenzione utilizzando AWS CLI

1. Apri AWS CLI ed esegui il seguente comando nella directory in cui hai inserito `mw-role-custom-policy.json` e `mw-role-trust-policy.json`. Il comando crea un ruolo di servizio della finestra di manutenzione chiamato `my-maintenance-window-role`, a cui collega la policy di fiducia.

#### Linux & macOS

```
aws iam create-role \
 --role-name "my-maintenance-window-role" \
 --assume-role-policy-document file://mw-role-trust-policy.json
```

#### Windows

```
aws iam create-role ^
 --role-name "my-maintenance-window-role" ^
 --assume-role-policy-document file://mw-role-trust-policy.json
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "Role": {
 "AssumeRolePolicyDocument": {
 "Version": "2012-10-17",
 "Statement": [
 {
 "Action": "sts:AssumeRole",
 "Effect": "Allow",
 "Principal": {
 "Service": "ssm.amazonaws.com"
 }
 }
]
 }
 }
}
```

```
],
 },
 "RoleId": "AROAIIZKPBKS2LEXAMPLE",
 "CreateDate": "2024-08-19T03:40:17.373Z",
 "RoleName": "my-maintenance-window-role",
 "Path": "/",
 "Arn": "arn:aws:iam::123456789012:role/my-maintenance-window-role"
 }
}
```

#### Note

Annota i valori di RoleName e Arn. Dovrai includerli nel comando successivo.

2. Esegui il seguente comando per collegare la policy gestita dal cliente al ruolo. Sostituisci il *account-id* segnaposto con il tuo ID Account AWS

#### Linux & macOS

```
aws iam attach-role-policy \
 --role-name "my-maintenance-window-role" \
 --policy-arn "arn:aws:iam::account-id:policy/mw-role-custom-policy.json"
```

#### Windows

```
aws iam attach-role-policy ^
 --role-name "my-maintenance-window-role" ^
 --policy-arn "arn:aws:iam::account-id:policy/mw-role-custom-policy.json"
```

3. Esegui il seguente comando per verificare che il ruolo sia stato creato e che la policy di fiducia sia stata collegata.

```
aws iam get-role --role-name my-maintenance-window-role
```

Questo comando restituisce informazioni simili alle seguenti:

```
{
 "Role": {
 "Path": "/",
 "RoleName": "my-maintenance-window-role",
```

```
"RoleId": "ARO123456789EXAMPLE",
"Arn": "arn:aws:iam::123456789012:role/my-maintenance-window-role",
"CreateDate": "2024-08-19T14:13:32+00:00",
"AssumeRolePolicyDocument": {
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "ssm.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
]
},
"MaxSessionDuration": 3600,
"RoleLastUsed": {
 "LastUsedDate": "2024-08-19T14:30:44+00:00",
 "Region": "us-east-2"
}
}
```

4. Esegui il seguente comando per verificare che la policy gestita dal cliente sia stata collegata al ruolo.

```
aws iam list-attached-role-policies --role-name my-maintenance-window-role
```

Questo comando restituisce informazioni simili alle seguenti:

```
{
 "AttachedPolicies": [
 {
 "PolicyName": "mw-role-custom-policy",
 "PolicyArn": "arn:aws:iam::123456789012:policy/mw-role-custom-policy"
 }
]
}
```

### Attività 3: concedi le autorizzazioni agli utenti specificati per registrare le attività della finestra di manutenzione utilizzando il AWS CLI

La concessione agli utenti delle autorizzazioni di accesso al ruolo di servizio personalizzato per la finestra di manutenzione consente loro di utilizzarlo con le attività delle finestre di manutenzione. Si tratta di un'aggiunta alle autorizzazioni già concesse agli utenti per lavorare con i comandi dell'API di Systems Manager dello strumento Maintenance Windows. Questo ruolo IAM trasmette le autorizzazioni necessarie per eseguire un'attività della finestra di manutenzione. Di conseguenza, un utente non può registrare le attività con una finestra di manutenzione utilizzando il ruolo di servizio personalizzato senza la possibilità di passare queste autorizzazioni IAM.

Quando registri un'attività con una finestra di manutenzione, devi specificare un ruolo di servizio per eseguire le operazioni dell'attività effettiva. È il ruolo che assume il servizio durante l'esecuzione di attività per conto dell'utente. Prima di ciò, per registrare l'attività stessa, assegna la policy IAM `PassRole` a un'entità IAM (come un utente o un gruppo). Ciò consente all'entità IAM di specificare, nell'ambito della registrazione di tali attività nella finestra di manutenzione, il ruolo da utilizzare durante l'esecuzione delle attività. Per informazioni, consulta [Concedi autorizzazioni utente per il passaggio di un ruolo a Servizio AWS](#) nella Guida per l'utente IAM.

Per configurare le autorizzazioni per gli utenti autorizzati a registrare le attività della finestra di manutenzione utilizzando AWS CLI

1. Copia e incolla la seguente policy AWS Identity and Access Management (IAM) in un editor di testo e salvala con il nome e l'estensione di file seguenti: `mw-passrole-policy.json`.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "iam:PassRole",
 "Resource": "arn:aws:iam::111122223333:role/my-maintenance-
window-role"
 },
 {
 "Effect": "Allow",
 "Action": "iam:ListRoles",
 "Resource": "arn:aws:iam::111122223333:role/"
 }
]
}
```

```
 },
 {
 "Effect": "Allow",
 "Action": "iam:ListRoles",
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/
ssm.amazonaws.com/"
 }
]
}
```

Sostituisci *my-maintenance-window-role* con il nome del ruolo della finestra di manutenzione personalizzata che hai creato in precedenza.

Sostituisci *account-id* con l'ID del tuo Account AWS. L'aggiunta di questa autorizzazione per la risorsa `arn:aws:iam::account-id:role/` consente agli utenti del gruppo di visualizzare e scegliere tra i ruoli dei clienti nella console quando creano un'attività della finestra di manutenzione. L'aggiunta di questa autorizzazione per `arn:aws:iam::account-id:role/aws-service-role/ssm.amazonaws.com/` consente agli utenti del gruppo di scegliere il ruolo Systems Manager collegato ai servizi nella console quando creano un'attività della finestra di manutenzione.

2. Apri il AWS CLI.
3. Per concedere l'autorizzazione a un'entità IAM (utente o gruppo), esegui uno dei seguenti comandi.

- Per un'entità IAM:

Linux & macOS

```
aws iam put-user-policy \
 --user-name "user-name" \
 --policy-name "policy-name" \
 --policy-document file://path-to-document
```

Windows

```
aws iam put-user-policy ^
 --user-name "user-name" ^
 --policy-name "policy-name" ^
 --policy-document file://path-to-document
```

Per *user-name*, specificare l'utente che assegna le attività alle finestre di manutenzione. Per *policy-name*, specifica il nome che desideri utilizzare per identificare la politica, ad esempio **my-iam-passrole-policy**. Per *path-to-document*, specifica il percorso del file salvato nel passaggio 1. Ad esempio: `file://C:\Temp\mw-passrole-policy.json`

#### Note

Per concedere l'accesso di un utente alla registrazione delle attività delle finestre di manutenzione utilizzando la console di Systems Manager, è inoltre necessario assegnare la policy `AmazonSSMFullAccess` all'utente (o una policy IAM che fornisca un insieme più piccolo di autorizzazioni di accesso per Systems Manager che esegue le attività delle finestre di manutenzione). Per assegnare la policy `AmazonSSMFullAccess` all'utente, esegui questo comando.

#### Linux & macOS

```
aws iam attach-user-policy \
 --policy-arn "arn:aws:iam::aws:policy/AmazonSSMFullAccess" \
 --user-name "user-name"
```

#### Windows

```
aws iam attach-user-policy ^
 --policy-arn "arn:aws:iam::aws:policy/AmazonSSMFullAccess" ^
 --user-name "user-name"
```

- Per un gruppo IAM:

#### Linux & macOS

```
aws iam put-group-policy \
 --group-name "group-name" \
 --policy-name "policy-name" \
 --policy-document file://path-to-document
```

#### Windows

```
aws iam put-group-policy ^
 --group-name "group-name" ^
```

```
--policy-name "policy-name" ^
--policy-document file://path-to-document
```

Per *group-name*, specifica il gruppo i cui membri assegnano le attività alle finestre di manutenzione. Per *policy-name*, specifica il nome che desideri utilizzare per identificare la politica, ad esempio **my-iam-passrole-policy**. Per *path-to-document*, specifica il percorso del file salvato nel passaggio 1. Ad esempio: `file://C:\Temp\mw-passrole-policy.json`

#### Note

Per concedere l'accesso ai membri di un gruppo per registrare le attività per le finestre di manutenzione utilizzando la console di Systems Manager, è anche necessario assegnare la policy AmazonSSMFullAccess al gruppo. Per assegnare questa policy al gruppo esegui il seguente comando.

Linux & macOS

```
aws iam attach-group-policy \
 --policy-arn "arn:aws:iam::aws:policy/AmazonSSMFullAccess" \
 --group-name "group-name"
```

Windows

```
aws iam attach-group-policy ^
 --policy-arn "arn:aws:iam::aws:policy/AmazonSSMFullAccess" ^
 --group-name "group-name"
```

4. Esegui il seguente comando per verificare che la policy sia stata assegnata al gruppo.

Linux & macOS

```
aws iam list-group-policies \
 --group-name "group-name"
```

Windows

```
aws iam list-group-policies ^
 --group-name "group-name"
```

## Attività 4: Impedire agli utenti specificati di registrare le attività della finestra di manutenzione utilizzando il AWS CLI

Puoi negare l'`ssm:RegisterTaskWithMaintenanceWindow` autorizzazione agli utenti del tuo account Account AWS che non desideri registrare le attività nelle finestre di manutenzione. Ciò fornisce un ulteriore livello di prevenzione per gli utenti che non devono registrare le attività della finestra di manutenzione.

A seconda del fatto che l'autorizzazione `ssm:RegisterTaskWithMaintenanceWindow` non venga assegnata a uno specifico utente o a un gruppo, utilizzare una delle procedure seguenti per impedire agli utenti di registrare attività con una finestra di manutenzione.

Per configurare le autorizzazioni per gli utenti a cui non è consentito registrare le attività della finestra di manutenzione utilizzando AWS CLI

1. Copia e incolla la seguente policy IAM in un editor di testo e salvala con il seguente nome ed estensione del file: **deny-mw-tasks-policy.json**.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Deny",
 "Action": "ssm:RegisterTaskWithMaintenanceWindow",
 "Resource": "*"
 }
]
}
```

2. Aprire il AWS CLI
3. Per concedere l'autorizzazione a un'entità IAM (utente o gruppo), esegui uno dei seguenti comandi.

- Per un utente:

Linux & macOS

```
aws iam put-user-policy \
 --user-name "user-name" \
```



```
--policy-name "policy-name" \
--policy-document file://path-to-document
```

## Windows

```
aws iam put-user-policy ^
 --user-name "user-name" ^
 --policy-name "policy-name" ^
 --policy-document file://path-to-document
```

Per *user-name*, specificare l'utente per impedire l'assegnazione di attività alle finestre di manutenzione. Per *policy-name*, specifica il nome che desideri utilizzare per identificare la politica, ad esempio **my-deny-mw-tasks-policy**. Per *path-to-document*, specifica il percorso del file salvato nel passaggio 1. Ad esempio: file://C:\Temp\deny-mw-tasks-policy.json

- Per un gruppo:

## Linux & macOS

```
aws iam put-group-policy \
 --group-name "group-name" \
 --policy-name "policy-name" \
 --policy-document file://path-to-document
```

## Windows

```
aws iam put-group-policy ^
 --group-name "group-name" ^
 --policy-name "policy-name" ^
 --policy-document file://path-to-document
```

Per *group-name*, specificate il gruppo a cui impedire l'assegnazione delle attività alle finestre di manutenzione. Per *policy-name*, specifica il nome che desideri utilizzare per identificare la policy, ad esempio **my-deny-mw-tasks-policy**. Per *path-to-document*, specifica il percorso del file salvato nel passaggio 1. Ad esempio: file://C:\Temp\deny-mw-tasks-policy.json

4. Esegui il seguente comando per verificare che la policy sia stata assegnata al gruppo.

## Linux & macOS

```
aws iam list-group-policies \
 --group-name "group-name"
```

## Windows

```
aws iam list-group-policies ^
 --group-name "group-name"
```

## Crea e gestisci finestre di manutenzione utilizzando la console

Questa sezione descrive come creare, configurare, aggiornare ed eliminare le finestre di manutenzione utilizzando la AWS Systems Manager console. Questa sezione fornisce anche informazioni sulla gestione delle destinazioni e delle attività di una finestra di manutenzione.

### Important

Consigliamo di iniziare creando e configurando finestre di manutenzione in un ambiente di test.

## Prima di iniziare

Prima di creare una finestra di manutenzione, è necessario configurare l'accesso a Maintenance Windows, uno strumento in AWS Systems Manager. Per ulteriori informazioni, consulta [Configurazione Intervallo di manutenzione](#).

## Argomenti

- [Creare una finestra di manutenzione utilizzando la console](#)
- [Assegnazione di destinazioni a una finestra di manutenzione utilizzando la console](#)
- [Assegnazione di attività a una finestra di manutenzione utilizzando la console](#)
- [Disabilitare o abilitare una finestra di manutenzione utilizzando la console](#)
- [Aggiorna o elimina le risorse della finestra di manutenzione utilizzando la console](#)

## Creare una finestra di manutenzione utilizzando la console

In questa procedura si crea una finestra di manutenzione in Maintenance Windows, uno strumento di AWS Systems Manager. È possibile specificare le opzioni di base, ad esempio nome, pianificazione e durata. Nelle fasi successive potrai scegliere le destinazioni, o risorse, aggiornate dalla finestra e le attività svolte quando viene eseguita la finestra di manutenzione.

### Note

Per una spiegazione di come le diverse opzioni relative alla pianificazione per le finestre di manutenzione siano tra loro correlate, consulta [Opzioni di pianificazione e periodo attivo per la finestra di manutenzione](#).

Per ulteriori informazioni sull'utilizzo dell'opzione `--schedule`, consulta [Riferimento: espressioni Cron e della frequenza per Systems Manager](#).

Per creare una finestra di manutenzione utilizzando la console

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Maintenance Windows.
3. Scegli Crea finestra di manutenzione.
4. Nel campo Name (Nome), inserire un nome descrittivo che aiuti a identificare questa finestra di manutenzione.
5. (Facoltativo) In Description (Descrizione), inserisci una descrizione per identificare come verrà utilizzata questa finestra di manutenzione.
6. (Facoltativo) Per consentire a un'attività di una finestra di manutenzione di essere eseguita su nodi gestiti, anche se tali nodi non sono stati registrati come destinazioni, scegliere Allow unregistered targets (Consenti destinazioni non registrate).

Se si sceglie questa opzione, è possibile scegliere i nodi non registrati (per ID nodo) quando si registra un'attività sulla finestra di manutenzione.

Se non si sceglie questa opzione, è necessario scegliere destinazioni precedentemente registrate quando si registra un'attività sulla finestra di manutenzione.

7. Specifica una pianificazione per la finestra di manutenzione utilizzando una delle tre opzioni di pianificazione.

Per informazioni sulla creazione di cron/rate espressioni, vedere [Riferimento: espressioni Cron e della frequenza per Systems Manager](#).

8. Per Durata, inserisci il numero di ore di esecuzione della finestra di manutenzione. Il valore specificato determina l'ora di fine specifica per la finestra di manutenzione in base all'ora di inizio. Nessuna attività della finestra di manutenzione può essere avviata dopo l'ora di fine risultante meno il numero di ore specificato per Arresta l'inizializzazione di attività nella fase successiva.

Ad esempio, se la finestra di manutenzione inizia alle 15:00, la durata è di tre ore e il valore Arresta l'inizializzazione di attività è un'ora, nessuna attività della finestra di manutenzione può iniziare dopo le 17:00.

9. In Stop initiating tasks (Interrompi l'avvio delle attività), inserire il numero di ore prima del termine della finestra di manutenzione a partire dalle quali il sistema deve interrompere la pianificazione dell'esecuzione di nuove attività.
10. (Facoltativo) Per la data di inizio della finestra, specificate una data e un'ora, in formato ISO-8601 esteso, per quando desiderate che la finestra di manutenzione diventi attiva. Ciò consente di ritardare l'attivazione della finestra di manutenzione fino alla data futura specificata.

 Note

Non è possibile specificare una data e un'ora di inizio passate.

11. (Facoltativo) Per la data di fine della finestra, specifica una data e un'ora, in formato ISO-8601 esteso, per quando desideri che la finestra di manutenzione diventi inattiva. Ciò consente di impostare una data e un'ora future dopo le quali la finestra di manutenzione non verrà più eseguita.
12. (Facoltativo) In Schedule timezone (Pianifica fuso orario), specificare il fuso orario da utilizzare come base quando vengono eseguite le finestre di manutenzione pianificate, nel formato IANA (Internet Assigned Numbers Authority). Ad esempio: "America/Los\_Angeles», "etc/UTC«, o "Asia/Seoul».

Per ulteriori informazioni sui formati validi, consulta il [Database dei fusi orari](#) sul sito web IANA.

13. (Facoltativo) In Pianifica offset, inserisci il numero di giorni di attesa dopo la data e l'ora specificate da un'espressione Cron o della frequenza prima dell'esecuzione della finestra di manutenzione. È possibile specificare da uno a sei giorni.

 Note

Questa opzione è disponibile solo se è stata specificata una pianificazione immettendo manualmente un'espressione Cron o della frequenza.

14. (Facoltativo) Nell'area **Gestisci i tag**, applica una o più name/value coppie di chiavi di tag alla finestra di manutenzione.

I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Ad esempio, è possibile applicare un tag a una finestra di manutenzione per identificare il tipo di attività eseguito, i tipi di destinazioni e l'ambiente in cui viene eseguita. In questo caso, puoi specificare le seguenti name/value coppie di chiavi:

- Key=TaskType, Value=AgentUpdate
- Key=OS, Value=Windows
- Key=Environment, Value=Production

15. Scegli **Crea finestra di manutenzione**. Il sistema reindirizza alla pagina della finestra di manutenzione. Lo stato della finestra di manutenzione appena creata è **Enabled** (Abilitata).

### Assegnazione di destinazioni a una finestra di manutenzione utilizzando la console

In questa procedura si registra una destinazione con una finestra di manutenzione. In altre parole, si specificano le risorse su cui la finestra di manutenzione esegue operazioni.

 Note

Se una singola attività della finestra di manutenzione è registrata con più destinazioni, le relative chiamate di attività vengono eseguite in sequenza e non in parallelo. Se l'attività deve essere eseguita su più destinazioni contemporaneamente, registrare un'attività per ogni destinazione singolarmente e assegnare a ciascuna attività lo stesso livello di priorità.

### Per assegnare destinazioni a una finestra di manutenzione utilizzando la console

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.

2. Nel pannello di navigazione, scegli Maintenance Windows.
3. Nell'elenco delle finestre di manutenzione, scegliere la finestra di manutenzione cui aggiungere le destinazioni.
4. Scegliere Actions (Operazioni) e successivamente Register targets (Registra destinazioni).
5. (Facoltativo) In Target name (Nome destinazione), inserire un nome per le destinazioni.
6. (Facoltativo) In Descrizione, immetti una descrizione.
7. (Facoltativo) Per informazioni sul proprietario, specifica le informazioni da includere in qualsiasi EventBridge evento Amazon generato durante l'esecuzione delle attività per questi obiettivi in questa finestra di manutenzione.

Per informazioni sull'utilizzo per EventBridge monitorare gli eventi di Systems Manager, consulta [Monitoraggio degli eventi di Systems Manager con Amazon EventBridge](#).

8. Nell'area Targets (Destinazioni), scegliere una delle opzioni descritte nella tabella seguente.

| Opzione                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Specifica tag delle istanze | <p>Nei riquadri Specify instance tags (Specifica tag delle istanze), specifica una o più chiavi di tag e valori (opzionali) che sono stati o verranno aggiunti ai nodi gestiti nel tuo account. Quando la finestra di manutenzione viene eseguita, tenta di eseguire attività su tutti i nodi gestiti a cui questi tag sono stati aggiunti.</p> <p>Se si specificano più chiavi di tag, un nodo deve essere contrassegnato con tutte le chiavi tag e i valori specificati per essere inclusi nel gruppo di destinazione.</p> |
| Scegli istanze manualmente  | Dall'elenco, seleziona la casella per ogni nodo che desideri includere nella destinazione della finestra di manutenzione.                                                                                                                                                                                                                                                                                                                                                                                                    |

| Opzione | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | <p>L'elenco include tutti i nodi nel tuo account che sono configurati per l'uso con Systems Manager.</p> <p>Se un nodo Amazon EC2 che ti aspetti di vedere non è presente nell'elenco, consulta <a href="#">Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti</a> per suggerimenti sulla risoluzione dei problemi.</p> <p>Per dispositivi edge e server on-premises e macchine virtuali (VM), consulta <a href="#">Gestione dei nodi in ambienti ibridi e multicloud con Systems Manager</a></p> |

| Opzione                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scelta di un gruppo di risorse | <p>In Resource group (Gruppo di risorse), scegli il nome di un gruppo di risorse esistente nel tuo account dall'elenco.</p> <p>Per informazioni sulla creazione e l'utilizzo di gruppi di risorse, consulta i seguenti argomenti:</p> <ul style="list-style-type: none"><li>• <a href="#">Cosa sono i gruppi di risorse?</a> nella Guida per l'utente di AWS Resource Groups</li><li>• <a href="#">Gruppi di risorse e assegnazione di tag per AWS</a> nel AWS blog Novità</li></ul> <p>(Facoltativo) Per Resource types (Tipi di risorse), selezionare fino a cinque tipi di risorse disponibili o scegliere All resource types (Tutti i tipi di risorse).</p> <p>Se le attività assegnate alla finestra di manutenzione non agiscono su uno dei tipi di risorse aggiunti alla destinazione, il sistema potrebbe segnalare un errore. Attività per le quali viene individuato un tipo di risorsa supportato continuano a essere eseguite nonostante questi errori.</p> <p>Ad esempio, supponiamo di aggiungere i seguenti tipi di risorse a questa destinazione:</p> <ul style="list-style-type: none"><li>• AWS::S3::Bucket</li><li>• AWS::DynamoDB::Table</li><li>• AWS::EC2::Instance</li></ul> <p>Ma in seguito, quando aggiungi attività alla finestra di manutenzione, includi solo</p> |



| Opzione | Description                                                                                                                                                                                                                                                                                                                                                                                                |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | quelle che eseguono operazioni su nodi, ad esempio l'applicazione di baseline delle patch o il riavvio di un nodo. Nel log della finestra di manutenzione, potrebbe essere segnalato un errore di mancata individuazione di bucket Amazon Simple Storage Service (Amazon S3) o tabelle Amazon DynamoDB. Tuttavia, la finestra di manutenzione continua a eseguire attività sui nodi nel gruppo di risorse. |

## 9. Scegli Registra destinazione.

Se desideri assegnare più destinazioni a questa finestra di manutenzione, scegli la scheda Targets (Destinazioni) e quindi seleziona Register target (Registra destinazione). Con questa opzione, è possibile scegliere diverse modalità di indicazione delle destinazioni. Ad esempio, se i nodi di destinazione sono stati in precedenza identificati per ID istanza, è possibile registrare nuove destinazioni e nodi di destinazione specificando i tag applicati a nodi gestiti o scegliendo tipi di risorse da un gruppo di risorse.

Assegnazione di attività a una finestra di manutenzione utilizzando la console

In questa procedura si aggiunge un'attività a una finestra di manutenzione. Le attività sono le operazioni eseguite quando viene eseguita una finestra di manutenzione.

I seguenti quattro tipi di attività possono essere aggiunti a una finestra di manutenzione:

- Comandi AWS Systems Manager Run Command
- Flussi di lavoro di automazione di Systems Manager
- AWS Step Functions attività
- AWS Lambda funzioni

### Important

La policy IAM per Maintenance Windows prevede che il nome (o l'alias) della funzione Lambda sia associato al prefisso SSM. Prima di procedere alla registrazione di questo tipo

di attività, aggiornane il nome inserendo SSM. AWS Lambda Ad esempio, se il nome della funzione Lambda è `MyLambdaFunction`, modifica tale nome in `SSMMyLambdaFunction`.

Per assegnare task a una finestra di manutenzione

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Maintenance Windows.
3. Scegliere una finestra di manutenzione dall'elenco.
4. Scegliere Actions (Operazioni), quindi scegliere l'opzione per il tipo di attività che si desidera registrare con la finestra di manutenzione.
  - Register run command task (Registra attività di esecuzione comandi)
  - Register Automation task (Registra attività di automazione)
  - Register Lambda task (Registra attività Lambda)
  - Register Step Functions task (Registra attività Step Functions)

 Note

Le attività della finestra di manutenzione supportano solo i flussi di lavoro delle macchine a stati standard di Step Functions. Non supportano i flussi di lavoro delle macchine a stati express. Per informazioni sui tipi di flusso di lavoro delle macchine a stati, consulta [Standard vs. Express Workflows](#) (Differenze flussi di lavoro standard ed express) nella Guida per gli sviluppatori di AWS Step Functions .

5. (Facoltativo) In Nome, immetti un nome per l'attività.
6. (Facoltativo) In Descrizione, immetti una descrizione.
7. Per Nuovo cutoff dell'invocazione delle attività, se non si desidera che vengano avviate nuove invocazioni di attività dopo il raggiungimento del tempo limite della finestra di manutenzione, scegliere Abilitato.

Quando questa opzione è non abilitato, l'attività continua a funzionare quando viene raggiunto il tempo limite e avvia nuove invocazioni di attività fino al completamento.

 Note

Lo stato delle attività che non vengono completate quando si abilita questa opzione è `TIMED_OUT`.

8. Per questo passaggio, segui i passaggi secondari relativi al tipo di attività selezionato.

#### Run Command

1. Nell'elenco Command document (Documento di comando) , scegli il documento SSM (documento di comando di Systems Manager) che definisce le attività da eseguire.
2. In Document version (Versione del documento), scegliere la versione del documento da utilizzare.
3. In Task priority (Priorità attività), specificare una priorità per questa attività. Zero (0) indica la priorità più elevata. Le attività di una finestra di manutenzione vengono pianificate in ordine di priorità con le attività che hanno la stessa priorità pianificate in parallelo.

#### Automation

1. Nell'elenco Automation document (Documento di automazione), scegli il runbook Automation che definisce le attività da eseguire.
2. In Document version (Versione del documento), scegliere la versione del runbook da utilizzare.
3. In Task priority (Priorità attività), specificare una priorità per questa attività. Zero (0) indica la priorità più elevata. Le attività di una finestra di manutenzione vengono pianificate in ordine di priorità con le attività che hanno la stessa priorità pianificate in parallelo.

#### Lambda

1. Nell'area Lambda parameters (Parametri Lambda), scegli una funzione Lambda dall'elenco.
2. (Facoltativo) Fornisci un contenuto per l'elemento Payload (Payload), Client Context (Contesto client) oppure Qualifier (Qualificatore) che desideri includere.

 Note

In alcuni casi, è possibile utilizzare uno pseudo parametro come parte del valore Payload. Quando poi viene eseguita, l'operazione della finestra di manutenzione trasmette i valori corretti invece dei segnaposto degli pseudoparametri. Per informazioni, consulta [Utilizzo degli pseudo parametri durante la registrazione delle attività della finestra di manutenzione](#).

3. In Task priority (Priorità attività), specificare una priorità per questa attività. Zero (0) indica la priorità più elevata. Le attività di una finestra di manutenzione vengono pianificate in ordine di priorità con le attività che hanno la stessa priorità pianificate in parallelo.

## Step Functions

1. Nell'area Step Functions parameters (Parametri di Step Functions), scegli una macchina a stati dall'elenco.
2. (Facoltativo) Fornisci un nome per l'esecuzione della macchina a stati e un contenuto per l'elemento Input che desideri includere.

 Note

In alcuni casi, è possibile utilizzare uno pseudo parametro come parte del valore Input. Quando poi viene eseguita, l'operazione della finestra di manutenzione trasmette i valori corretti invece dei segnaposto degli pseudoparametri. Per informazioni, consulta [Utilizzo degli pseudo parametri durante la registrazione delle attività della finestra di manutenzione](#).

3. In Task priority (Priorità attività), specificare una priorità per questa attività. Zero (0) indica la priorità più elevata. Le attività di una finestra di manutenzione vengono pianificate in ordine di priorità con le attività che hanno la stessa priorità pianificate in parallelo.
9. Nell'area Targets (Destinazioni), scegli una delle seguenti opzioni:
    - Selezione di gruppi di destinazione registrati: seleziona una o più destinazioni della finestra di manutenzione registrate con la finestra di manutenzione corrente.
    - Selezione di destinazioni non registrate: scegli le risorse disponibili una per una come destinazioni per l'attività.

Se un nodo Amazon EC2 che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

- Target attività non richiesto: i target per l'attività potrebbero essere già specificati in altre funzioni per tutte le attività di tipo Run Command.

Specifica uno o più target per le attività di tipo Run Command della finestra di manutenzione. A seconda dell'attività, gli obiettivi sono opzionali per altri tipi di attività della finestra di manutenzione (Automazione e AWS Step Functions). AWS Lambda Per ulteriori informazioni sull'esecuzione di attività che non specificano destinazioni, consulta [Registrazione delle attività della finestra di manutenzione senza destinazioni](#).

#### Note

In molti casi, non devi specificare esplicitamente una destinazione per un'attività di automazione. Ad esempio, supponiamo che tu stia creando un' Automation-type attività per aggiornare un Amazon Machine Image (AMI) per Linux usando il AWS-UpdateLinuxAmi runbook. Quando l'attività viene eseguita, AMI viene aggiornato con gli ultimi pacchetti di distribuzione Linux disponibili e il software Amazon. Nuove istanze create da AMI hanno già questi aggiornamenti installati. Perché l'ID dell'AMI da aggiornare è specificato nei parametri di input per il runbook, non è necessario specificare nuovamente una destinazione nel processo della finestra di manutenzione.

#### 10. Solo attività di automazione:

Nell'area Input parameters (Parametri di input), fornisci i valori per tutti i parametri obbligatori o facoltativi necessari per eseguire l'attività.

#### Note

In alcuni casi, è possibile utilizzare uno pseudo parametro per determinati valori dei parametri di input. Quando poi viene eseguita, l'operazione della finestra di manutenzione trasmette i valori corretti invece dei segnaposto degli pseudoparametri. Per informazioni, consulta [Utilizzo degli pseudo parametri durante la registrazione delle attività della finestra di manutenzione](#).

#### 11. In Controllo velocità:

- In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti presi di mira, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.
12. (Facoltativo) Per il Ruolo di servizio IAM, scegli un ruolo affinché Systems Manager conceda le autorizzazioni durante l'esecuzione di attività della finestra di manutenzione.

Se non specifichi un ARN del ruolo di servizio, Systems Manager utilizza un ruolo collegato al servizio nell'account. Questo ruolo non è elencato nel menu a discesa. Se nell'account non esiste un ruolo collegato al servizio appropriato per Systems Manager, questo viene creato quando l'attività viene registrata correttamente.

 Note

Per migliorare il livello di sicurezza, consigliamo vivamente di creare una policy personalizzata e un ruolo di servizio personalizzato per l'esecuzione delle attività della finestra di manutenzione. C'è la possibilità di creare la policy per fornire solo le autorizzazioni necessarie per le specifiche attività della finestra di manutenzione. Per ulteriori informazioni, consulta [Configurazione Intervallo di manutenzione](#).

13. Solo attività Run Command:

(Facoltativo) Per Output options (Opzioni di output) eseguire una delle seguenti operazioni:

- Seleziona la casella di controllo Enable writing to S3 (Abilita scrittura in S3) per salvare l'output del comando in un file. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

- Seleziona la casella CloudWatch di controllo Output per scrivere l'output completo su Amazon CloudWatch Logs. Inserisci il nome di un gruppo di CloudWatch log Logs.

 Note

Le autorizzazioni che garantiscono la possibilità di scrivere dati in un bucket S3 o in CloudWatch Logs sono quelle del profilo di istanza assegnato al nodo, non quelle dell'utente IAM che esegue questa attività. Per ulteriori informazioni, consulta la pagina [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#). Inoltre, se il bucket o il gruppo di log S3 specificato si trova in un altro Account AWS, verifica che il profilo di istanza associato al nodo disponga delle autorizzazioni necessarie per scrivere in quel bucket.

14. Solo attività Run Command:

Se si desidera che vengano inviate notifiche sullo stato dell'esecuzione del comando, nella sezione SNS notifications (Notifiche SNS) selezionare la casella di controllo Enable SNS notifications (Abilita notifiche SNS).

Per ulteriori informazioni, sulla configurazione delle notifiche Amazon SNS per Run Command consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

15. Solo attività Run Command:

Nell'area Parameters (Parametri), specifica i parametri per il documento.

 Note

In alcuni casi, è possibile utilizzare uno pseudo parametro per determinati valori dei parametri di input. Quando poi viene eseguita, l'operazione della finestra di manutenzione trasmette i valori corretti invece dei segnaposto degli pseudoparametri. Per informazioni, consulta [Utilizzo degli pseudo parametri durante la registrazione delle attività della finestra di manutenzione](#).

16. Solo attività Automation e Run Command:

(Facoltativo) Nell'area di CloudWatch allarme, per Nome allarme, scegli un CloudWatch avviso esistente da applicare all'attività per il monitoraggio.

Se l'allarme si attiva, l'attività viene interrotta.

 Note

Per allegare un CloudWatch allarme all'attività, il responsabile IAM che esegue l'operazione deve disporre dell'autorizzazione per `iam:createServiceLinkedRole`. Per ulteriori informazioni sugli CloudWatch allarmi, consulta [Utilizzo degli CloudWatch allarmi Amazon](#).

17. A seconda del tipo di task, scegli una delle seguenti opzioni:

- Register run command task (Registra attività di esecuzione comandi)
- Register Automation task (Registra attività di automazione)
- Register Lambda task (Registra attività Lambda)
- Register Step Functions task (Registra attività Step Functions)

Disabilitare o abilitare una finestra di manutenzione utilizzando la console

È possibile disattivare o abilitare una finestra di manutenzione in Maintenance Windows. È possibile scegliere una finestra di manutenzione alla volta per disabilitare o abilitare l'esecuzione della finestra di manutenzione. È possibile inoltre selezionare più finestre di manutenzione o tutte le finestre di manutenzione da abilitare e disabilitare.

Questa sezione descrive come disabilitare o abilitare una finestra di manutenzione utilizzando la console di Systems Manager. Per esempi di come eseguire questa operazione utilizzando AWS Command Line Interface (AWS CLI), vedete [Tutorial: Aggiornare una finestra di manutenzione utilizzando il AWS CLI](#).

## Argomenti

- [Disabilitare una finestra di manutenzione utilizzando la console](#)
- [Abilitare una finestra di manutenzione utilizzando la console](#)

Disabilitare una finestra di manutenzione utilizzando la console

È possibile disabilitare una finestra di manutenzione per sospendere un'attività per un periodo specificato e tale finestra rimarrà disponibile per essere riattivata in seguito.



## Disabilitare una finestra di manutenzione

1. Aprire la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Maintenance Windows.
3. Utilizzando la casella di controllo accanto alla finestra di manutenzione che desideri disabilitare, seleziona una o più finestre di manutenzione.
4. Scegli Disabilita finestra di manutenzione nel menu Operazioni. Il sistema richiede di confermare le operazioni.

## Abilitare una finestra di manutenzione utilizzando la console

È possibile abilitare una finestra di manutenzione per riprendere un'attività.

### Note

Se la finestra di manutenzione utilizza una pianificazione tariffaria e la data di inizio è attualmente impostata su una data e un'ora precedenti, la data e l'ora correnti vengono utilizzate come data di inizio della finestra di manutenzione. È possibile modificare la data di inizio della finestra di manutenzione prima o dopo averla abilitata. Per informazioni, consulta [Aggiorna o elimina le risorse della finestra di manutenzione utilizzando la console](#).

## Per abilitare una finestra di manutenzione

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Maintenance Windows.
3. Seleziona la casella di controllo accanto alla finestra di manutenzione per abilitarla.
4. Scegli Operazioni, Abilita finestra di manutenzione. Il sistema richiede di confermare le operazioni.

## Aggiorna o elimina le risorse della finestra di manutenzione utilizzando la console

È possibile aggiornare o eliminare una finestra di manutenzione in Maintenance Windows. È inoltre possibile aggiornare o eliminare le destinazioni o le attività di una finestra di manutenzione. Se si

modificano i dettagli di una finestra di manutenzione, è possibile modificarne la pianificazione, le destinazioni e le attività. È inoltre possibile specificare nomi e descrizioni per finestre, destinazioni e attività, per permettere di comprendere meglio il loro scopo e rendere più semplice la gestione della coda delle finestre.

Questa sezione descrive come aggiornare o eliminare una finestra di manutenzione, destinazioni e attività utilizzando la console di Systems Manager. Per esempi su come eseguire questa operazione utilizzando l' AWS Command Line Interface (AWS CLI), consulta [Tutorial: Aggiornare una finestra di manutenzione utilizzando il AWS CLI](#).

## Argomenti

- [Aggiornamento o eliminazione di una finestra di manutenzione utilizzando la console](#)
- [Aggiornamento o annullamento della registrazione delle destinazioni della finestra di manutenzione utilizzando la console](#)
- [Aggiornamento o annullamento della registrazione delle attività di una finestra di manutenzione utilizzando la console](#)

## Aggiornamento o eliminazione di una finestra di manutenzione utilizzando la console

È possibile aggiornare una finestra di manutenzione in modo da modificarne il nome, la descrizione e la pianificazione, nonché la possibilità di consentire le destinazioni non registrate.

Per aggiornare o eliminare una finestra di manutenzione

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Maintenance Windows.
3. Selezionare il pulsante accanto alla finestra di manutenzione che si desidera aggiornare o eliminare ed eseguire una delle operazioni seguenti:
  - Scegli Elimina. Il sistema richiede di confermare le operazioni.
  - Scegli Modifica. Nella pagina Modifica finestra di manutenzione, modifica i valori e le opzioni desiderate, quindi scegli Salva modifiche.

Per informazioni sulle scelte di configurazione disponibili, consulta [Creare una finestra di manutenzione utilizzando la console](#).

## Aggiornamento o annullamento della registrazione delle destinazioni della finestra di manutenzione utilizzando la console

È possibile aggiornare o annullare la registrazione delle destinazioni di una finestra di manutenzione. Se si sceglie di aggiornare una destinazione di una finestra di manutenzione, è possibile specificare nuovo nome, descrizione e proprietario della destinazione. È anche possibile scegliere diverse destinazioni.

Per aggiornare o eliminare le destinazioni di una finestra di manutenzione

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Maintenance Windows.
3. Scegliere il nome della finestra di manutenzione che si desidera aggiornare, scegliere la scheda Destinazioni, quindi eseguire una delle operazioni seguenti:
  - Per aggiornare le destinazioni, seleziona il pulsante accanto alla destinazione da aggiornare, quindi scegli Modifica.
  - Per annullare la registrazione delle destinazioni, selezionare il pulsante accanto alla destinazione di cui annullare la registrazione, quindi scegliere Annulla la registrazione della destinazione. Nella finestra di dialogo Annulla registrazione della destinazione delle finestre di manutenzione scegli Annulla registrazione.

## Aggiornamento o annullamento della registrazione delle attività di una finestra di manutenzione utilizzando la console

È possibile aggiornare o annullare la registrazione delle attività di una finestra di manutenzione. Se si sceglie l'aggiornamento, è possibile specificare nuovo nome, descrizione e proprietario dell'attività. Per le attività Run Command e di automazione, è possibile scegliere un documento SSM diverso per le attività. Non è possibile, tuttavia, modificare un'attività per modificarne il tipo. Ad esempio, se si crea un'attività di automazione, non è possibile modificare tale attività e modificarla in un'attività Run Command.

Per aggiornare o eliminare le attività di una finestra di manutenzione utilizzando la console

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Maintenance Windows.

3. Scegliere il nome della finestra di manutenzione che si desidera aggiornare.
4. Scegli la scheda Attività, quindi seleziona il pulsante accanto all'attività da aggiornare.
5. Esegui una delle seguenti operazioni:
  - Per annullare la registrazione di un'attività, scegli Annullamento registrazione attività.
  - Per modificare l'attività, scegliere Modifica. Modificare i valori e le opzioni desiderate, quindi scegliere Modifica attività.

## Esercitazioni

I tutorial mostrano come eseguire le attività comuni quando si utilizzano le finestre di manutenzione.

### Completamento dei prerequisiti

Prima di eseguire questi tutorial, completare le attività seguenti.

- Configuralo AWS CLI sul tuo computer locale: prima di poter eseguire AWS CLI i comandi, devi installare e configurare la CLI sul tuo computer locale. Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).
- Verifica i ruoli e le autorizzazioni delle finestre di manutenzione: un AWS amministratore del tuo account deve concederti le autorizzazioni AWS Identity and Access Management (IAM) necessarie per gestire le finestre di manutenzione utilizzando la CLI. Per informazioni, consulta [Configurazione Intervallo di manutenzione](#).
- Creazione o configurazione di un'istanza compatibile con Systems Manager: per poter completare i tutorial, è necessario disporre di almeno un'istanza Amazon Elastic Compute Cloud (Amazon EC2) configurata per l'uso con Systems Manager. Ciò significa che SSM Agent è installato sull'istanza e un profilo dell'istanza IAM per Systems Manager è collegato all'istanza.

Ti consigliamo di avviare un'istanza da un'istanza AWS managed Amazon Machine Image (AMI) con l'agente preinstallato. Per ulteriori informazioni, consulta [Trova AMI con il Agente SSM preinstallato](#).

Per informazioni su come installare SSM Agent su un'istanza, consulta i seguenti argomenti:

- [Installazione e disinstallazione manuali Agente SSM su istanze EC2 per Windows Server](#)
- [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#)

Per informazioni su come configurare le autorizzazioni IAM per Systems Manager per l'istanza in uso, consulta la pagina [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#).

- Crea risorse aggiuntive in base alle necessità: Run Command include molte attività che non richiedono la creazione di risorse diverse da quelle elencate in questo argomento sui prerequisiti. Per questo motivo, forniamo un'attività Run Command semplice che puoi utilizzare la prima volta che esegui i tutorial. È inoltre necessario disporre di un'istanza EC2 configurata per l'uso con Systems Manager, come descritto in precedenza in questo argomento. Dopo aver configurato l'istanza, potrai registrare un'attività Run Command semplice.

Lo strumento Maintenance Windows di Systems Manager supporta l'esecuzione dei quattro tipi di attività seguenti:

- Comandi Run Command
- Flussi di lavoro di automazione di Systems Manager
- AWS Lambda funzioni
- AWS Step Functions compiti

In linea generale, se un task della finestra di manutenzione che si desidera eseguire richiede risorse aggiuntive, è necessario crearle prima. Ad esempio, se desideri una finestra di manutenzione che esegua una AWS Lambda funzione, crea la funzione Lambda prima di iniziare; per un'Run Commandattività, crea il bucket S3 in cui puoi salvare l'output dei comandi (se prevedi di farlo) e così via.

## Esercitazioni

- [Tutorial: creazione e gestione delle finestre di manutenzione utilizzando AWS CLI](#)
- [Tutorial: creazione di una finestra di manutenzione per l'applicazione di patch tramite console](#)

## Tutorial: creazione e gestione delle finestre di manutenzione utilizzando AWS CLI

Questa sezione include tutorial, che consentono di imparare a utilizzare la AWS Command Line Interface (AWS CLI) per eseguire le operazioni seguenti:

- Creazione e configurazione di una finestra di manutenzione
- Visualizzazione delle informazioni sulle finestre di manutenzione

- Visualizzazione delle informazioni sui task relativi alle finestre di manutenzione e sulla loro esecuzione
- Aggiornamento di una finestra di manutenzione
- Eliminazione di una finestra di manutenzione

## Traccia degli ID risorsa

Man mano che completi le attività di questi AWS CLI tutorial, tieni traccia degli ID delle risorse generati dai comandi che esegui. Puoi utilizzare molti di questi ID come input per i comandi successivi. Ad esempio, quando crei la finestra di manutenzione, il sistema fornisce il relativo ID nel seguente formato.

```
{
 "WindowId": "mw-0c50858d01EXAMPLE"
}
```

Annota i seguenti ID generati dal sistema perché saranno utilizzati dal tutorial descritto in questa sezione:

- WindowId
- WindowTargetId
- WindowTaskId
- WindowExecutionId
- TaskExecutionId
- InvocationId
- ExecutionId

Inoltre, devi disporre dell'ID dell'istanza EC2 che prevedi di utilizzare nei tutorial. Ad esempio: `i-02573cafcfEXAMPLE`

## Esercitazioni

- [Tutorial: Creare e configurare una finestra di manutenzione utilizzando il AWS CLI](#)
- [Tutorial: Visualizza le informazioni sulle finestre di manutenzione utilizzando il AWS CLI](#)
- [Tutorial: Visualizza informazioni sulle attività e sulle esecuzioni delle attività utilizzando il AWS CLI](#)
- [Tutorial: Aggiornare una finestra di manutenzione utilizzando il AWS CLI](#)

- [Tutorial: Eliminare una finestra di manutenzione utilizzando il AWS CLI](#)

## Tutorial: Creare e configurare una finestra di manutenzione utilizzando il AWS CLI

Questo tutorial illustra come utilizzare il AWS Command Line Interface (AWS CLI) per creare e configurare una finestra di manutenzione, i relativi obiettivi e le relative attività. L'esecuzione del tutorial si articola in semplici passi. È infatti possibile creare una singola finestra di manutenzione, identificare una singola destinazione e impostare l'esecuzione di un'operazione semplice da parte della finestra di manutenzione. Durante l'intera procedura verranno visualizzate altre informazioni che potrai usare per ottenere scenari più complessi.

Mentre segui i passaggi di questo tutorial, sostituisci i valori nel *red* testo in corsivo con le tue opzioni e i tuoi ID. Ad esempio, sostituisci l'ID della finestra di manutenzione *mw-0c50858d01EXAMPLE* e l'ID dell'istanza *i-02573cafcfEXAMPLE* con gli ID delle risorse che crei.

### Indice

- [Fase 1: Creare la finestra di manutenzione utilizzando AWS CLI](#)
- [Fase 2: Registrare un nodo di destinazione nella finestra di manutenzione utilizzando AWS CLI](#)
- [Fase 3: Registrare un'attività nella finestra di manutenzione utilizzando AWS CLI](#)

## Fase 1: Creare la finestra di manutenzione utilizzando AWS CLI

In questa fase è possibile creare una finestra di manutenzione e specificarne le opzioni di base, come il nome, la pianificazione e la durata. Nelle fasi successive verrà scelta l'istanza da aggiornare e il task da eseguire.

In questo esempio, è necessario creare una finestra di manutenzione che viene eseguita ogni cinque minuti. Di solito, non è possibile eseguire una finestra di manutenzione con questa frequenza. Tuttavia, con questa frequenza è possibile velocizzare la visualizzazione dei risultati del tutorial. Al termine dell'esecuzione di quest'attività verrà illustrato come impostare una frequenza di aggiornamento più bassa.

### Note

Per una spiegazione di come le diverse opzioni relative alla pianificazione per le finestre di manutenzione siano tra loro correlate, consulta [Opzioni di pianificazione e periodo attivo per la finestra di manutenzione](#).

Per ulteriori informazioni sull'utilizzo dell'opzione `--schedule`, consulta [Riferimento: espressioni Cron e della frequenza per Systems Manager](#).

Per creare una finestra di manutenzione utilizzando il AWS CLI

1. Apri AWS Command Line Interface (AWS CLI) ed esegui il seguente comando sul tuo computer locale per creare una finestra di manutenzione che esegua le seguenti operazioni:
  - Avvia l'esecuzione ogni cinque minuti per un massimo di due ore (in base alle esigenze).
  - Impedisce l'avvio di nuovi task nell'ora successiva alla fine dell'operazione della finestra di manutenzione.
  - Consente il supporto di destinazioni non associate (istanze non registrate con la finestra di manutenzione).
  - Mediante l'uso di tag personalizzati indica che l'autore intende utilizzare la finestra di manutenzione in un tutorial.

## Linux & macOS

```
aws ssm create-maintenance-window \
 --name "My-First-Maintenance-Window" \
 --schedule "rate(5 minutes)" \
 --duration 2 \
 --cutoff 1 \
 --allow-unassociated-targets \
 --tags "Key=Purpose,Value=Tutorial"
```

## Windows

```
aws ssm create-maintenance-window ^
 --name "My-First-Maintenance-Window" ^
 --schedule "rate(5 minutes)" ^
 --duration 2 ^
 --cutoff 1 ^
 --allow-unassociated-targets ^
 --tags "Key"="Purpose","Value"="Tutorial"
```

Questo sistema restituisce informazioni simili alle seguenti.



```
{
 "WindowId": "mw-0c50858d01EXAMPLE"
}
```

2. Eseguire il seguente comando per visualizzare ulteriori informazioni su questa e altre finestre di manutenzione già presenti nell'account.

```
aws ssm describe-maintenance-windows
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowIdentities": [
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "My-First-Maintenance-Window",
 "Enabled": true,
 "Duration": 2,
 "Cutoff": 1,
 "NextExecutionTime": "2019-05-11T16:46:16.991Z"
 }
]
}
```

Continua su [Fase 2: Registrare un nodo di destinazione nella finestra di manutenzione utilizzando AWS CLI](#).

Fase 2: Registrare un nodo di destinazione nella finestra di manutenzione utilizzando AWS CLI

In questa fase viene registrata una destinazione con la nuova finestra di manutenzione. In questo caso, specifica quale nodo aggiornare durante l'esecuzione della finestra di manutenzione.

Per un esempio di registrazione di più nodi alla volta utilizzando gli ID nodo, esempi di utilizzo di tag per identificare più nodi ed esempi di specifica di gruppi di risorse come destinazioni, consulta [Esempi: registrazione delle destinazioni con una finestra di manutenzione](#).

 Note

Per eseguire questa fase, è necessario aver già creato un'istanza Amazon Elastic Compute Cloud (Amazon EC2), come descritto nei [prerequisiti per il tutorial relativo alle Maintenance Windows](#).

Per registrare un nodo di destinazione con una finestra di manutenzione utilizzando il AWS CLI

1. Esegui il comando seguente sul computer locale. Sostituisci ogni *example resource placeholder* con le tue informazioni.

## Linux &amp; macOS

```
aws ssm register-target-with-maintenance-window \
 --window-id "mw-0c50858d01EXAMPLE" \
 --resource-type "INSTANCE" \
 --target "Key=InstanceIds,Values=i-02573cafcfEXAMPLE"
```

## Windows

```
aws ssm register-target-with-maintenance-window ^
 --window-id "mw-0c50858d01EXAMPLE" ^
 --resource-type "INSTANCE" ^
 --target "Key=InstanceIds,Values=i-02573cafcfEXAMPLE"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowTargetId": "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
}
```

2. Esegui ora questo comando sul computer locale per visualizzare i dettagli sulla destinazione della finestra di manutenzione.

## Linux &amp; macOS

```
aws ssm describe-maintenance-window-targets \
 --window-id "mw-0c50858d01EXAMPLE"
```

## Windows

```
aws ssm describe-maintenance-window-targets ^
 --window-id "mw-0c50858d01EXAMPLE"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "Targets": [
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowTargetId": "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE",
 "ResourceType": "INSTANCE",
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
 "i-02573cafcfEXAMPLE"
]
 }
]
 }
]
}
```

Continua su [Fase 3: Registrare un'attività nella finestra di manutenzione utilizzando AWS CLI](#).

Esempi: registrazione delle destinazioni con una finestra di manutenzione

Puoi registrare un singolo nodo come destinazione utilizzandone l'ID nodo, come mostrato in [Fase 2: Registrare un nodo di destinazione nella finestra di manutenzione utilizzando AWS CLI](#). Puoi anche registrare uno o più nodi come destinazioni utilizzando i formati di comando forniti in questa pagina.

In generale, sono disponibili due metodi per identificare i nodi da utilizzare come destinazioni della finestra di manutenzione: specificare li singoli nodi e utilizzare i tag delle risorse. Il metodo dei tag delle risorse fornisce più opzioni, come mostrato negli esempi 2-3.

Puoi anche specificare uno o più gruppi di risorse come la destinazione di una finestra di manutenzione. Un gruppo di risorse può includere nodi e molti altri tipi di AWS risorse supportate. Gli

esempi 4 e 5, di seguito, mostrano come aggiungere gruppi di risorse alle destinazioni della finestra di manutenzione.

#### Note

Se una singola attività della finestra di manutenzione è registrata con più destinazioni, le relative chiamate di attività vengono eseguite in sequenza e non in parallelo. Se l'attività deve essere eseguita su più destinazioni contemporaneamente, registrare un'attività per ogni destinazione singolarmente e assegnare a ciascuna attività lo stesso livello di priorità.

Per ulteriori informazioni sulla creazione e la gestione di gruppi di risorse, consulta [Cosa sono i gruppi di risorse?](#) nella AWS Resource Groups Guida per l'utente e [Gruppi di risorse e Assegnazione di tag per AWS](#) nel AWS News Blog.

Per informazioni sulle quote per Maintenance Windows, oltre a quelle specificate negli esempi seguenti, vedere le quote di servizio di [Systems Manager](#) nella. Riferimenti generali di Amazon Web Services

#### Esempio 1: registrazione di più destinazioni con gli ID nodo

Esegui il comando seguente sul computer per registrare più nodi come destinazioni utilizzando i relativi ID nodo. Sostituisci ogni *example resource placeholder* con le tue informazioni.

#### Linux & macOS

```
aws ssm register-target-with-maintenance-window \
 --window-id "mw-0c50858d01EXAMPLE" \
 --resource-type "INSTANCE" \
 --target
 "Key=InstanceIds,Values=i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE,i-07782c72faEXAMPLE"
```

#### Windows

```
aws ssm register-target-with-maintenance-window ^
 --window-id "mw-0c50858d01EXAMPLE" ^
 --resource-type "INSTANCE" ^
 --target
 "Key=InstanceIds,Values=i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE,i-07782c72faEXAMPLE"
```

Utilizzo consigliato: questa opzione è particolarmente utile quando si registra per la prima volta un gruppo unico di nodi con una qualsiasi finestra di manutenzione e quando questi nodi non condividono un tag di nodo comune.

Quote: è possibile specificare fino a un massimo di 50 nodi totali per ogni destinazione della finestra di manutenzione.

Esempio 2: registrazione delle destinazioni con i tag delle risorse applicati ai nodi

Esegui il comando seguente sul computer locale per registrare tutti i nodi già contrassegnate con una coppia chiave-valore che hai assegnato. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux & macOS

```
aws ssm register-target-with-maintenance-window \
 --window-id "mw-0c50858d01EXAMPLE" \
 --resource-type "INSTANCE" \
 --target "Key=tag:Region,Values=East"
```

Windows

```
aws ssm register-target-with-maintenance-window ^
 --window-id "mw-0c50858d01EXAMPLE" ^
 --resource-type "INSTANCE" ^
 --target "Key=tag:Region,Values=East"
```

Utilizzo consigliato: questa opzione è particolarmente utile quando si registra per la prima volta un gruppo unico di nodi con una qualsiasi finestra di manutenzione e quando questi nodi non condividono un tag di nodo comune.

Quote: è possibile specificare fino a cinque coppie chiave-valore in totale per ogni destinazione. Se si specificano più coppie chiave-valore, un nodo deve essere contrassegnato con tutte le chiavi tag e i valori specificati per essere inclusi nel gruppo di destinazione.

#### Note

È possibile applicare tag a un gruppo di nodi con la chiave di tag Patch Group o PatchGroup e assegnare ai nodi un valore di chiave comune, ad esempio my-patch-

group. (È necessario utilizzare PatchGroup, senza spazio, se sono presenti [tag consentiti nei metadati dell'istanza EC2](#).) Patch Manager, uno strumento di Systems Manager, valuta la chiave Patch Group o PatchGroup sui nodi per determinare quale baseline delle patch vi si può applicare. Se l'attività eseguirà il documento SSM AWS-RunPatchBaseline o il documento legacy SSM AWS-ApplyPatchBaseline, è possibile specificare la stessa coppia chiave-valore Patch Group o PatchGroup quando si registrano destinazioni con una finestra di manutenzione. Ad esempio: `--target "Key=tag:PatchGroup,Values=my-patch-group`. In questo modo è possibile utilizzare una finestra di manutenzione per aggiornare le patch su un gruppo di nodi già associati alla stessa baseline delle patch. Per ulteriori informazioni, consulta [Gruppi di patch](#).

Esempio 3: registrazione delle destinazioni con un gruppo di chiavi dei tag (senza valori di tag)

Esegui il comando seguente sul computer locale per registrare tutti i nodi che hanno una o più chiavi dei tag assegnate, indipendentemente dai valori delle chiavi. Sostituisci ogni *example resource placeholder* con le tue informazioni.

## Linux & macOS

```
aws ssm register-target-with-maintenance-window \
 --window-id "mw-0c50858d01EXAMPLE" \
 --resource-type "INSTANCE" \
 --target "Key=tag-key,Values=Name,Instance-Type,CostCenter"
```

## Windows

```
aws ssm register-target-with-maintenance-window ^
 --window-id "mw-0c50858d01EXAMPLE" ^
 --resource-type "INSTANCE" ^
 --target "Key=tag-key,Values=Name,Instance-Type,CostCenter"
```

Utilizzo consigliato: utile quando si desidera definire i nodi come destinazioni specificando più chiavi dei tag (senza i relativi valori) invece di una sola coppia tag-chiave o coppia di tag chiave-valore.

Quote: è possibile specificare fino a cinque coppie tag-chiave in totale per ogni destinazione. Se si specificano più chiavi di tag, un nodo deve essere contrassegnato con tutte le chiavi tag specificate per essere incluse nel gruppo di destinazione.

## Esempio 4: registrazione di destinazioni utilizzando un nome del gruppo di risorse

Esegui il comando seguente sul computer locale per registrare un gruppo di risorse specificato, a prescindere dal tipo di risorse che contiene. `mw-0c50858d01EXAMPLE` Sostituiscilo con le tue informazioni. Se le attività assegnate alla finestra di manutenzione non agiscano su un tipo di risorsa incluso in questo gruppo di risorse, il sistema potrebbe segnalare un errore. Attività per le quali viene individuato un tipo di risorsa supportato continuano a essere eseguite nonostante questi errori.

### Linux & macOS

```
aws ssm register-target-with-maintenance-window \
 --window-id "mw-0c50858d01EXAMPLE" \
 --resource-type "RESOURCE_GROUP" \
 --target "Key=resource-groups:Name,Values=MyResourceGroup"
```

### Windows

```
aws ssm register-target-with-maintenance-window ^
 --window-id "mw-0c50858d01EXAMPLE" ^
 --resource-type "RESOURCE_GROUP" ^
 --target "Key=resource-groups:Name,Values=MyResourceGroup"
```

Uso consigliato: utile quando desideri specificare rapidamente un gruppo di risorse come una destinazione senza valutare se tutti i tipi di risorse saranno selezionati per una finestra di manutenzione, oppure quando sai che il gruppo di risorse contiene solo i tipi di risorse su cui le attività eseguono operazioni.

Quote: è possibile specificare un solo gruppo di risorse come una destinazione.

## Esempio 5: registrazione di destinazioni filtrando tipi di risorse in un gruppo di risorse

Esegui il comando seguente sul computer locale per registrare solo determinati tipi di risorse che appartengono a un gruppo di risorse specificato. Sostituisci `mw-0c50858d01EXAMPLE` con le tue informazioni. Con questa opzione, anche se aggiungi un'attività per un tipo di risorsa che appartiene al gruppo di risorse, l'attività non verrà eseguita se non hai aggiunto esplicitamente il tipo di risorsa al filtro.

### Linux & macOS

```
aws ssm register-target-with-maintenance-window \
```

```
--window-id "mw-0c50858d01EXAMPLE" \
--resource-type "RESOURCE_GROUP" \
--target "Key=resource-groups:Name,Values=MyResourceGroup" \
"Key=resource-
groups:ResourceTypeFilters,Values=AWS::EC2::Instance,AWS::ECS::Cluster"
```

## Windows

```
aws ssm register-target-with-maintenance-window ^
--window-id "mw-0c50858d01EXAMPLE" ^
--resource-type "RESOURCE_GROUP" ^
--target "Key=resource-groups:Name,Values=MyResourceGroup" ^
"Key=resource-
groups:ResourceTypeFilters,Values=AWS::EC2::Instance,AWS::ECS::Cluster"
```

Uso consigliato: utile quando si desidera mantenere un controllo rigoroso sui tipi di AWS risorse su cui la finestra di manutenzione può eseguire azioni o quando il gruppo di risorse contiene un numero elevato di tipi di risorse e si desidera evitare segnalazioni di errori non necessarie nei registri della finestra di manutenzione.

Quote: è possibile specificare un solo gruppo di risorse come una destinazione.

### Fase 3: Registrare un'attività nella finestra di manutenzione utilizzando AWS CLI

In questa fase del tutorial, registri un' AWS Systems Manager Run Commandattività che esegue il df comando sulla tua istanza Amazon Elastic Compute Cloud (Amazon EC2) per Linux. I risultati di questo comando Linux standard mostrano la quantità di spazio libero disponibile e la quantità di spazio utilizzato sul file system del disco dell'istanza.

oppure

Se utilizzi un'istanza Amazon EC2 per Windows Server anziché una di Linux, nel comando seguente devi sostituire df con ipconfig. Nell'output di questo comando sono elencati i dettagli relativi all'indirizzo IP, alla maschera di sottorete e al gateway predefinito per i convertitori sull'istanza di destinazione.

Quando sei pronto a registrare altri tipi di task oppure a utilizzare un maggior numero di opzioni Run Command di Systems Manager disponibili, consulta [Esempi: registrazione delle operazioni con una finestra di manutenzione](#). In questo argomento sono disponibili ulteriori informazioni su tutti e quattro



i tipi di task e su alcune delle opzioni più importanti in modo da consentirti di creare scenari reali più complessi.

Per registrare un task con una finestra di manutenzione

1. Esegui il comando seguente sul computer locale. Sostituisci ogni *example resource placeholder* con le tue informazioni. La versione da eseguire da un computer Windows locale include i caratteri di escape ("/") necessari per eseguire il comando dallo strumento a riga di comando.

## Linux & macOS

```
aws ssm register-task-with-maintenance-window \
 --window-id mw-0c50858d01EXAMPLE \
 --task-arn "AWS-RunShellScript" \
 --max-concurrency 1 --max-errors 1 \
 --priority 10 \
 --targets "Key=InstanceIds,Values=i-0471e04240EXAMPLE" \
 --task-type "RUN_COMMAND" \
 --task-invocation-parameters '{"RunCommand":{"Parameters":{"commands":
["df"]}}}'
```

## Windows

```
aws ssm register-task-with-maintenance-window ^
 --window-id mw-0c50858d01EXAMPLE ^
 --task-arn "AWS-RunShellScript" ^
 --max-concurrency 1 --max-errors 1 ^
 --priority 10 ^
 --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE" ^
 --task-type "RUN_COMMAND" ^
 --task-invocation-parameters={"RunCommand":{"Parameters":{"commands\":
["df\""]}}}
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE"
}
```

2. Eseguire il comando seguente per visualizzare i dettagli relativi alla finestra di manutenzione creata.

### Linux & macOS

```
aws ssm describe-maintenance-window-tasks \
 --window-id mw-0c50858d01EXAMPLE
```

### Windows

```
aws ssm describe-maintenance-window-tasks ^
 --window-id mw-0c50858d01EXAMPLE
```

3. Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "Tasks": [
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
 "TaskArn": "AWS-RunShellScript",
 "Type": "RUN_COMMAND",
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
 "i-02573cafcfEXAMPLE"
]
 }
],
 "TaskParameters": {},
 "Priority": 10,
 "ServiceRoleArn": "arn:aws:iam::123456789012:role/
MyMaintenanceWindowServiceRole",
 "MaxConcurrency": "1",
 "MaxErrors": "1"
 }
]
}
```

4. Attendere il completamento dell'esecuzione del task, in base alla pianificazione specificata nella [Fase 1: Creare la finestra di manutenzione utilizzando AWS CLI](#). Ad esempio, se è stato

specificato **--schedule "rate(5 minutes)"**, attendere cinque minuti. Eseguire quindi il comando seguente per visualizzare le informazioni sulle esecuzioni completate per questo task.

## Linux & macOS

```
aws ssm describe-maintenance-window-executions \
 --window-id mw-0c50858d01EXAMPLE
```

## Windows

```
aws ssm describe-maintenance-window-executions ^
 --window-id mw-0c50858d01EXAMPLE
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowExecutions": [
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowExecutionId": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
 "Status": "SUCCESS",
 "StartTime": 1557593493.096,
 "EndTime": 1557593498.611
 }
]
}
```

### Tip

Dopo aver eseguito l'attività, è possibile ridurre la frequenza con cui viene eseguita la finestra di manutenzione. Ad esempio, eseguire il comando seguente per ridurre la frequenza a una volta alla settimana. *mw-0c50858d01EXAMPLE* Sostituiscila con le tue informazioni.

## Linux & macOS

```
aws ssm update-maintenance-window \
 --window-id mw-0c50858d01EXAMPLE \
 --schedule "rate(7 days)"
```

## Windows

```
aws ssm update-maintenance-window ^
 --window-id mw-0c50858d01EXAMPLE ^
 --schedule "rate(7 days)"
```

Per informazioni sulla gestione delle pianificazioni delle finestre di manutenzione, consulta [Riferimento: espressioni Cron e della frequenza per Systems Manager](#) e [Opzioni di pianificazione e periodo attivo per la finestra di manutenzione](#).

Per informazioni sull'uso di AWS Command Line Interface (AWS CLI) per modificare una finestra di manutenzione, vedere [Tutorial: Aggiornare una finestra di manutenzione utilizzando il AWS CLI](#).

Per esercitarsi nell'esecuzione dei AWS CLI comandi per visualizzare maggiori dettagli sull'attività della finestra di manutenzione e sulle relative esecuzioni, continua a [Tutorial: Visualizza informazioni sulle attività e sulle esecuzioni delle attività utilizzando il AWS CLI](#).

### Accesso all'output dei comandi del tutorial

Non rientra nello scopo di questo tutorial utilizzare il AWS CLI per visualizzare l'output del Run Command comando associato alle esecuzioni delle attività della finestra di manutenzione.

È possibile visualizzare questi dati utilizzando AWS CLI. Puoi anche visualizzare l'output nella console di Systems Manager o in un file di registro archiviato in un bucket Amazon Simple Storage Service (Amazon S3), se hai configurato la finestra di manutenzione per archiviare l'output in tale contenitore. L'output del `df` comando su un'istanza EC2 per Linux è simile al seguente.

```
Filesystem 1K-blocks Used Available Use% Mounted on

devtmpfs 485716 0 485716 0% /dev

tmpfs 503624 0 503624 0% /dev/shm

tmpfs 503624 328 503296 1% /run

tmpfs 503624 0 503624 0% /sys/fs/cgroup

/dev/xvda1 8376300 1464160 6912140 18% /
```

L'output del comando `ipconfig` in un'istanza EC2 per Windows Server è simile a quello riportato di seguito:

#### Windows IP Configuration

##### Ethernet adapter Ethernet 2:

```
Connection-specific DNS Suffix . : example.com
IPv4 Address. : 10.24.34.0/23
Subnet Mask : 255.255.255.255
Default Gateway : 0.0.0.0
```

##### Ethernet adapter Ethernet:

```
Media State : Media disconnected
Connection-specific DNS Suffix . : abc1.wa.example.net
```

##### Wireless LAN adapter Local Area Connection\* 1:

```
Media State : Media disconnected
Connection-specific DNS Suffix . :
```

##### Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . :
Link-local IPv6 Address : fe80::100b:c234:66d6:d24f%4
IPv4 Address. : 192.0.2.0
Subnet Mask : 255.255.255.0
Default Gateway : 192.0.2.0
```

##### Ethernet adapter Bluetooth Network Connection:

```
Media State : Media disconnected
Connection-specific DNS Suffix . :
```

Esempi: registrazione delle operazioni con una finestra di manutenzione

È possibile registrare un'attività inRun Command, con una finestra di manutenzione, utilizzando il pulsante AWS Command Line Interface (AWS CLI), come illustrato in [Registra attività con la finestra di manutenzione](#). È inoltre possibile registrare le attività per i flussi di lavoro, AWS Lambda le funzioni

e le AWS Step Functions attività di Systems Manager Automation, come illustrato più avanti in questo argomento.

#### Note

Specifica uno o più target per le attività di tipo Run Command della finestra di manutenzione. A seconda dell'attività, gli obiettivi sono opzionali per altri tipi di attività della finestra di manutenzione (Automazione e AWS Step Functions). AWS Lambda Per ulteriori informazioni sull'esecuzione di attività che non specificano destinazioni, consulta [Registrazione delle attività della finestra di manutenzione senza destinazioni](#).

In questo argomento, forniamo esempi di utilizzo del comando AWS Command Line Interface (AWS CLI) `register-task-with-maintenance-window` per registrare ciascuno dei quattro tipi di attività supportati con una finestra di manutenzione. Gli esempi sono solo a titolo dimostrativo, ma è possibile modificarli per creare comandi di registrazione di task funzionanti.

#### Utilizzo dell'opzione `--cli-input-json`

Per ottimizzare la gestione delle opzioni relative ai task, è possibile utilizzare l'opzione di comando `--cli-input-json`, con i valori delle opzioni inclusi in un file JSON.

Per utilizzare il contenuto del file JSON di esempio disponibile negli esempi, eseguire la procedura seguente nel computer locale:

1. Creare un file assegnandogli, ad esempio, il nome `MyRunCommandTask.json`, `MyAutomationTask.json` oppure il nome desiderato.
2. Copiare il contenuto dell'esempio JSON nel file.
3. Modificare il contenuto del file per la registrazione del task, quindi salvare il file.
4. Nella stessa directory in cui è stato salvato il file, eseguire il comando seguente. Sostituisci il nome del file con. *MyFile.json*

#### Linux & macOS

```
aws ssm register-task-with-maintenance-window \
--cli-input-json file://MyFile.json
```

## Windows

```
aws ssm register-task-with-maintenance-window ^
 --cli-input-json file://MyFile.json
```

### Pseudo parametri nelle attività della finestra di manutenzione

In alcuni esempi vengono utilizzati gli pseudoparametri come metodo per passare le informazioni sugli ID ai task. Ad esempio, `{{TARGET_ID}}` e `{{RESOURCE_ID}}` sono utilizzabili per passare gli ID delle risorse AWS alle operazioni di Automazione, Lambda e Step Functions. Per ulteriori informazioni sugli pseudoparametri nel parametro `--task-invocation-parameters`, consulta [Utilizzo degli pseudo parametri durante la registrazione delle attività della finestra di manutenzione](#).

### Ulteriori informazioni

- [Opzioni dei parametri per il comando register-task-with-maintenance-windows](#).
- [register-task-with-maintenance-window](#) in Riferimento ai comandi AWS CLI
- [RegisterTaskWithMaintenanceWindow](#) nella Documentazione di riferimento API di AWS Systems Manager

### Esempi di registrazione dei task

Le sezioni seguenti forniscono un AWS CLI comando di esempio per la registrazione di un tipo di attività supportato e un esempio JSON che può essere utilizzato con l'opzione. `--cli-input-json`

#### Registra un gestore di sistemi Run Command task

I seguenti esempi illustrano come registrare i task Run Command di Systems Manager con una finestra di manutenzione utilizzando l' AWS CLI.

### Linux & macOS

```
aws ssm register-task-with-maintenance-window \
 --window-id mw-0c50858d01EXAMPLE \
 --task-arn "AWS-RunShellScript" \
 --max-concurrency 1 --max-errors 1 --priority 10 \
 --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE" \
 --task-type "RUN_COMMAND" \
 --cli-input-json file://example.json
```

```
--task-invocation-parameters '{"RunCommand":{"Parameters":{"commands":["df"]}}}'
```

## Windows

```
aws ssm register-task-with-maintenance-window ^
 --window-id mw-0c50858d01EXAMPLE ^
 --task-arn "AWS-RunShellScript" ^
 --max-concurrency 1 --max-errors 1 --priority 10 ^
 --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE" ^
 --task-type "RUN_COMMAND" ^
 --task-invocation-parameters "{\"RunCommand\":{\"Parameters\":{\"commands\":[\"df\"]}}}"
```

Contenuto JSON da utilizzare con l'opzione di file **--cli-input-json**:

```
{
 "TaskType": "RUN_COMMAND",
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Description": "My Run Command task to update SSM Agent on an instance",
 "MaxConcurrency": "1",
 "MaxErrors": "1",
 "Name": "My-Run-Command-Task",
 "Priority": 10,
 "Targets": [
 {
 "Key": "WindowTargetIds",
 "Values": [
 "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
]
 }
],
 "TaskArn": "AWS-UpdateSSMAgent",
 "TaskInvocationParameters": {
 "RunCommand": {
 "Comment": "A TaskInvocationParameters test comment",
 "NotificationConfig": {
 "NotificationArn": "arn:aws:sns:region:123456789012:my-sns-topic-name",
 "NotificationEvents": [
 "All"
],
 "NotificationType": "Invocation"
 }
 }
 },
}
```



```

 "OutputS3BucketName": "amzn-s3-demo-bucket",
 "OutputS3KeyPrefix": "S3-PREFIX",
 "TimeoutSeconds": 3600
 }
}

```

## Registra un task di automazione Systems Manager

I seguenti esempi illustrano come registrare i task di automazione di Systems Manager con una finestra di manutenzione utilizzando l' AWS CLI:

### AWS CLI comando:

#### Linux & macOS

```

aws ssm register-task-with-maintenance-window \
 --window-id "mw-0c50858d01EXAMPLE" \
 --task-arn "AWS-RestartEC2Instance" \
 --service-role-arn arn:aws:iam::123456789012:role/MyMaintenanceWindowServiceRole \
 --task-type AUTOMATION \
 --task-invocation-parameters
 "Automation={DocumentVersion=5,Parameters={InstanceId='{{RESOURCE_ID}}'}}" \
 --priority 0 --name "My-Restart-EC2-Instances-Automation-Task" \
 --description "Automation task to restart EC2 instances"

```

#### Windows

```

aws ssm register-task-with-maintenance-window ^
 --window-id "mw-0c50858d01EXAMPLE" ^
 --task-arn "AWS-RestartEC2Instance" ^
 --service-role-arn arn:aws:iam::123456789012:role/MyMaintenanceWindowServiceRole ^
 --task-type AUTOMATION ^
 --task-invocation-parameters
 "Automation={DocumentVersion=5,Parameters={InstanceId='{{TARGET_ID}}'}}" ^
 --priority 0 --name "My-Restart-EC2-Instances-Automation-Task" ^
 --description "Automation task to restart EC2 instances"

```

Contenuto JSON da utilizzare con l'opzione di file **--cli-input-json**:

```
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "TaskArn": "AWS-PatchInstanceWithRollback",
 "TaskType": "AUTOMATION", "TaskInvocationParameters": {
 "Automation": {
 "DocumentVersion": "1",
 "Parameters": {
 "instanceId": [
 "{{RESOURCE_ID}}"
]
 }
 }
 }
}
```

## Registra un AWS Lambda task

I seguenti esempi illustrano come registrare le operazioni delle funzioni Lambda con una finestra di manutenzione utilizzando la AWS CLI.

### Important

Le funzioni Lambda devono trovarsi nella Account AWS stessa finestra di manutenzione quando si utilizza il ruolo collegato al servizio (). `AWSServiceRoleForAmazonSSM` Cross-account L'invocazione Lambda non è supportata con il ruolo collegato al servizio. Se devi richiamare una funzione Lambda in un account diverso, specifica un ruolo di servizio personalizzato utilizzando il `--service-role-arn` parametro con autorizzazioni esplicitamente limitate all'account di destinazione e aggiungi una policy basata sulle risorse sulla funzione Lambda di destinazione che concede l'accesso di invocazione al tuo ruolo personalizzato.

Per questi esempi, l'utente che ha creato la funzione Lambda ha denominato tale funzione `SSMrestart-my-instances` e ha creato due parametri denominati `instanceId` e `targetType`.

### Important

La policy IAM per Maintenance Windows prevede che il nome (o l'alias) della funzione Lambda sia associato al prefisso SSM. Prima di procedere alla registrazione di questo tipo

di attività, aggiorna il suo nome inserendo. AWS Lambda SSM Ad esempio, se il nome della funzione Lambda è `MyLambdaFunction`, modificalo in `SSMMyLambdaFunction`.

AWS CLI comando:

Linux & macOS

#### Important

Se stai usando la versione 2 di AWS CLI, devi includere l'opzione `--cli-binary-format raw-in-base64-out` nel comando seguente se il payload Lambda non è codificato in base64. L'opzione `cli_binary_format` è disponibile solo nella versione 2. Per informazioni su questa e altre impostazioni dei file, consulta Impostazioni dei file AWS CLI config config file [supportate nella Guida per l'utente](#). AWS Command Line Interface

```
aws ssm register-task-with-maintenance-window \
 --window-id "mw-0c50858d01EXAMPLE" \
 --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" \
 --priority 2 --max-concurrency 10 --max-errors 5 --name "My-Lambda-Example" \
 --description "A description for my LAMBDA example task" --task-type "LAMBDA" \
 --task-arn "arn:aws:lambda:region:123456789012:function:serverlessrepo-SSMrestart-my-instances-C4JF9EXAMPLE" \
 --task-invocation-parameters '{"Lambda":{"Payload":{"\"InstanceId\": \"{{RESOURCE_ID}}\", \"targetType\": \"{{TARGET_TYPE}}\"}, \"Qualifier\": \"$LATEST\"}}'
```

PowerShell

#### Important

Se si utilizza la versione 2 di AWS CLI, è necessario includere l'opzione `--cli-binary-format raw-in-base64-out` nel comando seguente se il payload Lambda non è codificato in base64. L'opzione `cli_binary_format` è disponibile solo nella versione 2. Per informazioni su questa e altre impostazioni dei file, consulta Impostazioni dei file AWS CLI config config file [supportate nella Guida per l'utente](#). AWS Command Line Interface

```
aws ssm register-task-with-maintenance-window `
 --window-id "mw-0c50858d01EXAMPLE" `
 --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" `
 --priority 2 --max-concurrency 10 --max-errors 5 --name "My-Lambda-Example" `
 --description "A description for my LAMBDA example task" --task-type "LAMBDA" `
 --task-arn "arn:aws:lambda:region:123456789012:function:serverlessrepo-
SSMrestart-my-instances-C4JF9EXAMPLE" `
 --task-invocation-parameters '{"Lambda":{"Payload":{"\\"InstanceId\\"":\\"
\\"{{RESOURCE_ID}}\\""},\\"targetType\\"":\\"\\"{{TARGET_TYPE}}\\""},\\"Qualifier\\"":
\\"$LATEST\\"}}'
```

Contenuto JSON da utilizzare con l'opzione di file **--cli-input-json**:

```
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Targets": [
 {
 "Key": "WindowTargetIds",
 "Values": [
 "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
]
 }
],
 "TaskArn": "SSM_RestartMyInstances",
 "TaskType": "LAMBDA",
 "MaxConcurrency": "10",
 "MaxErrors": "10",
 "TaskInvocationParameters": {
 "Lambda": {
 "ClientContext": "ew0KICAi--truncated--0KIEXAMPLE",
 "Payload": "{ \"instanceId\": \"{{RESOURCE_ID}}\", \"targetType\":
\\\"{{TARGET_TYPE}}\\\" }",
 "Qualifier": "$LATEST"
 }
 },
 "Name": "My-Lambda-Task",
 "Description": "A description for my LAMBDA task",
 "Priority": 5
}
```

## Register a Step Functions task (Registra un'attività Step Functions)

I seguenti esempi illustrano come registrare i task delle macchine a stati Step Functions con una finestra di manutenzione utilizzando l' AWS CLI.

### Important

Le macchine a stati di Step Functions devono trovarsi nella Account AWS stessa finestra di manutenzione. Cross-account L'invocazione di Step Functions non è supportata indipendentemente dal fatto che si utilizzi il ruolo collegato al servizio o un ruolo di servizio personalizzato.

### Note

Le attività della finestra di manutenzione supportano solo i flussi di lavoro delle macchine a stati standard di Step Functions. Non supportano i flussi di lavoro delle macchine a stati express. Per informazioni sui tipi di flusso di lavoro delle macchine a stati, consulta [Standard vs. Express Workflows](#) (Differenze flussi di lavoro standard ed express) nella Guida per gli sviluppatori di AWS Step Functions .

Per questi esempi, l'utente che ha creato le macchine a stati Step Functions ha creato una macchina a stati denominata SSMMyStateMachine con un parametro denominato `instanceId`.

### Important

La policy AWS Identity and Access Management (IAM) per Maintenance Windows richiede di anteporre ai nomi delle macchine di stato di Step Functions il prefisso. SSM Prima di procedere alla registrazione di questo tipo di task, è necessario aggiornare il relativo nome in AWS Step Functions in modo da includere SSM. Ad esempio, se il nome della macchina a stati è `MyStateMachine`, modifica tale nome in `SSMMyStateMachine`.

AWS CLI comando:

Linux & macOS

```
aws ssm register-task-with-maintenance-window \
```

```
--window-id "mw-0c50858d01EXAMPLE" \
--targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" \
--task-arn arn:aws:states:region:123456789012:stateMachine:SSMMyStateMachine-
MggiqEXAMPLE \
--task-type STEP_FUNCTIONS \
--task-invocation-parameters '{"StepFunctions":{"Input":{"\"InstanceId\":
\"{{RESOURCE_ID}}\""}, "Name":{"\"{{INVOCATION_ID}}\""}}}' \
--priority 0 --max-concurrency 10 --max-errors 5 \
--name "My-Step-Functions-Task" --description "A description for my Step
Functions task"
```

## PowerShell

```
aws ssm register-task-with-maintenance-window `
--window-id "mw-0c50858d01EXAMPLE" `
--targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" `
--task-arn arn:aws:states:region:123456789012:stateMachine:SSMMyStateMachine-
MggiqEXAMPLE `
--task-type STEP_FUNCTIONS `
--task-invocation-parameters '{"StepFunctions\":{\"Input\":{\"\"\\\\\"InstanceId\\\\
\":\\\\\"{{RESOURCE_ID}}\\\\\"\"}, \"Name\":{\"\"{{INVOCATION_ID}}\"\"}}}' `
--priority 0 --max-concurrency 10 --max-errors 5 `
--name "My-Step-Functions-Task" --description "A description for my Step
Functions task"
```

Contenuto JSON da utilizzare con l'opzione di file **--cli-input-json**:

```
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Targets": [
 {
 "Key": "WindowTargetIds",
 "Values": [
 "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
]
 }
],
 "TaskArn": "SSM_MyStateMachine",
 "TaskType": "STEP_FUNCTIONS",
 "MaxConcurrency": "10",
 "MaxErrors": "10",
 "TaskInvocationParameters": {
```

```
 "StepFunctions": {
 "Input": "{ \"InstanceId\": \"{{TARGET_ID}}\" }",
 "Name": "{{INVOCATION_ID}}"
 },
 "Name": "My-Step-Functions-Task",
 "Description": "A description for my Step Functions task",
 "Priority": 5
 }
```

## Opzioni dei parametri per il comando `register-task-with-maintenance-windows`

Il comando `register-task-with-maintenance-window` dispone di diverse opzioni per la configurazione di un task in base a esigenze specifiche. Alcune opzioni sono obbligatorie, altre sono facoltative, mentre alcune di esse sono valide solo per un tipo specifico di task della finestra di manutenzione.

Questo argomento fornisce informazioni su alcune di queste opzioni a supporto delle procedure di utilizzo degli esempi disponibili in questa sezione del tutorial. Per informazioni su altre opzioni di comando, consulta [register-task-with-maintenance-window](#) nelle Informazioni di riferimento sui comandi AWS CLI .

### Opzione di comando: `--task-arn`

L'opzione `--task-arn` consente di specificare la risorsa utilizzata dal task durante l'operazione. Il valore che è possibile specificare dipende dal tipo di task che si sta registrando, come descritto nella seguente tabella.

#### TaskArn formati per le attività delle finestre di manutenzione

| Tipo di task della finestra di manutenzione | TaskArn valore                                                                                                                                                                                          |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RUN_COMMAND</b> e <b>AUTOMATION</b>      | TaskArn è il nome del documento SSM o l'Amazon Resource Name (ARN). Ad esempio:<br><br>AWS-RunBatchShellScript<br><br>oppure<br><br>arn:aws:ssm: <i>region</i> :11112222<br>3333:document/My-Document . |

| Tipo di task della finestra di manutenzione | TaskArn valore                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>LAMBDA</b>                               | <p>TaskArn è l'ARN o il nome della funzione. Ad esempio:</p> <p>SSMMY-Lambda-Function</p> <p>oppure</p> <p>arn:aws:lambda: <i>region</i>:111122223333:function:SSMMYLambdaFunction .</p> <div data-bbox="829 688 1507 1289"><p> <b>Important</b></p><p>La policy IAM per Maintenance Windows prevede che il nome (o l'alias) della funzione Lambda sia associato al prefisso SSM. Prima di procedere alla registrazione di questo tipo di attività, aggiorna il nome inserendo SSM. AWS Lambda Ad esempio, se il nome della funzione Lambda è MyLambdaFunction , modificalo in SSMMYLambdaFunction .</p></div> <div data-bbox="829 1356 1507 1864"><p> <b>Note</b></p><p>La funzione Lambda deve essere nello stesso account della finestra di manutenzione quando si utilizza il ruolo collegato al servizio. Per l'invocazione tra più account, utilizzala <code>--service-role-arn</code> con un ruolo personalizzato e aggiungi una policy basata sulle risorse sulla funzione di destinazione.</p></div> |



| Tipo di task della finestra di manutenzione | TaskArn valore                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>STEP_FUNCTIONS</b>                       | <p>TaskArn è l'ARN della macchina a stati. Ad esempio:</p> <pre>arn:aws:states:us-east-2:111122223333:stateMachine:SSMMyStateMachine .</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                                             | <div><p> <b>Important</b></p><p>La policy IAM per le finestre di manutenzione prevede che i nomi delle macchine a stati Step Functions siano associati al prefisso SSM. Prima di registrare questo tipo di task, è necessario aggiornare il relativo nome in AWS Step Functions in modo da includere SSM. Ad esempio, se il nome della macchina a stati è <code>MyStateMachine</code> , modifica tale nome in <code>SSMMyStateMachine</code> .</p></div> <div><p> <b>Note</b></p><p>La macchina a stati deve trovarsi nello stesso account della finestra di manutenzione. Non è possibile richiamare una macchina a stati tra più account.</p></div> |

Opzione di comando: `--service-role-arn`

Il ruolo da assumere durante l'esecuzione del AWS Systems Manager task della finestra di manutenzione.

Per ulteriori informazioni, consulta [Configurazione Intervallo di manutenzione](#)

Opzione di comando: **--task-invocation-parameters**

L'opzione `--task-invocation-parameters` viene utilizzata per specificare i parametri univoci per ciascuno dei quattro tipi di task. I parametri supportati per ciascuno dei quattro tipi di task sono descritti nella tabella riportata di seguito.

 Note

Per informazioni sull'utilizzo degli pseudoparametri nel contenuto `--task-invocation-parameters`, ad esempio `{{TARGET_ID}}`, consulta [Utilizzo degli pseudo parametri durante la registrazione delle attività della finestra di manutenzione](#).

Opzioni dei parametri di invocazione dei task per i task della finestra di manutenzione

| Tipo di task della finestra di manutenzione | Parametri disponibili | Esempio                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RUN_COMMAND                                 | Comment               | <pre>"TaskInvocationParameters": {   "RunCommand": {     "Comment" : "My Run Command task comment",     "DocumentHash": "6554ed3d--truncated--5EXAMPLE",     "DocumentHashType": "Sha256",     "NotificationConfig": {       "NotificationArn": "arn:aws:sns:region:123456789012:my-sns-topic-name",</pre> |
|                                             | DocumentHash          |                                                                                                                                                                                                                                                                                                            |
|                                             | DocumentHashType      |                                                                                                                                                                                                                                                                                                            |
|                                             | NotificationConfig    |                                                                                                                                                                                                                                                                                                            |
|                                             | OutputS3BucketName    |                                                                                                                                                                                                                                                                                                            |
|                                             | OutPutS3KeyPrefix     |                                                                                                                                                                                                                                                                                                            |
|                                             | Parameters            |                                                                                                                                                                                                                                                                                                            |
|                                             | ServiceRoleArn        |                                                                                                                                                                                                                                                                                                            |
|                                             | TimeoutSeconds        |                                                                                                                                                                                                                                                                                                            |

| Tipo di task della finestra di manutenzione | Parametri disponibili | Esempio                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                             |                       | <pre>"NotificationEvents": [     "FAILURE" ],  "NotificationType": "Invocation" }, "OutputS3 BucketName": "amzn-s3- demo-bucket", "OutputS3 KeyPrefix": "  S3-PREFIX ", "Paramete rs": {  "commands": [  "Get-ChildItem\$env: temp-Recurse Remove- Item-Recurse-force" ] }, "ServiceR oleArn": "arn:aws: iam::123456789012: role/MyMaintenance WindowServiceRole", "TimeoutS econds": 3600 } }</pre> |

| Tipo di task della finestra di manutenzione | Parametri disponibili                         | Esempio                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AUTOMATION</b>                           | DocumentVersion<br><br>Parameters             | <pre>"TaskInvocationParameters": {<br/>    "Automation": {<br/>        "DocumentVersion": "3",<br/>        "Parameters": {<br/><br/>            "instanceid": [<br/><br/>                "{{TARGET_ID}}"<br/>            ]<br/>        }<br/>    }<br/>}</pre>                                                             |
| <b>LAMBDA</b>                               | ClientContext<br><br>Payload<br><br>Qualifier | <pre>"TaskInvocationParameters": {<br/>    "Lambda": {<br/>        "ClientContext": "ew0KICAi<br/>--truncated--0KIEX<br/>AMPLE",<br/>        "Payload": "{ \"targetId\":<br/>\\\"{{TARGET_ID}}\\\",<br/>\\\"targetType\":<br/>\\\"{{TARGET_TYPE}}\\\"<br/>\" }",<br/>        "Qualifier": "\$LATEST"<br/>    }<br/>}</pre> |

| Tipo di task della finestra di manutenzione | Parametri disponibili | Esempio                                                                                                                                                         |
|---------------------------------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>STEP_FUNCTIONS</b>                       | Input<br><br>Name     | <pre> "TaskInvocationParameters": {   "StepFunctions": {     "Input":       "{ \"targetId\": \"{{TARGET_ID}}\", \"Name\": \"{{INVOCATION_ID}}\" }"   } } </pre> |

Tutorial: Visualizza le informazioni sulle finestre di manutenzione utilizzando il AWS CLI

Questo tutorial include comandi che consentono di aggiornare o ottenere informazioni su finestre di manutenzione, task, esecuzioni e invocazioni. Gli esempi sono organizzati per comando, per dimostrare come utilizzare le opzioni dei comandi per filtrare il tipo di dettaglio che si desidera visualizzare.

Man mano che segui i passaggi di questo tutorial, sostituisci i valori in corsivo con le **red** tue opzioni e i tuoi ID. Ad esempio, sostituisci l'ID della finestra di manutenzione ***mw-0c50858d01EXAMPLE*** e l'ID dell'istanza ***i-02573cafcfEXAMPLE*** con gli ID delle risorse che crei.

Per informazioni sull'impostazione e la configurazione di AWS Command Line Interface (AWS CLI), consultate [Installazione, aggiornamento e disinstallazione di AWS CLI](#) e [Configurazione](#) di AWS CLI.

### Esempi di comando

- [Esempi per "describe-maintenance-windows"](#)
- [Esempi per "describe-maintenance-window-targets"](#)
- [Esempi per "describe-maintenance-window-tasks"](#)
- [Esempi per "describe-maintenance-windows-for-target"](#)
- [Esempi per "describe-maintenance-window-executions"](#)
- [Esempi per "describe-maintenance-window-schedule"](#)

## Esempi per "describe-maintenance-windows"

Elenca tutte le finestre di manutenzione presenti nel Account AWS

Eseguire il seguente comando seguente.

```
aws ssm describe-maintenance-windows
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowIdentities": [
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "My-First-Maintenance-Window",
 "Enabled": true,
 "Duration": 2,
 "Cutoff": 0,
 "NextExecutionTime": "2019-05-18T17:01:01.137Z"
 },
 {
 "WindowId": "mw-9a8b7c6d5eEXAMPLE",
 "Name": "My-Second-Maintenance-Window",
 "Enabled": true,
 "Duration": 4,
 "Cutoff": 1,
 "NextExecutionTime": "2019-05-30T03:30:00.137Z"
 }
]
}
```

Elenca tutte le finestre di manutenzione abilitate

Eseguire il seguente comando seguente.

```
aws ssm describe-maintenance-windows --filters "Key=Enabled,Values=true"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowIdentities": [
```

```
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "My-First-Maintenance-Window",
 "Enabled": true,
 "Duration": 2,
 "Cutoff": 0,
 "NextExecutionTime": "2019-05-18T17:01:01.137Z"
},
{
 "WindowId": "mw-9a8b7c6d5eEXAMPLE",
 "Name": "My-Second-Maintenance-Window",
 "Enabled": true,
 "Duration": 4,
 "Cutoff": 1,
 "NextExecutionTime": "2019-05-30T03:30:00.137Z"
},
]
```

Elenca tutte le finestre di manutenzione disabilitate

Eseguire il seguente comando seguente.

```
aws ssm describe-maintenance-windows --filters "Key=Enabled,Values=false"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowIdentities": [
 {
 "WindowId": "mw-6e5c9d4b7cEXAMPLE",
 "Name": "My-Disabled-Maintenance-Window",
 "Enabled": false,
 "Duration": 2,
 "Cutoff": 1
 }
]
}
```

Elenca tutte le finestre di manutenzione con nomi che iniziano con un determinato prefisso

Eseguire il seguente comando seguente.

```
aws ssm describe-maintenance-windows --filters "Key=Name,Values=My"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowIdentities": [
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "My-First-Maintenance-Window",
 "Enabled": true,
 "Duration": 2,
 "Cutoff": 0,
 "NextExecutionTime": "2019-05-18T17:01:01.137Z"
 },
 {
 "WindowId": "mw-9a8b7c6d5eEXAMPLE",
 "Name": "My-Second-Maintenance-Window",
 "Enabled": true,
 "Duration": 4,
 "Cutoff": 1,
 "NextExecutionTime": "2019-05-30T03:30:00.137Z"
 },
 {
 "WindowId": "mw-6e5c9d4b7cEXAMPLE",
 "Name": "My-Disabled-Maintenance-Window",
 "Enabled": false,
 "Duration": 2,
 "Cutoff": 1
 }
]
}
```

### Esempi per "describe-maintenance-window-targets"

Visualizza le destinazioni di una finestra di manutenzione che corrispondono a un determinato valore delle informazioni dello specifico proprietario

Eseguire il seguente comando seguente.

### Linux & macOS

```
aws ssm describe-maintenance-window-targets \
```



```
--window-id "mw-6e5c9d4b7cEXAMPLE" \
--filters "Key=OwnerInformation,Values=CostCenter1"
```

## Windows

```
aws ssm describe-maintenance-window-targets ^
--window-id "mw-6e5c9d4b7cEXAMPLE" ^
--filters "Key=OwnerInformation,Values=CostCenter1"
```

### Note

Le chiavi di filtro supportate sono Type, WindowTargetId e OwnerInformation.

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "Targets": [
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowTargetId": "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE",
 "ResourceType": "INSTANCE",
 "Targets": [
 {
 "Key": "tag:Name",
 "Values": [
 "Production"
]
 }
],
 "OwnerInformation": "CostCenter1",
 "Name": "Target1"
 }
]
}
```

Esempi per "describe-maintenance-window-tasks"

Mostra tutte le attività registrate che richiamano al documento del comando SSM **AWS-RunPowerShellScript**

Eseguire il seguente comando seguente.

## Linux & macOS

```
aws ssm describe-maintenance-window-tasks \
 --window-id "mw-0c50858d01EXAMPLE" \
 --filters "Key=TaskArn,Values=AWS-RunPowerShellScript"
```

## Windows

```
aws ssm describe-maintenance-window-tasks ^
 --window-id "mw-0c50858d01EXAMPLE" ^
 --filters "Key=TaskArn,Values=AWS-RunPowerShellScript"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "Tasks":[
 {
 "ServiceRoleArn": "arn:aws:iam::111122223333:role/
MyMaintenanceWindowServiceRole",
 "MaxErrors":"1",
 "TaskArn":"AWS-RunPowerShellScript",
 "MaxConcurrency":"1",
 "WindowTaskId":"4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
 "TaskParameters":{"
 "commands":{"
 "Values":[
 "driverquery.exe"
]
 }
 },
 "Priority":3,
 "Type":"RUN_COMMAND",
 "Targets":[
 {
 "TaskTargetId":"i-02573cafcfEXAMPLE",
 "TaskTargetType":"INSTANCE"
 }
]
 },
 {
```

```

 "ServiceRoleArn": "arn:aws:iam::111122223333:role/
MyMaintenanceWindowServiceRole",
 "MaxErrors": "1",
 "TaskArn": "AWS-RunPowerShellScript",
 "MaxConcurrency": "1",
 "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
 "TaskParameters": {
 "commands": {
 "Values": [
 "ipconfig"
]
 }
 },
 "Priority": 1,
 "Type": "RUN_COMMAND",
 "Targets": [
 {
 "TaskTargetId": "i-02573cafcfEXAMPLE",
 "TaskTargetType": "WINDOW_TARGET"
 }
]
}
]
}
}

```

Mostra tutte le attività registrate che hanno una priorità di "3"

Eseguire il seguente comando seguente.

### Linux & macOS

```

aws ssm describe-maintenance-window-tasks \
 --window-id "mw-9a8b7c6d5eEXAMPLE" \
 --filters "Key=Priority,Values=3"

```

### Windows

```

aws ssm describe-maintenance-window-tasks ^
 --window-id "mw-9a8b7c6d5eEXAMPLE" ^
 --filters "Key=Priority,Values=3"

```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "Tasks":[
 {
 "ServiceRoleArn":"arn:aws:iam::111122223333:role/
MyMaintenanceWindowServiceRole",
 "MaxErrors":"1",
 "TaskArn":"AWS-RunPowerShellScript",
 "MaxConcurrency":"1",
 "WindowTaskId":"4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
 "TaskParameters":{"
 "commands":{"
 "Values":[
 "driverquery.exe"
]
 }
 },
 "Priority":3,
 "Type":"RUN_COMMAND",
 "Targets":[
 {
 "TaskTargetId":"i-02573cafcfEXAMPLE",
 "TaskTargetType":"INSTANCE"
 }
]
 }
]
}
```

Mostra tutte le attività registrate che hanno una priorità di "1" e utilizzano Run Command

Eseguire il seguente comando seguente.

## Linux & macOS

```
aws ssm describe-maintenance-window-tasks \
 --window-id "mw-0c50858d01EXAMPLE" \
 --filters "Key=Priority,Values=1" "Key=TaskType,Values=RUN_COMMAND"
```

## Windows

```
aws ssm describe-maintenance-window-tasks ^
 --window-id "mw-0c50858d01EXAMPLE" ^
```

```
--filters "Key=Priority,Values=1" "Key=TaskType,Values=RUN_COMMAND"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "Tasks": [
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
 "TaskArn": "AWS-RunShellScript",
 "Type": "RUN_COMMAND",
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
 "i-02573cafcfEXAMPLE"
]
 }
],
 "TaskParameters": {},
 "Priority": 1,
 "ServiceRoleArn": "arn:aws:iam::111122223333:role/MyMaintenanceWindowServiceRole",
 "MaxConcurrency": "1",
 "MaxErrors": "1"
 },
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowTaskId": "8a5c4629-31b0-4edd-8aea-33698EXAMPLE",
 "TaskArn": "AWS-UpdateSSMAgent",
 "Type": "RUN_COMMAND",
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
 "i-0471e04240EXAMPLE"
]
 }
],
 "TaskParameters": {},
 "Priority": 1,
 }
]
}
```

```
 "ServiceRoleArn": "arn:aws:iam::111122223333:role/MyMaintenanceWindowServiceRole",
 "MaxConcurrency": "1",
 "MaxErrors": "1",
 "Name": "My-Run-Command-Task",
 "Description": "My Run Command task to update SSM Agent on an instance"
 }
]
```

## Esempi per "describe-maintenance-windows-for-target"

Elenca le informazioni sulle destinazioni della finestra di manutenzione o sui task associati a un nodo specifico.

Eseguire il seguente comando seguente.

### Linux & macOS

```
aws ssm describe-maintenance-windows-for-target \
 --resource-type INSTANCE \
 --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE" \
 --max-results 10
```

### Windows

```
aws ssm describe-maintenance-windows-for-target ^
 --resource-type INSTANCE ^
 --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE" ^
 --max-results 10
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowIdentities": [
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "My-First-Maintenance-Window"
 },
 {
 "WindowId": "mw-9a8b7c6d5eEXAMPLE",
 "Name": "My-Second-Maintenance-Window"
 }
]
}
```

```
 }
]
}
```

Esempi per "describe-maintenance-window-executions"

Visualizza tutte le attività eseguite prima di una determinata data

Eseguire il seguente comando seguente.

Linux & macOS

```
aws ssm describe-maintenance-window-executions \
 --window-id "mw-9a8b7c6d5eEXAMPLE" \
 --filters "Key=ExecutedBefore,Values=2019-05-12T05:00:00Z"
```

Windows

```
aws ssm describe-maintenance-window-executions ^
 --window-id "mw-9a8b7c6d5eEXAMPLE" ^
 --filters "Key=ExecutedBefore,Values=2019-05-12T05:00:00Z"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowExecutions": [
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowExecutionId": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
 "Status": "FAILED",
 "StatusDetails": "The following SSM parameters are invalid: LevelUp",
 "StartTime": 1557617747.993,
 "EndTime": 1557617748.101
 },
 {
 "WindowId": "mw-9a8b7c6d5eEXAMPLE",
 "WindowExecutionId": "791b72e0-f0da-4021-8b35-f95dfEXAMPLE",
 "Status": "SUCCESS",
 "StartTime": 1557594085.428,
 "EndTime": 1557594090.978
 },
],
}
```

```

 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowExecutionId": "ecec60fa-6bb0-4d26-98c7-140308EXAMPLE",
 "Status": "SUCCESS",
 "StartTime": 1557593793.483,
 "EndTime": 1557593798.978
 }
]
}

```

Elenca tutte le attività eseguite dopo una determinata data

Eseguire il seguente comando seguente.

## Linux & macOS

```

aws ssm describe-maintenance-window-executions \
 --window-id "mw-9a8b7c6d5eEXAMPLE" \
 --filters "Key=ExecutedAfter,Values=2018-12-31T17:00:00Z"

```

## Windows

```

aws ssm describe-maintenance-window-executions ^
 --window-id "mw-9a8b7c6d5eEXAMPLE" ^
 --filters "Key=ExecutedAfter,Values=2018-12-31T17:00:00Z"

```

Questo sistema restituisce informazioni simili alle seguenti.

```

{
 "WindowExecutions": [
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowExecutionId": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
 "Status": "FAILED",
 "StatusDetails": "The following SSM parameters are invalid: LevelUp",
 "StartTime": 1557617747.993,
 "EndTime": 1557617748.101
 },
 {
 "WindowId": "mw-9a8b7c6d5eEXAMPLE",
 "WindowExecutionId": "791b72e0-f0da-4021-8b35-f95dfEXAMPLE",
 "Status": "SUCCESS",
 "StartTime": 1557594085.428,

```



```

 "EndTime": 1557594090.978
 },
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowExecutionId": "ecec60fa-6bb0-4d26-98c7-140308EXAMPLE",
 "Status": "SUCCESS",
 "StartTime": 1557593793.483,
 "EndTime": 1557593798.978
 }
]
 }

```

## Esempi per "describe-maintenance-window-schedule"

Visualizza le prossime dieci esecuzioni programmate della finestra di manutenzione per un determinato nodo.

Eseguire il seguente comando seguente.

### Linux & macOS

```

aws ssm describe-maintenance-window-schedule \
 --resource-type INSTANCE \
 --targets "Key=InstanceIds,Values=i-07782c72faEXAMPLE" \
 --max-results 10

```

### Windows

```

aws ssm describe-maintenance-window-schedule ^
 --resource-type INSTANCE ^
 --targets "Key=InstanceIds,Values=i-07782c72faEXAMPLE" ^
 --max-results 10

```

Questo sistema restituisce informazioni simili alle seguenti.

```

{
 "ScheduledWindowExecutions": [
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "My-First-Maintenance-Window",
 "ExecutionTime": "2019-05-18T23:35:24.902Z"
 },

```

```
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "My-First-Maintenance-Window",
 "ExecutionTime": "2019-05-25T23:35:24.902Z"
},
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "My-First-Maintenance-Window",
 "ExecutionTime": "2019-06-01T23:35:24.902Z"
},
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "My-First-Maintenance-Window",
 "ExecutionTime": "2019-06-08T23:35:24.902Z"
},
{
 "WindowId": "mw-9a8b7c6d5eEXAMPLE",
 "Name": "My-Second-Maintenance-Window",
 "ExecutionTime": "2019-06-15T23:35:24.902Z"
},
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "My-First-Maintenance-Window",
 "ExecutionTime": "2019-06-22T23:35:24.902Z"
},
{
 "WindowId": "mw-9a8b7c6d5eEXAMPLE",
 "Name": "My-Second-Maintenance-Window",
 "ExecutionTime": "2019-06-29T23:35:24.902Z"
},
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "My-First-Maintenance-Window",
 "ExecutionTime": "2019-07-06T23:35:24.902Z"
},
{
 "WindowId": "mw-9a8b7c6d5eEXAMPLE",
 "Name": "My-Second-Maintenance-Window",
 "ExecutionTime": "2019-07-13T23:35:24.902Z"
},
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "My-First-Maintenance-Window",
 "ExecutionTime": "2019-07-20T23:35:24.902Z"
}
```

```
 }
],
 "NextToken": "AAEABUXdceT92FvtKld/dGHELj5Mi+GKW/EXAMPLE"
}
```

Visualizza la pianificazione della finestra di manutenzione per i nodi taggati con una determinata coppia chiave-valore

Eseguire il seguente comando seguente.

### Linux & macOS

```
aws ssm describe-maintenance-window-schedule \
 --resource-type INSTANCE \
 --targets "Key=tag:prod,Values=rhel7"
```

### Windows

```
aws ssm describe-maintenance-window-schedule ^
 --resource-type INSTANCE ^
 --targets "Key=tag:prod,Values=rhel7"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "ScheduledWindowExecutions": [
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "DemoRateStartDate",
 "ExecutionTime": "2019-10-20T05:34:56-07:00"
 },
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "DemoRateStartDate",
 "ExecutionTime": "2019-10-21T05:34:56-07:00"
 },
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "DemoRateStartDate",
 "ExecutionTime": "2019-10-22T05:34:56-07:00"
 },
],
}
```

```
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "DemoRateStartDate",
 "ExecutionTime": "2019-10-23T05:34:56-07:00"
},
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "Name": "DemoRateStartDate",
 "ExecutionTime": "2019-10-24T05:34:56-07:00"
}
],
"NextToken": "AAEABccwSXqQRGKiTZ1yzGELR6cxW4W/EXAMPLE"
}
```

Visualizza gli orari di inizio delle prossime quattro esecuzioni di una finestra di manutenzione

Eseguire il seguente comando seguente.

## Linux & macOS

```
aws ssm describe-maintenance-window-schedule \
 --window-id "mw-0c50858d01EXAMPLE" \
 --max-results "4"
```

## Windows

```
aws ssm describe-maintenance-window-schedule ^
 --window-id "mw-0c50858d01EXAMPLE" ^
 --max-results "4"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowSchedule": [
 {
 "ScheduledWindowExecutions": [
 {
 "ExecutionTime": "2019-10-04T10:10:10Z",
 "Name": "My-First-Maintenance-Window",
 "WindowId": "mw-0c50858d01EXAMPLE"
 },
 {
```

```

 "ExecutionTime": "2019-10-11T10:10:10Z",
 "Name": "My-First-Maintenance-Window",
 "WindowId": "mw-0c50858d01EXAMPLE"
 },
 {
 "ExecutionTime": "2019-10-18T10:10:10Z",
 "Name": "My-First-Maintenance-Window",
 "WindowId": "mw-0c50858d01EXAMPLE"
 },
 {
 "ExecutionTime": "2019-10-25T10:10:10Z",
 "Name": "My-First-Maintenance-Window",
 "WindowId": "mw-0c50858d01EXAMPLE"
 }
]
}

```

Tutorial: Visualizza informazioni sulle attività e sulle esecuzioni delle attività utilizzando il AWS CLI

Questo tutorial dimostra come utilizzare AWS Command Line Interface (AWS CLI) per visualizzare i dettagli sulle attività completate nella finestra di manutenzione.

Se arrivi direttamente da [Tutorial: Creare e configurare una finestra di manutenzione utilizzando il AWS CLI](#), verifica di aver lasciato tempo sufficiente alla finestra di manutenzione per completare l'esecuzione almeno una volta al fine di visualizzare i risultati dell'esecuzione.

Man mano che seguite i passaggi di questo tutorial, sostituite i valori nel **red** testo in corsivo con le vostre opzioni e ID. Ad esempio, sostituisci l'ID della finestra di manutenzione ***mw-0c50858d01EXAMPLE*** e l'ID dell'istanza ***i-02573cafcfEXAMPLE*** con gli ID delle risorse che crei.

Per visualizzare informazioni sulle attività e sulle esecuzioni delle attività utilizzando il AWS CLI

1. Per visualizzare un elenco di esecuzioni delle attività per una specifica finestra di manutenzione, eseguire il seguente comando.

Linux & macOS

```
aws ssm describe-maintenance-window-executions \
 --window-id "mw-0c50858d01EXAMPLE"
```

## Windows

```
aws ssm describe-maintenance-window-executions ^
 --window-id "mw-0c50858d01EXAMPLE"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowExecutions": [
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowExecutionId": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
 "Status": "SUCCESS",
 "StartTime": 1557593793.483,
 "EndTime": 1557593798.978
 },
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowExecutionId": "791b72e0-f0da-4021-8b35-f95dfEXAMPLE",
 "Status": "SUCCESS",
 "StartTime": 1557593493.096,
 "EndTime": 1557593498.611
 },
 {
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowExecutionId": "ecec60fa-6bb0-4d26-98c7-140308EXAMPLE",
 "Status": "SUCCESS",
 "StatusDetails": "No tasks to execute.",
 "StartTime": 1557593193.309,
 "EndTime": 1557593193.334
 }
]
}
```

2. Per ottenere informazioni sull'esecuzione di un'attività in una finestra di manutenzione, eseguire il seguente comando.

## Linux & macOS

```
aws ssm get-maintenance-window-execution \
```

```
--window-execution-id "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE"
```

## Windows

```
aws ssm get-maintenance-window-execution ^
--window-execution-id "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowExecutionId": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
 "TaskIds": [
 "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE"
],
 "Status": "SUCCESS",
 "StartTime": 1557593493.096,
 "EndTime": 1557593498.611
}
```

3. Per visualizzare l'elenco delle attività completate nell'ambito di un'esecuzione di una finestra di manutenzione, eseguire il seguente comando.

## Linux & macOS

```
aws ssm describe-maintenance-window-execution-tasks \
--window-execution-id "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE"
```

## Windows

```
aws ssm describe-maintenance-window-execution-tasks ^
--window-execution-id "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowExecutionTaskIdentities": [
 {
 "WindowExecutionId": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
 "TaskExecutionId": "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE",
 }
]
}
```

```

 "Status": "SUCCESS",
 "StartTime": 1557593493.162,
 "EndTime": 1557593498.57,
 "TaskArn": "AWS-RunShellScript",
 "TaskType": "RUN_COMMAND"
 }
]
}

```

4. Per ottenere informazioni su un'esecuzione di attività, esegui il seguente comando.

### Linux & macOS

```

aws ssm get-maintenance-window-execution-task \
 --window-execution-id "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE" \
 --task-id "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE"

```

### Windows

```

aws ssm get-maintenance-window-execution-task ^
 --window-execution-id "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE" ^
 --task-id "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE"

```

Questo sistema restituisce informazioni simili alle seguenti.

```

{
 "WindowExecutionId": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
 "TaskExecutionId": "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE",
 "TaskArn": "AWS-RunShellScript",
 "ServiceRole": "arn:aws:iam::111122223333:role/MyMaintenanceWindowServiceRole",
 "Type": "RUN_COMMAND",
 "TaskParameters": [
 {
 "aws:InstanceId": {
 "Values": [
 "i-02573cafcfEXAMPLE"
]
 },
 "commands": {
 "Values": [
 "df"
]
 }
 }
]
}

```



```

]
 }
}
],
"Priority": 10,
"MaxConcurrency": "1",
"MaxErrors": "1",
"Status": "SUCCESS",
"StartTime": 1557593493.162,
"EndTime": 1557593498.57
}

```

5. Per ottenere la specifica chiamata dell'attività eseguita per l'esecuzione di un'attività, esegui il seguente comando.

#### Linux & macOS

```

aws ssm describe-maintenance-window-execution-task-invocations \
 --window-execution-id "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE" \
 --task-id "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE"

```

#### Windows

```

aws ssm describe-maintenance-window-execution-task-invocations ^
 --window-execution-id "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE" ^
 --task-id "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE"

```

Questo sistema restituisce informazioni simili alle seguenti.

```

{
 "WindowExecutionTaskInvocationIdentities": [
 {
 "WindowExecutionId": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
 "TaskExecutionId": "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE",
 "InvocationId": "c336d2ab-09de-44ba-8f6a-6136cEXAMPLE",
 "ExecutionId": "76a5a04f-caf6-490c-b448-92c02EXAMPLE",
 "TaskType": "RUN_COMMAND",
 "Parameters": "{\"documentName\":\"AWS-RunShellScript\",\"instanceIds\":[\"i-02573cafcfEXAMPLE\"],\"maxConcurrency\":\"1\",\"maxErrors\":\"1\", \"parameters\":{\"commands\":[\"df\"]}}",
 "Status": "SUCCESS",
 }
]
}

```

```
 "StatusDetails": "Success",
 "StartTime": 1557593493.222,
 "EndTime": 1557593498.466
 }
]
 }
```

## Tutorial: Aggiornare una finestra di manutenzione utilizzando il AWS CLI

Questo tutorial dimostra come utilizzare AWS Command Line Interface (AWS CLI) per aggiornare una finestra di manutenzione. Mostra anche come aggiornare diversi tipi di attività, inclusi quelli per AWS Systems Manager Run Command e Automation AWS Lambda, e AWS Step Functions.

Gli esempi di questa sezione utilizzano le seguenti operazioni Systems Manager per l'aggiornamento di una finestra di manutenzione:

- [UpdateMaintenanceWindow](#)
- [UpdateMaintenanceWindowTarget](#)
- [UpdateMaintenanceWindowTask](#)
- [DeregisterTargetFromMaintenanceWindow](#)

Per informazioni sull'utilizzo della console di Systems Manager per aggiornare una finestra di manutenzione, consulta [Aggiorna o elimina le risorse della finestra di manutenzione utilizzando la console](#).

Mentre segui i passaggi di questo tutorial, sostituisci i valori in *red* testo in corsivo con le tue opzioni e i tuoi ID. Ad esempio, sostituisci l'ID della finestra di manutenzione *mw-0c50858d01EXAMPLE* e l'ID dell'istanza *i-02573cafcfEXAMPLE* con gli ID delle risorse che crei.

## Per aggiornare una finestra di manutenzione utilizzando il AWS CLI

1. Apri AWS CLI ed esegui il seguente comando per aggiornare una destinazione in modo che includa un nome e una descrizione.

### Linux & macOS

```
aws ssm update-maintenance-window-target \
 --window-id "mw-0c50858d01EXAMPLE" \
 --window-target-id "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" \
```

```
--name "My-Maintenance-Window-Target" \
--description "Description for my maintenance window target"
```

## Windows

```
aws ssm update-maintenance-window-target ^
--window-id "mw-0c50858d01EXAMPLE" ^
--window-target-id "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" ^
--name "My-Maintenance-Window-Target" ^
--description "Description for my maintenance window target"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowTargetId": "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE",
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
 "i-02573cafcfEXAMPLE"
]
 }
],
 "Name": "My-Maintenance-Window-Target",
 "Description": "Description for my maintenance window target"
}
```

2. Eseguire questo comando per utilizzare l'opzione `replace` per rimuovere il campo descrizione e aggiungere un'ulteriore destinazione. Il campo descrizione è rimosso, perché l'aggiornamento non include il campo (valore nullo). Assicurarsi di specificare un nodo aggiuntivo configurato per l'utilizzo con Systems Manager.

## Linux & macOS

```
aws ssm update-maintenance-window-target \
--window-id "mw-0c50858d01EXAMPLE" \
--window-target-id "d208dedf-3f6b-41ff-ace8-8e751EXAMPLE" \
--targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE" \
--name "My-Maintenance-Window-Target" \

```

```
--replace
```

## Windows

```
aws ssm update-maintenance-window-target ^
 --window-id "mw-0c50858d01EXAMPLE" ^
 --window-target-id "d208dedf-3f6b-41ff-ace8-8e751EXAMPLE" ^
 --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE" ^
 --name "My-Maintenance-Window-Target" ^
 --replace
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowTargetId": "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE",
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
 "i-02573cafcfEXAMPLE",
 "i-0471e04240EXAMPLE"
]
 }
],
 "Name": "My-Maintenance-Window-Target"
}
```

3. L'`start-date` opzione consente di ritardare l'attivazione di una finestra di manutenzione fino a una data futura specificata. L'`end-date` opzione consente di impostare una data e un'ora future dopo le quali la finestra di manutenzione non viene più eseguita. Specificate le opzioni in formato ISO-8601 esteso.

Eseguire il comando seguente per specificare un intervallo di data e ora per esecuzioni regolarmente pianificate della finestra di manutenzione.

## Linux & macOS

```
aws ssm update-maintenance-window \
 --window-id "mw-0c50858d01EXAMPLE" \
 --start-date "2020-10-01T10:10:10Z" \
 --replace
```

```
--end-date "2020-11-01T10:10:10Z"
```

## Windows

```
aws ssm update-maintenance-window ^
 --window-id "mw-0c50858d01EXAMPLE" ^
 --start-date "2020-10-01T10:10:10Z" ^
 --end-date "2020-11-01T10:10:10Z"
```

4. Esegui il seguente comando per aggiornare un task Run Command.

### Tip

Se il target è un'istanza Amazon Elastic Compute Cloud (Amazon EC2) per Windows Server, modifica da `df` a `ipconfig` e da `AWS-RunShellScript` a `AWS-RunPowerShellScript` nel comando seguente.

## Linux & macOS

```
aws ssm update-maintenance-window-task \
 --window-id "mw-0c50858d01EXAMPLE" \
 --window-task-id "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE" \
 --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" \
 --task-arn "AWS-RunShellScript" \
 --service-role-arn "arn:aws:iam::account-id:role/MaintenanceWindowsRole" \
 --task-invocation-parameters "RunCommand={Comment=Revising my Run Command task,Parameters={commands=df}}" \
 --priority 1 --max-concurrency 10 --max-errors 4 \
 --name "My-Task-Name" --description "A description for my Run Command task"
```

## Windows

```
aws ssm update-maintenance-window-task ^
 --window-id "mw-0c50858d01EXAMPLE" ^
 --window-task-id "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE" ^
 --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" ^
 --task-arn "AWS-RunShellScript" ^
 --service-role-arn "arn:aws:iam::account-id:role/MaintenanceWindowsRole" ^
```

```
--task-invocation-parameters "RunCommand={Comment=Revising my Run Command task,Parameters={commands=df}}" ^
--priority 1 --max-concurrency 10 --max-errors 4 ^
--name "My-Task-Name" --description "A description for my Run Command task"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
 "Targets": [
 {
 "Key": "WindowTargetIds",
 "Values": [
 "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
]
 }
],
 "TaskArn": "AWS-RunShellScript",
 "ServiceRoleArn": "arn:aws:iam::111122223333:role/MaintenanceWindowsRole",
 "TaskParameters": {},
 "TaskInvocationParameters": {
 "RunCommand": {
 "Comment": "Revising my Run Command task",
 "Parameters": {
 "commands": [
 "df"
]
 }
 }
 },
 "Priority": 1,
 "MaxConcurrency": "10",
 "MaxErrors": "4",
 "Name": "My-Task-Name",
 "Description": "A description for my Run Command task"
}
```

5. Adatta ed esegui il seguente comando per aggiornare un task Lambda.

## Linux &amp; macOS

```
aws ssm update-maintenance-window-task \
 --window-id mw-0c50858d01EXAMPLE \
 --window-task-id 4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE \
 --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" \
 --task-arn "arn:aws:lambda:region:111122223333:function:SSMTestLambda" \
 --service-role-arn "arn:aws:iam:account-id:role/MaintenanceWindowsRole" \
 --task-invocation-parameters '{"Lambda":{"Payload":"{\"InstanceId\":
\"{{RESOURCE_ID}}\", \"targetType\": \"{{TARGET_TYPE}}\"}}' \
 --priority 1 --max-concurrency 10 --max-errors 5 \
 --name "New-Lambda-Task-Name" \
 --description "A description for my Lambda task"
```

## Windows

```
aws ssm update-maintenance-window-task ^
 --window-id mw-0c50858d01EXAMPLE ^
 --window-task-id 4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE ^
 --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" ^
 --task-arn --task-arn
 "arn:aws:lambda:region:111122223333:function:SSMTestLambda" ^
 --service-role-arn "arn:aws:iam:account-id:role/MaintenanceWindowsRole" ^
 --task-invocation-parameters '{"Lambda":{"Payload":"{\"InstanceId\":
\"{{RESOURCE_ID}}\", \"targetType\": \"{{TARGET_TYPE}}\"}}' ^
 --priority 1 --max-concurrency 10 --max-errors 5 ^
 --name "New-Lambda-Task-Name" ^
 --description "A description for my Lambda task"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
 "Targets": [
 {
 "Key": "WindowTargetIds",
 "Values": "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
```

```

 }
],
 "TaskArn": "arn:aws:lambda:us-east-2:111122223333:function:SSMTestLambda",
 "ServiceRoleArn": "arn:aws:iam::111122223333:role/MaintenanceWindowsRole",
 "TaskParameters": {},
 "TaskInvocationParameters": {
 "Lambda": {
 "Payload": "e30="
 }
 },
 "Priority": 1,
 "MaxConcurrency": "10",
 "MaxErrors": "5",
 "Name": "New-Lambda-Task-Name",
 "Description": "A description for my Lambda task"
}

```

6. In caso di aggiornamento di un task Step Functions, adatta ed esegui il comando seguente per aggiornare la relativa voce task-invocation-parameters.

## Linux & macOS

```

aws ssm update-maintenance-window-task \
 --window-id "mw-0c50858d01EXAMPLE" \
 --window-task-id "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE" \
 --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" \
 --task-arn "arn:aws:states:region:execution:SSMStepFunctionTest" \
 --service-role-arn "arn:aws:iam:account-id:role/MaintenanceWindowsRole" \
 --task-invocation-parameters '{"StepFunctions":{"Input":{"InstanceId":\
 \{"{{RESOURCE_ID}}\"}"}}}' \
 --priority 0 --max-concurrency 10 --max-errors 5 \
 --name "My-Step-Functions-Task" \
 --description "A description for my Step Functions task"

```

## Windows

```

aws ssm update-maintenance-window-task ^
 --window-id "mw-0c50858d01EXAMPLE" ^
 --window-task-id "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE" ^
 --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" ^
 --task-arn "arn:aws:states:region:execution:SSMStepFunctionTest" ^

```



```
--service-role-arn "arn:aws:iam:account-id:role/MaintenanceWindowsRole" ^
--task-invocation-parameters '{"StepFunctions":{"Input":{"\"InstanceId\":
\"{{RESOURCE_ID}}\"}}}' ^
--priority 0 --max-concurrency 10 --max-errors 5 ^
--name "My-Step-Functions-Task" ^
--description "A description for my Step Functions task"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
 "Targets": [
 {
 "Key": "WindowTargetIds",
 "Values": [
 "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
]
 }
],
 "TaskArn": "arn:aws:states:us-east-2:111122223333:execution:SSMStepFunctionTest",
 "ServiceRoleArn": "arn:aws:iam::111122223333:role/MaintenanceWindowsRole",
 "TaskParameters": {},
 "TaskInvocationParameters": {
 "StepFunctions": {
 "Input": "{\"InstanceId\": \"{{RESOURCE_ID}}\"}"
 }
 },
 "Priority": 0,
 "MaxConcurrency": "10",
 "MaxErrors": "5",
 "Name": "My-Step-Functions-Task",
 "Description": "A description for my Step Functions task"
}
```

7. Eseguire il comando seguente per annullare la registrazione di una destinazione da una finestra di manutenzione. Questo esempio utilizza il parametro `safe` per determinare se la destinazione è referenziata da una qualsiasi e quindi se l'annullamento della registrazione è sicuro.

## Linux & macOS

```
aws ssm deregister-target-from-maintenance-window \
 --window-id "mw-0c50858d01EXAMPLE" \
 --window-target-id "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" \
 --safe
```

## Windows

```
aws ssm deregister-target-from-maintenance-window ^
 --window-id "mw-0c50858d01EXAMPLE" ^
 --window-target-id "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" ^
 --safe
```

Questo sistema restituisce informazioni simili alle seguenti.

```
An error occurred (TargetInUseException) when calling the
DeregisterTargetFromMaintenanceWindow operation:
This Target cannot be deregistered because it is still referenced in Task:
4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE
```

8. Eseguire il comando seguente per annullare la registrazione di una destinazione da una finestra di manutenzione anche se la destinazione è referenziata da un'attività. È possibile forzare l'operazione di annullamento della registrazione utilizzando il parametro `no-safe`.

## Linux & macOS

```
aws ssm deregister-target-from-maintenance-window \
 --window-id "mw-0c50858d01EXAMPLE" \
 --window-target-id "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" \
 --no-safe
```

## Windows

```
aws ssm deregister-target-from-maintenance-window ^
 --window-id "mw-0c50858d01EXAMPLE" ^
 --window-target-id "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" ^
 --no-safe
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowTargetId": "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
}
```

9. Esegui il seguente comando per aggiornare un task Run Command. Questo esempio utilizza un parametro Parameter Store Systems Manager denominato `UpdateLevel`, formattato nel seguente modo: `'{{ssm:UpdateLevel}}'`

### Linux & macOS

```
aws ssm update-maintenance-window-task \
 --window-id "mw-0c50858d01EXAMPLE" \
 --window-task-id "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE" \
 --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE" \
 --task-invocation-parameters "RunCommand={Comment=A comment for my task
 update,Parameters={UpdateLevel='{{ssm:UpdateLevel}}'}}
```

### Windows

```
aws ssm update-maintenance-window-task ^
 --window-id "mw-0c50858d01EXAMPLE" ^
 --window-task-id "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE" ^
 --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE" ^
 --task-invocation-parameters "RunCommand={Comment=A comment for my task
 update,Parameters={UpdateLevel='{{ssm:UpdateLevel}}'}}
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
 "i-02573cafcfEXAMPLE"
]
 }
]
}
```

```

]
 }
],
"TaskArn": "AWS-RunShellScript",
"ServiceRoleArn": "arn:aws:iam::111122223333:role/
MyMaintenanceWindowServiceRole",
"TaskParameters": {},
"TaskInvocationParameters": {
 "RunCommand": {
 "Comment": "A comment for my task update",
 "Parameters": {
 "UpdateLevel": [
 "{{ssm:UpdateLevel}}"
]
 }
 }
},
"Priority": 10,
"MaxConcurrency": "1",
"MaxErrors": "1"
}

```

10. Eseguire questo comando per aggiornare un'attività di automazione per specificare i parametri WINDOW\_ID e WINDOW\_TASK\_ID per il parametro task-invocation-parameters:

### Linux & macOS

```

aws ssm update-maintenance-window-task \
 --window-id "mw-0c50858d01EXAMPLE" \
 --window-task-id "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE" \
 --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" \
 --task-arn "AutoTestDoc" \
 --service-role-arn "arn:aws:iam:account-id:role/
MyMaintenanceWindowServiceRole \
 --task-invocation-parameters
 "Automation={Parameters={InstanceId='{{RESOURCE_ID}}',initiator='{{WINDOW_ID}}.Task-
{{WINDOW_TASK_ID}}'}}" \
 --priority 3 --max-concurrency 10 --max-errors 5

```

### Windows

```

aws ssm update-maintenance-window-task ^
 --window-id "mw-0c50858d01EXAMPLE" ^

```

```
--window-task-id "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE" ^
--targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" ^
--task-arn "AutoTestDoc" ^
--service-role-arn "arn:aws:iam:account-id:role/
MyMaintenanceWindowServiceRole ^
--task-invocation-parameters
"Automation={Parameters={InstanceId='{{RESOURCE_ID}}',initiator='{{WINDOW_ID}}.Task-
{{WINDOW_TASK_ID}}'}}" ^
--priority 3 --max-concurrency 10 --max-errors 5
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowId": "mw-0c50858d01EXAMPLE",
 "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
 "Targets": [
 {
 "Key": "WindowTargetIds",
 "Values": [
 "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
]
 }
],
 "TaskArn": "AutoTestDoc",
 "ServiceRoleArn": "arn:aws:iam::111122223333:role/
MyMaintenanceWindowServiceRole",
 "TaskParameters": {},
 "TaskInvocationParameters": {
 "Automation": {
 "Parameters": {
 "multi": [
 "{{WINDOW_TASK_ID}}"
],
 "single": [
 "{{WINDOW_ID}}"
]
 }
 }
 },
 "Priority": 0,
 "MaxConcurrency": "10",
 "MaxErrors": "5",
```

```
"Name": "My-Automation-Task",
"Description": "A description for my Automation task"
}
```

Tutorial: Eliminare una finestra di manutenzione utilizzando il AWS CLI

Per eliminare una finestra di manutenzione creata in queste esercitazioni, eseguire il seguente comando.

```
aws ssm delete-maintenance-window --window-id "mw-0c50858d01EXAMPLE"
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "WindowId": "mw-0c50858d01EXAMPLE"
}
```

Tutorial: creazione di una finestra di manutenzione per l'applicazione di patch tramite console

#### Important

Puoi continuare a usare questo argomento legacy per creare una finestra di manutenzione per l'applicazione di patch. Consigliamo, tuttavia, di utilizzare una policy di patch. Per ulteriori informazioni, consulta [Configurazioni delle policy sulle patch in Configurazione rapida](#) e [Configurare l'applicazione di patch per le istanze in un'organizzazione utilizzando un Configurazione rapida politica sulle patch](#).

Per ridurre al minimo l'impatto sulla disponibilità dei server, ti consigliamo di configurare una finestra di manutenzione per eseguire l'applicazione di patch in orari che non interrompano le attività aziendali.

Prima di iniziare questa procedura, dovrai configurare i ruoli e le autorizzazioni per la Maintenance Windows. Per ulteriori informazioni, consulta [Configurazione Intervallo di manutenzione](#).

Per creare una finestra di manutenzione per l'applicazione di patch

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.

2. Nel pannello di navigazione, scegli Maintenance Windows.
3. Scegli Crea finestra di manutenzione.
4. Nel campo Nome, immetti un nome che lo indichi come una finestra di manutenzione per l'applicazione di aggiornamenti critici e importanti.
5. (Facoltativo) In Descrizione, immetti una descrizione.
6. Scegli Consenti destinazioni non registrate per consentire a un'attività di una finestra di manutenzione di essere eseguita su nodi gestiti, anche se tali nodi non sono stati registrati come destinazioni.

Se si sceglie questa opzione, è possibile scegliere i nodi non registrati (per ID nodo) quando si registra un'attività sulla finestra di manutenzione.

Se non si sceglie questa opzione, è necessario scegliere destinazioni precedentemente registrate quando si registra un'attività sulla finestra di manutenzione.

7. Nella parte superiore della sezione Pianificazione, specifica una pianificazione per la finestra di manutenzione tramite una delle tre opzioni di pianificazione.

Per informazioni sulla creazione di cron/rate espressioni, vedere [Riferimento: espressioni Cron e della frequenza per Systems Manager](#).

8. Per Durata, inserisci il numero di ore di esecuzione della finestra di manutenzione. Il valore specificato determina l'ora di fine specifica per la finestra di manutenzione in base all'ora di inizio. Nessuna attività della finestra di manutenzione può essere avviata dopo l'ora di fine risultante meno il numero di ore specificato per Arresta l'inizializzazione di attività nella fase successiva.

Ad esempio, se la finestra di manutenzione inizia alle 15:00, la durata è di tre ore e il valore Arresta l'inizializzazione di attività è un'ora, nessuna attività della finestra di manutenzione può iniziare dopo le 17:00.

9. In Stop initiating tasks (Interrompi l'avvio delle attività), inserire il numero di ore prima del termine della finestra di manutenzione a partire dalle quali il sistema deve interrompere la pianificazione dell'esecuzione di nuove attività.
10. (Facoltativo) Per la data di inizio della finestra, specificate una data e un'ora, in formato ISO-8601 esteso, per quando desiderate che la finestra di manutenzione diventi attiva. Ciò consente di ritardare l'attivazione della finestra di manutenzione fino alla data futura specificata.
11. (Facoltativo) Per la data di fine della finestra, specifica una data e un'ora, in formato ISO-8601 esteso, per quando desideri che la finestra di manutenzione diventi inattiva. Ciò consente di

impostare una data e un'ora future dopo le quali la finestra di manutenzione non verrà più eseguita.

12. (Facoltativo) In Pianificazione fuso orario, specifica il fuso orario su cui deve essere basata la pianificazione delle esecuzioni della finestra di manutenzione, nel formato IANA (Internet Assigned Numbers Authority). Ad esempio: "America/Los\_Angeles», "etc/UTC«, o "Asia/Seoul».

Per ulteriori informazioni sui formati validi, consulta il [Database dei fusi orari](#) sul sito web IANA.

13. (Facoltativo) Nell'area Gestisci i tag, applica una o più name/value coppie di chiavi di tag alla finestra di manutenzione.

I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Ad esempio, è possibile applicare un tag a questa finestra di manutenzione per identificare il tipo di attività eseguito. In questo caso, puoi specificare la seguente name/value coppia di chiavi:

- Key=TaskType, Value=Patching

14. Scegli Crea finestra di manutenzione.
15. Nell'elenco delle finestre di manutenzione, scegli la finestra di manutenzione appena creata, quindi scegli Operazioni, Registra destinazioni.
16. (Facoltativo) Nella sezione Dettagli della finestra di manutenzione di destinazione, specifica il nome, la descrizione e le informazioni sul proprietario (il proprio nome o alias) per la destinazione.
17. In Selezione della destinazione, scegli Specifica tag delle istanze.
18. In Specifica tag delle istanze, immetti una chiave e un valore di tag per identificare i nodi da registrare nella finestra di manutenzione, quindi scegli Aggiungi.
19. Scegli Registra destinazione. Il sistema crea una finestra di manutenzione di destinazione.
20. Nella pagina dei dettagli della finestra di manutenzione creata, scegli Operazioni, Registra attività di esecuzione comandi.
21. (Facoltativo) In Dettagli attività finestra di manutenzione fornisci il nome e la descrizione dell'attività.
22. Per Documento comando, scegli AWS-RunPatchBaseline.
23. Per Priorità attività, scegli una priorità. Zero (0) indica la priorità più elevata.
24. In Destinazioni, sotto Destinazione di, scegli la finestra di manutenzione di destinazione creata precedentemente in questa procedura.
25. In Controllo velocità:



- In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti presi di mira, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.
26. (Facoltativo) Per il Ruolo di servizio IAM, scegli un ruolo affinché Systems Manager conceda le autorizzazioni durante l'esecuzione di attività della finestra di manutenzione.

Se non specifichi un ARN del ruolo di servizio, Systems Manager utilizza un ruolo collegato al servizio nell'account. Se nell'account non esiste un ruolo collegato al servizio appropriato per Systems Manager, questo viene creato quando l'attività viene registrata correttamente.

 Note

Per migliorare il livello di sicurezza, consigliamo vivamente di creare una policy personalizzata e un ruolo di servizio personalizzato per l'esecuzione delle attività della finestra di manutenzione. C'è la possibilità di creare la policy per fornire solo le autorizzazioni necessarie per le specifiche attività della finestra di manutenzione. Per ulteriori informazioni, consulta [Configurazione Intervallo di manutenzione](#).

27. (Facoltativo) In Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Abilita scrittura in S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

 Note

Le autorizzazioni S3 che consentono di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza assegnate al nodo gestito e non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle](#)

[autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova in un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato all'istanza disponga delle autorizzazioni necessarie per scrivere su quel bucket.

Per trasmettere l'output a un gruppo di CloudWatch log di Amazon Logs, seleziona la CloudWatch casella di output. Inserisci il nome del gruppo di log nella casella.

28. Nella sezione SNS notifications (Notifiche SNS), se si desidera che vengano inviate notifiche sullo stato di esecuzione del comando, selezionare la casella di controllo Enable SNS notifications (Abilita notifiche SNS).

Per ulteriori informazioni sulla configurazione delle notifiche Amazon SNS per Run Command, consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

29. In Parametri:

- Nell'elenco Operazione, scegli Scansiona per cercare le patch mancanti oppure Installa per cercare e installare le patch mancanti.
- Non è necessario specificare nulla nel campo Snapshot Id (ID snapshot). Questo sistema genera e fornisce automaticamente questo parametro.
- Non è necessario specificare nulla nel campo Installa elenco sostituzioni, a meno che non si desideri che Patch Manager utilizzi un set di patch diverso da quello specificato per la baseline delle patch. Per informazioni, consulta [Nome parametro: InstallOverrideList](#).
- Per RebootOption, specifica se desideri che i nodi si riavviino se le patch vengono installate durante l'Installazione o se Patch Manager rileva altre patch installate dopo il riavvio dell'ultimo nodo. Per informazioni, consulta [Nome parametro: RebootOption](#).
- (Facoltativo) In Comment (Commento) immettere una nota di tracciamento o un promemoria su questo comando.
- Nella casella Timeout (seconds) (Timeout (secondi)) immettere il numero di secondi che devono trascorrere per il completamento dell'operazione prima che il sistema la consideri come non andata a buon fine.

30. Scegliere Register Run command task (Registra attività di esecuzione comandi).

Al termine dell'attività della finestra di manutenzione, è possibile visualizzare i dettagli di conformità delle patch nella console di Systems Manager nello strumento [Fleet Manager](#).

È inoltre possibile visualizzare le informazioni sulla conformità nello strumento [Patch Manager](#), nella scheda Creazione di rapporti sulla conformità.

Puoi anche utilizzare le [DescribeInstancePatchStatesForPatchGroup](#) API [DescribePatchGroupState](#) and per visualizzare i dettagli sulla conformità. Per informazioni sui dati di conformità delle patch, consulta [Informazioni sulla conformità delle patch](#).

## Piani di applicazione di patch con le finestre di manutenzione

Dopo avere configurato una baseline delle patch, ed eventualmente un gruppo di patch, è possibile applicare le patch al nodo utilizzando una finestra di manutenzione. Una finestra di manutenzione può ridurre l'impatto sulla disponibilità del server consentendoti di specificare un'ora per l'applicazione di patch che non interrompa le operazioni aziendali. Una finestra di manutenzione funziona in questo modo:

1. Creare una finestra di manutenzione con una pianificazione per le operazioni di applicazione di patch.
2. Scegli gli obiettivi per la finestra di manutenzione specificando il PatchGroup tag Patch Group o per il nome del tag e qualsiasi valore per il quale hai definito i tag Amazon Elastic Compute Cloud (Amazon EC2), ad esempio «server web» o ". US-EAST-PROD Se sono presenti [tag consentiti nei metadati dell'istanza EC2](#), è necessario utilizzare PatchGroup (senza spazio).
3. Creare una nuova attività della finestra di manutenzione task e specificare il documento AWS-RunPatchBaseline.

Quando configuri l'attività, è possibile scegliere di effettuare la scansione del nodo o di effettuare la scansione e installare le patch nei nodi. Se scegli di effettuare la scansione dei nodi, Patch Manager, uno strumento di AWS Systems Manager, effettua la scansione di ciascun nodo e genera un elenco delle patch mancanti da verificare.

Se scegli di effettuare la scansione e installare le patch, Patch Manager effettua la scansione di ogni nodo e confronta l'elenco delle patch installate a fronte di quello delle patch approvate nella baseline. Patch Manager identifica le patch mancanti, quindi scarica e installa tutte le patch approvate e mancanti.

Per eseguire un'unica scansione o installazione per risolvere un problema, è possibile utilizzare Run Command per chiamare direttamente il documento AWS-RunPatchBaseline.

 Important

Dopo l'installazione delle patch, Systems Manager riavvia ciascuna nodo. Il riavvio è necessario per garantire che le patch siano installate correttamente e per assicurarsi che il sistema non abbia lasciato il nodo in uno stato potenzialmente negativo. (Eccezione: se il parametro `RebootOption` è impostato su `NoReboot` nel documento `AWS-RunPatchBaseline`, il nodo non viene riavviato dopo l'esecuzione di Patch Manager. Per ulteriori informazioni, consulta [Nome parametro: RebootOption](#).)

## Utilizzo degli pseudo parametri durante la registrazione delle attività della finestra di manutenzione

Quando si registra un'attività in `Maintenance Windows`, si specificano i parametri univoci per ciascuno dei quattro tipi di attività. (Nei comandi CLI, questi vengono forniti utilizzando l'opzione `--task-invocation-parameters`.)

Puoi anche fare riferimento a determinati valori utilizzando la sintassi degli pseudoparametri, ad esempio `{{RESOURCE_ID}}`, `{{TARGET_TYPE}}` e `{{WINDOW_TARGET_ID}}`. Quando viene eseguita, l'operazione della finestra di manutenzione trasmette i valori corretti invece dei segnaposto degli pseudoparametri. L'elenco completo degli pseudo parametri che è possibile utilizzare è fornito di seguito in questo argomento in [Pseudoparametri supportati](#).

 Important

Per il tipo di destinazione `RESOURCE_GROUP`, a seconda del formato ID necessario per l'attività, è possibile scegliere tra utilizzare `{{TARGET_ID}}` e `{{RESOURCE_ID}}` e fare riferimento alla risorsa quando viene eseguita l'attività. `{{TARGET_ID}}` restituisce l'ARN completo della risorsa. `{{RESOURCE_ID}}` restituisce solo un nome o un ID più breve della risorsa, come mostrato in questi esempi.

- `{{TARGET_ID}}` format: `arn:aws:ec2:us-east-1:123456789012:instance/i-02573cafcfEXAMPLE`
- `{{RESOURCE_ID}}` format: `i-02573cafcfEXAMPLE`

Per il tipo di destinazione INSTANCE, i parametri sia `{{TARGET_ID}}` sia `{{RESOURCE_ID}}` restituiscono solo l'ID istanza. Per ulteriori informazioni, consulta [Pseudoparametri supportati](#). `{{TARGET_ID}}` e `{{RESOURCE_ID}}` può essere utilizzato per passare gli ID delle AWS risorse solo alle attività di Automation, Lambda e Step Functions. Questi due pseudo parametri non possono essere usati con attività Run Command.

## Esempi di pseudoparametri

Supponiamo che il payload per un' AWS Lambda attività debba fare riferimento a un'istanza tramite il relativo ID.

Sia che si utilizzi una destinazione della finestra di manutenzione INSTANCE o RESOURCE\_GROUP, è possibile ottenere questo risultato utilizzando lo pseudoparametro `{{RESOURCE_ID}}`. Ad esempio:

```
"TaskArn": "arn:aws:lambda:us-east-2:111122223333:function:SSMTestFunction",
"TaskType": "LAMBDA",
"TaskInvocationParameters": {
 "Lambda": {
 "ClientContext": "ew0KICAi--truncated--0KIEXAMPLE",
 "Payload": "{ \"instanceId\": \"{{RESOURCE_ID}}\" }",
 "Qualifier": "$LATEST"
 }
}
```

Se l'attività Lambda è destinata a essere eseguita su un altro tipo di destinazione supportato oltre alle istanze Amazon Elastic Compute Cloud (Amazon EC2), ad esempio una tabella Amazon DynamoDB, è possibile utilizzare la stessa sintassi e `{{RESOURCE_ID}}` restituisce solo il nome della tabella. Tuttavia, se si richiede l'ARN completo della tabella, utilizzare `{{TARGET_ID}}`, come illustrato nell'esempio seguente.

```
"TaskArn": "arn:aws:lambda:us-east-2:111122223333:function:SSMTestFunction",
"TaskType": "LAMBDA",
"TaskInvocationParameters": {
 "Lambda": {
 "ClientContext": "ew0KICAi--truncated--0KIEXAMPLE",
 "Payload": "{ \"tableArn\": \"{{TARGET_ID}}\" }",
 }
}
```

```
 "Qualifier": "$LATEST"
 }
}
```

La stessa sintassi funziona per il targeting di istanze o altri tipi di risorse. Quando più tipi di risorse sono stati aggiunti a un gruppo di risorse, l'attività viene eseguita su ciascuna delle risorse appropriate.

 Important

Non tutti i tipi di risorse che potrebbero essere inclusi in un gruppo di risorse producono un valore per il parametro `{{RESOURCE_ID}}`. Per un elenco dei tipi di risorse supportati, vedere [Pseudoparametri supportati](#).

A titolo di esempio aggiuntivo, per eseguire un task di automazione che interrompa l'esecuzione delle istanze EC2, devi specificare il documento di Systems Manager `AWS-StopEC2Instance` (documento SSM) come valore `TaskArn` e utilizzare lo pseudoparametro `{{RESOURCE_ID}}`:

```
"TaskArn": "AWS-StopEC2Instance",
"TaskType": "AUTOMATION"
"TaskInvocationParameters": {
 "Automation": {
 "DocumentVersion": "1",
 "Parameters": {
 "instanceId": [
 "{{RESOURCE_ID}}"
]
 }
 }
}
```

Per eseguire un'attività di automazione che copia uno snapshot di un volume Amazon Elastic Block Store (Amazon EBS), specificare il documento SSM `AWS-CopySnapshot` come valore `TaskArn` e utilizzare lo pseudoparametro `{{RESOURCE_ID}}`.

```
"TaskArn": "AWS-CopySnapshot",
"TaskType": "AUTOMATION"
"TaskInvocationParameters": {
 "Automation": {
```

```

 "DocumentVersion": "1",
 "Parameters": {
 "SourceRegion": "us-east-2",
 "targetType": "RESOURCE_GROUP",
 "SnapshotId": [
 "{{RESOURCE_ID}}"
]
 }
 }
}

```

## Pseudoparametri supportati

Nell'elenco seguente sono riportati gli pseudoparametri che puoi specificare utilizzando la sintassi `{{PSEUDO_PARAMETER}}` nell'opzione `--task-invocation-parameters`.

- **WINDOW\_ID**: ID della finestra di manutenzione di destinazione.
- **WINDOW\_TASK\_ID**: l'ID dell'attività della finestra che è in esecuzione.
- **WINDOW\_TARGET\_ID**: l'ID della destinazione della finestra che include la destinazione (ID destinazione).
- **WINDOW\_EXECUTION\_ID**: l'ID dell'esecuzione della finestra corrente.
- **TASK\_EXECUTION\_ID**: l'ID dell'esecuzione dell'attività corrente.
- **INVOCATION\_ID**: l'ID dell'invocazione corrente.
- **TARGET\_TYPE**: il tipo di destinazione. I tipi supportati includono RESOURCE\_GROUP e INSTANCE.
- **TARGET\_ID**:

Se il tipo di destinazione specificato è INSTANCE, lo pseudoparametro TARGET\_ID viene sostituito dall'ID dell'istanza. Ad esempio, `i-078a280217EXAMPLE`.

Se il tipo di destinazione specificato è RESOURCE\_GROUP, il valore a cui si fa riferimento per l'esecuzione dell'attività è l'ARN completo della risorsa. Ad esempio: `arn:aws:ec2:us-east-1:123456789012:instance/i-078a280217EXAMPLE`. Nella tabella seguente sono riportati i valori TARGET\_ID di esempio per particolari tipi di risorse in un gruppo di risorse.

### Note

TARGET\_ID non è supportato per le attività Run Command.

| Tipo di risorsa          | Esempio TARGET_ID                                                                     |  |
|--------------------------|---------------------------------------------------------------------------------------|--|
| AWS::CloudWatch::Alarm   | arn:aws:cloudwatch:us-east-1:123456789012:alarm:MyCloudWatchAlarm i-078a280217EXAMPLE |  |
| AWS::DynamoDB::Table     | arn:aws:dynamodb:us-east-1:123456789012:table/MyTable                                 |  |
| AWS::EC2::Instance       | arn:aws:ec2:us-east-1:123456789012:instance/ i-078a280217EXAMPLE                      |  |
| AWS::EC2::Image          | arn:aws:ec2:us-east-1:123456789012:image/ami-02250b3732EXAMPLE                        |  |
| AWS::EC2::Security Group | arn:aws:ec2:us-east-1:123456789012:security-group/sg-cEXAMPLE                         |  |
| AWS::EC2::Snapshot       | arn:aws:ec2:us-east-1:123456789012:snapshot/snap-03866bf003EXAMPLE                    |  |
| AWS::EC2::Volume         | arn:aws:ec2:us-east-1:123456789012:volume/vol-0912e04d78EXAMPLE                       |  |



| Tipo di risorsa           | Esempio TARGET_ID                                                                      |  |
|---------------------------|----------------------------------------------------------------------------------------|--|
| AWS::ECS::Service         | arn:aws:ecs:us-east-1:123456789012:service/my-ecs-service                              |  |
| AWS::RDS::DBCluster       | arn:aws:rds:us-east-2:123456789012:cluster:My-Cluster                                  |  |
| AWS::RDS::DBInstance      | arn:aws:rds:us-east-1:123456789012:db:My-SQL-Instance                                  |  |
| AWS::S3::Bucket           | arn:aws:s3:::amzn-s3-demo-bucket                                                       |  |
| AWS::SSM::ManagedInstance | arn:aws:ssm:us-east-1:123456789012:managed-instance/managed-instance-0feadcf2d9EXAMPLE |  |

- **RESOURCE\_ID:** ID breve di un tipo di risorsa contenuto in un gruppo di risorse. Nella tabella seguente sono riportati i valori RESOURCE\_ID di esempio per particolari tipi di risorse in un gruppo di risorse.

 Note

RESOURCE\_ID non è supportato per le attività Run Command.

| Tipo di risorsa        | Esempio RESOURCE_ID |  |
|------------------------|---------------------|--|
| AWS::CloudWatch::Alarm | MyCloudWatchAlarm   |  |
| AWS::DynamoDB::Table   | MyTable             |  |

| Tipo di risorsa           | Esempio RESOURCE_ID    |  |
|---------------------------|------------------------|--|
| AWS::EC2::Instance        | i-078a280217EXAMPLE    |  |
| AWS::EC2::Image           | ami-02250b3732EXAMPLE  |  |
| AWS::EC2::Security Group  | sg-cEXAMPLE            |  |
| AWS::EC2::Snapshot        | snap-03866bf003EXAMPLE |  |
| AWS::EC2::Volume          | vol-0912e04d78EXAMPLE  |  |
| AWS::ECS::Service         | my-ecs-service         |  |
| AWS::RDS::DBCluster       | My-Cluster             |  |
| AWS::RDS::DBInstance      | My-SQL-Instance        |  |
| AWS::S3::Bucket           | amzn-s3-demo-bucket    |  |
| AWS::SSM::ManagedInstance | mi-0feadcf2d9EXAMPLE   |  |

#### Note

Se il gruppo di AWS risorse specificato include tipi di risorse che non generano un RESOURCE\_ID valore e non sono elencati nella tabella precedente, il RESOURCE\_ID parametro non viene compilato. Una chiamata di esecuzione verrà comunque eseguita per tale risorsa. In questi casi, utilizzare invece lo pseudo parametro TARGET\_ID, che verrà sostituito con l'ARN completo della risorsa.

## Opzioni di pianificazione e periodo attivo per la finestra di manutenzione

Quando si crea una finestra di manutenzione, è necessario specificare la frequenza con la quale viene eseguita utilizzando un'[espressione Cron o della frequenza](#). Facoltativamente, puoi specificare un intervallo di date durante il quale la finestra di manutenzione può essere eseguita in base alla pianificazione periodica, nonché un fuso orario sul quale basare la pianificazione periodica.

Tieni tuttavia presente che l'opzione relativa al fuso orario e le opzioni relative a data di inizio e fine non si influenzano a vicenda. Qualsiasi data/ora di inizio e fine specificata (con o senza un offset per il fuso orario) determina solo il periodo di validità durante il quale la finestra di manutenzione può essere eseguita in base alla pianificazione. Un'opzione relativa al fuso orario determina il fuso orario internazionale sul quale è basata la pianificazione per la finestra di manutenzione durante il suo periodo di validità.

### Note

È possibile specificare le date di inizio e fine in formato ISO-8601 timestamp. Ad esempio:

`2021-04-07T14:29:00-08:00`

I fusi orari devono essere specificati nel formato IANA (Internet Assigned Numbers Authority).

Ad esempio: America/Chicago, Europe/Berlin o Asia/Tokyo

### Esempi

- [Esempio 1: specificare la data di inizio di una finestra di manutenzione](#)
- [Esempio 2: specificare una data di inizio e fine di una finestra di manutenzione](#)
- [Esempio 3: creare una finestra di manutenzione che viene eseguita solo una volta](#)
- [Esempio 4: specificare il numero di giorni di offset di pianificazione per una finestra di manutenzione](#)

### Esempio 1: specificare la data di inizio di una finestra di manutenzione

Supponiamo di utilizzare AWS Command Line Interface (AWS CLI) per creare una finestra di manutenzione con le seguenti opzioni:

- `--start-date 2021-01-01T00:00:00-08:00`
- `--schedule-timezone "America/Los_Angeles"`

- `--schedule "cron(0 09 ? * WED *)"`

Esempio:

## Linux & macOS

```
aws ssm create-maintenance-window \
 --name "My-LAX-Maintenance-Window" \
 --allow-unassociated-targets \
 --duration 3 \
 --cutoff 1 \
 --start-date 2021-01-01T00:00:00-08:00 \
 --schedule-timezone "America/Los_Angeles" \
 --schedule "cron(0 09 ? * WED *)"
```

## Windows

```
aws ssm create-maintenance-window ^
 --name "My-LAX-Maintenance-Window" ^
 --allow-unassociated-targets ^
 --duration 3 ^
 --cutoff 1 ^
 --start-date 2021-01-01T00:00:00-08:00 ^
 --schedule-timezone "America/Los_Angeles" ^
 --schedule "cron(0 09 ? * WED *)"
```

In questo caso, il primo utilizzo della finestra di manutenzione si verificherà solo dopo la data e l'ora di inizio specificate, che corrispondono alle 12:00 (fuso orario Stati Uniti/Pacifico) di venerdì 1° gennaio 2021, ovvero otto ore indietro rispetto all'orario UTC. In questo caso, la data e l'ora di inizio del periodo della finestra non rappresentano la prima esecuzione delle finestre di manutenzione. Nel loro insieme, i `--schedule` valori `--schedule-timezone` and indicano che la finestra di manutenzione viene aperta alle 9:00 di ogni mercoledì nel fuso orario degli Stati Uniti del Pacifico (rappresentato da "America/Los Angeles» in formato IANA). La prima esecuzione nel periodo consentito avverrà mercoledì 4 gennaio 2021, alle 9:00 (fuso orario Stati Uniti/Pacifico).

Esempio 2: specificare una data di inizio e fine di una finestra di manutenzione

Supponiamo che in seguito si crei una finestra di manutenzione con queste opzioni:

- `--start-date 2019-01-01T00:03:15+09:00`

- `--end-date 2019-06-30T00:06:15+09:00`
- `--schedule-timezone "Asia/Tokyo"`
- `--schedule "rate(7 days)"`

Ad esempio:

## Linux & macOS

```
aws ssm create-maintenance-window \
 --name "My-NRT-Maintenance-Window" \
 --allow-unassociated-targets \
 --duration 3 \
 --cutoff 1 \
 --start-date 2019-01-01T00:03:15+09:00 \
 --end-date 2019-06-30T00:06:15+09:00 \
 --schedule-timezone "Asia/Tokyo" \
 --schedule "rate(7 days)"
```

## Windows

```
aws ssm create-maintenance-window ^
 --name "My-NRT-Maintenance-Window" ^
 --allow-unassociated-targets ^
 --duration 3 ^
 --cutoff 1 ^
 --start-date 2019-01-01T00:03:15+09:00 ^
 --end-date 2019-06-30T00:06:15+09:00 ^
 --schedule-timezone "Asia/Tokyo" ^
 --schedule "rate(7 days)"
```

Il periodo consentito per questa finestra di manutenzione inizia alle 03:15 del 1° gennaio 2019, nel fuso orario standard del Giappone. Il periodo valido per questa finestra di manutenzione termina alle 06:15 di domenica 30 giugno 2019, nel fuso orario standard del Giappone. ovvero nove ore in avanti rispetto all'ora UTC. Nel loro insieme, i `--schedule` valori `--schedule-timezone` and indicano che la finestra di manutenzione viene aperta alle 3:15 di martedì nel fuso orario standard del Giappone (rappresentato da "Asia/Tokyo" in formato IANA). Ciò è dovuto al fatto che la finestra di manutenzione viene eseguita ogni sette giorni e diventa attiva alle 03:15 di martedì 1° gennaio. L'ultima esecuzione sarà alle 03:15 del 25 giugno 2019, nel fuso orario standard del Giappone.

Questo è l'ultimo martedì prima che il periodo della finestra di manutenzione consentita termini cinque giorni più tardi.

Esempio 3: creare una finestra di manutenzione che viene eseguita solo una volta

Ora è possibile creare una finestra di manutenzione con questa opzione:

- `--schedule "at(2020-07-07T15:55:00)"`

Ad esempio:

Linux & macOS

```
aws ssm create-maintenance-window \
 --name "My-One-Time-Maintenance-Window" \
 --schedule "at(2020-07-07T15:55:00)" \
 --duration 5 \
 --cutoff 2 \
 --allow-unassociated-targets
```

Windows

```
aws ssm create-maintenance-window ^
 --name "My-One-Time-Maintenance-Window" ^
 --schedule "at(2020-07-07T15:55:00)" ^
 --duration 5 ^
 --cutoff 2 ^
 --allow-unassociated-targets
```

Questa finestra di manutenzione viene eseguita solo una volta, alle ore 15:55 UTC del 7 luglio 2020. La finestra di manutenzione è abilitata per essere eseguita fino a cinque ore, a seconda delle esigenze, ma le nuove attività non possono iniziare due ore prima della fine del periodo di finestra di manutenzione.

Esempio 4: specificare il numero di giorni di offset di pianificazione per una finestra di manutenzione

Ora è possibile creare una finestra di manutenzione con questa opzione:

```
--schedule-offset 2
```

Ad esempio:

## Linux & macOS

```
aws ssm create-maintenance-window \
 --name "My-Cron-Offset-Maintenance-Window" \
 --schedule "cron(0 30 23 ? * TUE#3 *)" \
 --duration 4 \
 --cutoff 1 \
 --schedule-offset 2 \
 --allow-unassociated-targets
```

## Windows

```
aws ssm create-maintenance-window ^
 --name "My-Cron-Offset-Maintenance-Window" ^
 --schedule "cron(0 30 23 ? * TUE#3 *)" ^
 --duration 4 ^
 --cutoff 1 ^
 --schedule-offset 2 ^
 --allow-unassociated-targets
```

Un offset di pianificazione è il numero di giorni di attesa dopo la data e l'ora specificate da un'espressione CRON per l'avvio dell'esecuzione della finestra di manutenzione.

Nell'esempio precedente, l'espressione CRON pianifica l'esecuzione di una finestra di manutenzione il terzo martedì di ogni mese alle 23:30:

```
--schedule "cron(0 30 23 ? * TUE#3 *)"
```

Tuttavia, includendo `--schedule-offset 2`, la finestra di manutenzione verrà eseguita due giorni dopo il terzo martedì di ogni mese alle 23:30.

Gli offset di pianificazione sono supportati solo per le espressioni CRON.

## Ulteriori informazioni

- [Riferimento: espressioni Cron e della frequenza per Systems Manager](#)
- [Creare una finestra di manutenzione utilizzando la console](#)
- [Tutorial: Creare e configurare una finestra di manutenzione utilizzando il AWS CLI](#)

- [CreateMaintenanceWindow](#) nel Documentazione di riferimento API di AWS Systems Manager
- [create-maintenance-window](#) nella AWS Systems Manager sezione del AWS CLI Command Reference
- [Time Zone Database](#) sul sito Web IANA

## Registrazione delle attività della finestra di manutenzione senza destinazioni

Per ogni finestra di manutenzione creata, è possibile specificare uno o più task da eseguire quando viene eseguita la finestra di manutenzione. Nella maggior parte dei casi, è necessario specificare le risorse o le destinazioni su cui eseguire l'attività. In alcuni casi, tuttavia, non devi specificare le destinazioni in modo esplicito nell'attività.

È necessario specificare uno o più oggetti per le attività di tipo Run Command di Systems Manager della finestra di manutenzione. A seconda della natura dell'attività, gli obiettivi sono facoltativi per altri tipi di attività della finestra di manutenzione (Systems Manager Automation e AWS Step Functions).  
AWS Lambda

Per i tipi di attività Lambda e Step Functions, se è necessaria una destinazione dipende dal contenuto della funzione o della macchina creati.

### Note

Quando un'attività ha obiettivi registrati AWS Lambda, Automation e AWS Step Functions Tasks risolvono gli obiettivi dai gruppi di risorse e dai tag e inviano una chiamata per risorsa risolta, il che si traduce in più chiamate di attività. Ad esempio, supponiamo di volere una sola invocazione per un'attività Lambda registrata in un gruppo di risorse contenente più di un'istanza. In questo caso, se stai lavorando nella Console di gestione AWS, scegli l'opzione Target attività non richiesto nella pagina Registra attività Lambda o Modifica attività Lambda. Se si utilizza il AWS CLI comando, non specificare gli obiettivi utilizzando il `--targets` parametro durante l'esecuzione del comando o del [register-task-with-maintenance-window](#) comando. [update-maintenance-window-task](#)

In molti casi, non devi specificare esplicitamente una destinazione per un'attività di automazione. Ad esempio, supponiamo che stiate creando un' Automation-type attività per aggiornare un Amazon Machine Image (AMI) per Linux usando il AWS-UpdateLinuxAmi runbook. Quando l'attività viene eseguita, AMI viene aggiornato con gli ultimi pacchetti di distribuzione Linux disponibili e il software



Amazon. Nuove istanze create da AMI hanno già questi aggiornamenti installati. Perché l'ID dell'AMI da aggiornare è specificato nei parametri di input per il runbook, non è necessario specificare nuovamente una destinazione nel processo della finestra di manutenzione.

Allo stesso modo, supponiamo di utilizzare AWS Command Line Interface (AWS CLI) per registrare un'attività di automazione della finestra di manutenzione che utilizza il `AWS-RestartEC2Instance` runbook. Poiché il nodo da riavviare è specificato nell'argomento `--task-invocation-parameters`, non è necessario specificare anche un'opzione `--targets`.

#### Note

Per le attività della finestra di manutenzione senza una destinazione specificata, non è possibile fornire valori per `--max-errors` e `--max-concurrency`. Invece, il sistema inserisce un valore segnaposto pari a 1, che potrebbe essere segnalato nella risposta a comandi come [describe-maintenance-window-tasks](#) e [get-maintenance-window-task](#). Questi valori non influiscono sull'esecuzione di un'attività e possono essere ignorati.

L'esempio seguente mostra le omissioni delle opzioni `--targets`, `--max-errors` e `--max-concurrency` per un'attività di una finestra di manutenzione senza destinazione.

#### Linux & macOS

```
aws ssm register-task-with-maintenance-window \
 --window-id "mw-ab12cd34eEXAMPLE" \
 --service-role-arn "arn:aws:iam::123456789012:role/
MaintenanceWindowAndAutomationRole" \
 --task-type "AUTOMATION" \
 --name "RestartInstanceWithoutTarget" \
 --task-arn "AWS-RestartEC2Instance" \
 --task-invocation-parameters "{\"Automation\":{\"Parameters\":{\"InstanceId\":
[\"i-02573cafcfEXAMPLE\"]}}}" \
 --priority 10
```

#### Windows

```
aws ssm register-task-with-maintenance-window ^
 --window-id "mw-ab12cd34eEXAMPLE" ^
 --service-role-arn "arn:aws:iam::123456789012:role/
MaintenanceWindowAndAutomationRole" ^
 --task-type "AUTOMATION" ^
```

```
--name "RestartInstanceWithoutTarget" ^
--task-arn "AWS-RestartEC2Instance" ^
--task-invocation-parameters "{\"Automation\":{\"Parameters\":{\"InstanceId\":
[\"i-02573cafcfEXAMPLE\"]}}}" ^
--priority 10
```

### Note

Per le attività della finestra di manutenzione registrate prima del 23 dicembre 2020: se sono stati specificati obiettivi per l'attività e uno non è più necessario, è possibile aggiornare l'attività per rimuovere gli obiettivi utilizzando la console Systems Manager o il [update-maintenance-window-task](#) AWS CLI comando.

### Ulteriori informazioni

- [Messaggi di errore: «Le attività della finestra di manutenzione senza obiettivi non supportano MaxConcurrency i valori» e «Le attività della finestra di manutenzione senza obiettivi non supportano MaxErrors i valori»](#)

## Risoluzione dei problemi di finestre di manutenzione

Utilizza le informazioni seguenti per risolvere i problemi relativi alle finestre di manutenzione.

### Argomenti

- [Errore nella modifica dell'attività: nella pagina per la modifica di un'attività della finestra di manutenzione, l'elenco dei ruoli IAM restituisce un messaggio di errore: "Non è stato possibile individuare il ruolo IAM della finestra di manutenzione specificato per questa attività. Potrebbe essere stato cancellato o potrebbe non essere stato ancora creato".](#)
- [Non tutte le destinazioni di finestra di manutenzione vengono aggiornate](#)
- [L'attività non riesce con lo stato di richiamo dell'attività: «Il ruolo fornito non contiene le autorizzazioni SSM corrette».](#)
- [L'attività fallisce con messaggio di errore: "Il passaggio da esito negativo quando convalida e risolve gli input del passaggio"](#)
- [Messaggi di errore: «Le attività della finestra di manutenzione senza obiettivi non supportano MaxConcurrency i valori» e «Le attività della finestra di manutenzione senza obiettivi non supportano MaxErrors i valori»](#)

Errore nella modifica dell'attività: nella pagina per la modifica di un'attività della finestra di manutenzione, l'elenco dei ruoli IAM restituisce un messaggio di errore: "Non è stato possibile individuare il ruolo IAM della finestra di manutenzione specificato per questa attività. Potrebbe essere stato cancellato o potrebbe non essere stato ancora creato".

Problema 1: il ruolo della finestra di manutenzione AWS Identity and Access Management (IAM) specificato originariamente è stato eliminato dopo la creazione del task.

Possibile soluzione: (1) seleziona un altro ruolo IAM per la finestra di manutenzione, se disponibile nell'account, oppure creane uno nuovo e selezionalo per l'attività.

Problema 2: se l'attività è stata creata utilizzando AWS Command Line Interface (AWS CLI) o un AWS SDK AWS Tools for Windows PowerShell, potrebbe essere stato specificato un nome di ruolo della finestra di manutenzione IAM inesistente. Ad esempio, il ruolo IAM per la finestra di manutenzione potrebbe essere stato eliminato prima della creazione dell'attività, oppure il nome del ruolo potrebbe essere stato digitato non correttamente, ad esempio **myrole** invece di **my-role**.

Possibile soluzione: seleziona il nome corretto del ruolo IAM per la finestra di manutenzione che desideri utilizzare o creane uno nuovo specifico per l'attività.

Non tutte le destinazioni di finestra di manutenzione vengono aggiornate

Problema: si nota che le attività della finestra di manutenzione non sono state eseguite su tutte le risorse interessate dalla finestra di manutenzione. Ad esempio, nei risultati dell'esecuzione della finestra di manutenzione, l'attività per tale risorsa viene contrassegnata come non riuscita o scaduta.

Soluzione: i motivi più comuni per cui un'attività della finestra di manutenzione non è in esecuzione su una risorsa di destinazione riguardano connettività e disponibilità. Ad esempio:

- Systems Manager ha perso la connessione alla risorsa prima o durante l'operazione di manutenzione della finestra.
- La risorsa non è in linea o è stata arrestata durante l'operazione di manutenzione della finestra.

È possibile attendere il periodo successivo pianificato della finestra di manutenzione per eseguire le attività sulle risorse. È possibile eseguire manualmente le attività della finestra di manutenzione sulle risorse non disponibili o non in linea.

L'attività non riesce con lo stato di richiamo dell'attività: «Il ruolo fornito non contiene le autorizzazioni SSM corrette».

Problema: è stato specificato un ruolo di servizio della finestra di manutenzione per un'attività, ma l'esecuzione dell'attività non riesce e lo stato di richiamo dell'attività riporta che «Il ruolo fornito non contiene le autorizzazioni SSM corrette».

- Soluzione: In [Attività 1: crea una policy personalizzata per il ruolo di servizio della finestra di manutenzione tramite la console](#), forniamo una policy di base che si può allegare al [ruolo di servizio personalizzato della finestra di manutenzione](#). La policy include le autorizzazioni necessarie per molti scenari di attività. Tuttavia, a causa dell'ampia varietà di attività che è possibile eseguire, potrebbe essere necessario fornire autorizzazioni aggiuntive nella policy per il ruolo della finestra di manutenzione.

Ad esempio, alcune azioni di automazione funzionano con gli stack. AWS CloudFormation. Pertanto, potrebbe essere necessario dover aggiungere le autorizzazioni aggiuntive `cloudformation:CreateStack`, `cloudformation:DescribeStacks` e `cloudformation>DeleteStack` alla policy per il ruolo di servizio della finestra di manutenzione.

Un altro esempio: il runbook di automazione AWS-CopySnapshot richiede le autorizzazioni per creare uno snapshot Amazon Elastic Block Store (Amazon EBS). Pertanto, potrebbe essere necessario dover aggiungere l'autorizzazione `ec2:CreateSnapshot`.

Per informazioni sulle autorizzazioni di ruolo necessarie per un runbook di Automation AWS gestito, consulta le descrizioni del runbook nell'Automation Runbook Reference. [AWS Systems Manager](#)

Per informazioni sulle autorizzazioni di ruolo necessarie per un documento SSM AWS gestito, rivedi il contenuto del documento nella sezione Documenti della console di Systems Manager. <https://console.aws.amazon.com/systems-manager/documents>

Per informazioni sulle autorizzazioni dei ruoli necessarie per le attività Step Functions, Lambda, i runbook Automation personalizzati e i documenti SSM, verifica i requisiti di autorizzazione con l'autore di tali risorse.

L'attività fallisce con messaggio di errore: "Il passaggio da esito negativo quando convalida e risolve gli input del passaggio"

Problema: un runbook Automation o un documento di comando di Systems Manager utilizzato in un'attività richiede l'immissione di input quali InstanceId o SnapshotId, ma un valore non viene fornito o non viene fornito in modo corretto.

- Soluzione 1: se l'attività è destinata a una singola risorsa, ad esempio un singolo nodo o una singola snapshot, inserire il relativo ID nei parametri di input per l'attività.
- Soluzione 2: se l'attività è destinata a più risorse, ad esempio la creazione di immagini da più nodi quando si utilizza il runbook AWS-CreateImage, è possibile utilizzare uno degli pseudoparametri supportati per le attività della finestra di manutenzione nei parametri di input per rappresentare gli ID nodo nel comando.

I seguenti comandi registrano un'attività di automazione di Systems Manager con una finestra di manutenzione tramite AWS CLI. Il valore `--targets` indica un ID di destinazione della finestra di manutenzione. Inoltre, anche se il parametro `--targets` specifica un ID di destinazione della finestra, i parametri del runbook Automation richiedono che venga fornito un ID nodo. In questo caso, il comando utilizza lo pseudoparametro `{{RESOURCE_ID}}` come valore InstanceId.

AWS CLI comando:

Linux & macOS

Il comando di esempio seguente riavvia le istanze Amazon Elastic Compute Cloud (Amazon EC2) che appartengono al gruppo di destinazione della finestra di manutenzione con ID e32eeeb2-646c-4f4b-8ed1-205fbEXAMPLE.

```
aws ssm register-task-with-maintenance-window \
 --window-id "mw-0c50858d01EXAMPLE" \
 --targets Key=WindowTargetIds,Values=e32eeeb2-646c-4f4b-8ed1-205fbEXAMPLE \
 --task-arn "AWS-RestartEC2Instance" \
 --service-role-arn arn:aws:iam::123456789012:role/
MyMaintenanceWindowServiceRole \
 --task-type AUTOMATION \
 --task-invocation-parameters
 "Automation={DocumentVersion=5,Parameters={InstanceId='{{RESOURCE_ID}}'}}" \
 --priority 0 --max-concurrency 10 --max-errors 5 --name "My-Restart-EC2-
Instances-Automation-Task" \
 --description "Automation task to restart EC2 instances"
```

## Windows

```
aws ssm register-task-with-maintenance-window ^
 --window-id "mw-0c50858d01EXAMPLE" ^
 --targets Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE ^
 --task-arn "AWS-RestartEC2Instance" ^
 --service-role-arn arn:aws:iam::123456789012:role/
MyMaintenanceWindowServiceRole ^
 --task-type AUTOMATION ^
 --task-invocation-parameters
 "Automation={DocumentVersion=5,Parameters={InstanceId='{{RESOURCE_ID}}'}}" ^
 --priority 0 --max-concurrency 10 --max-errors 5 --name "My-Restart-EC2-
Instances-Automation-Task" ^
 --description "Automation task to restart EC2 instances"
```

Per ulteriori informazioni sull'utilizzo di pseudoparametri per le attività della finestra di manutenzione, consulta [Utilizzo degli pseudo parametri durante la registrazione delle attività della finestra di manutenzione](#) e [Esempi di registrazione dei task](#).

Messaggi di errore: «Le attività della finestra di manutenzione senza obiettivi non supportano MaxConcurrency i valori» e «Le attività della finestra di manutenzione senza obiettivi non supportano MaxErrors i valori»

Problema: quando si registra un'attività di tipo Run Command, è necessario specificare almeno una destinazione su cui eseguire l'attività. Per altri tipi di attività (automazione e AWS Step Functions), a seconda della natura dell'attività, gli obiettivi sono opzionali. AWS Lambda Le opzioni MaxConcurrency (il numero di risorse su cui eseguire un'attività contemporaneamente) e MaxErrors (il numero di errori per l'esecuzione dell'attività sulle risorse di destinazione prima che l'attività abbia esito negativo) non sono obbligatorie o supportate per le attività della finestra di manutenzione che non specificano le destinazioni. Il sistema genera questi messaggi di errore se vengono specificati valori per una di queste opzioni quando non viene specificata alcuna destinazione dell'attività.

Soluzione: se si riceve uno di questi errori, rimuovere i valori per la concorrenza e la soglia di errore prima di continuare a registrare o aggiornare l'attività della finestra di manutenzione.

Per ulteriori informazioni sull'esecuzione di attività che non specificano destinazioni, consulta [Registrazione delle attività della finestra di manutenzione senza destinazioni](#) nella Guida per l'utente di AWS Systems Manager .

# AWS Systems Manager Configurazione rapida

Utilizzalo Quick Setup per configurare rapidamente i servizi e le funzionalità di Amazon Web Services utilizzati di frequente con le best practice consigliate. Quick Setup semplifica la configurazione dei servizi, incluso Systems Manager, automatizzando le attività comuni o consigliate. Queste attività includono, ad esempio, la creazione di ruoli di profilo delle istanze obbligatorie AWS Identity and Access Management (IAM) e l'impostazione di best practice operative, come scansioni periodiche delle patch e raccolta dell'inventario. L'uso di Quick Setup non prevede alcun costo. Tuttavia, i costi possono essere addebitati in base al tipo di servizi impostato e ai limiti di utilizzo senza costi per i servizi utilizzati per configurare il servizio. Per cominciare a utilizzare Quick Setup, apri la [console di Systems Manager](#). Nel pannello di navigazione, scegli Quick Setup.

Questa sezione contiene gli argomenti seguenti.

- [Annullare la registrazione di un amministratore delegato per Quick Setup](#)
- [Risoluzione dei problemi Configurazione rapida results](#)
- [Utilizzo di un amministratore delegato per Configurazione rapida](#)
- [Configurazione per Assume il ruolo per Systems Manager](#)
- [Registrazione di un amministratore delegato per Quick Setup](#)
- [Utilizzo di Configurazione rapida API per gestire configurazioni e implementazioni](#)
- [Nozioni di base su Configurazione rapida](#)
- [Learn \(Guida\) Configurazione rapida terminologia e dettagli](#)
- [Supportata Configurazione rapida tipi di configurazione](#)

## Note

Se sei stato indirizzato a Quick Setup per aiutarti a configurare le istanze da gestire con Systems Manager, completa la procedura in [Configura la gestione degli host di Amazon EC2 utilizzando Configurazione rapida](#).

## Quali sono i vantaggi di Configurazione rapida?

Alcuni vantaggi di Quick Setup sono i seguenti:

- Semplificare la configurazione dei servizi e

Quick Setup illustra la configurazione delle best practice operative e distribuisce automaticamente tali configurazioni. Il pannello di controllo Quick Setup consente di visualizzare una visualizzazione in tempo reale dello stato di distribuzione della configurazione.

- Distribuire automaticamente le configurazioni su più account

Puoi Quick Setup utilizzarlo singolarmente Account AWS o in più Account AWS e Regioni AWS integrandoti con AWS Organizations. L'utilizzo Quick Setup su più account aiuta a garantire che l'organizzazione mantenga configurazioni coerenti.

- Eliminare la deviazione della configurazione

La deriva della configurazione si verifica ogni volta che un utente apporta modifiche a un servizio o a una funzionalità in conflitto con le selezioni effettuate tramite Quick Setup. Quick Setup verifica periodicamente la deriva della configurazione e tenta di correggerla.

## Chi dovrebbe utilizzarlo Configurazione rapida?

Quick Setup è particolarmente utile per i clienti che hanno già una certa esperienza con i servizi e le funzionalità che stanno configurando e che desiderano semplificare il processo di configurazione. Se non conosci il servizio con Servizio AWS cui stai configurando Quick Setup, ti consigliamo di saperne di più sul servizio. Prima di creare una configurazione con Quick Setup, esamina il contenuto della Guida per l'utente pertinente.

## Disponibilità di Configurazione rapida in Regioni AWS

Di seguito Regioni AWS, puoi utilizzare tutti i tipi di Quick Setup configurazione per un'intera organizzazione, come configurato in AWS Organizations, o solo per gli account organizzativi e le regioni scelti. È possibile anche utilizzare Quick Setup con un solo account in tali Regioni.

- Stati Uniti orientali (Ohio)
- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti occidentali (California settentrionale)
- Stati Uniti occidentali (Oregon)
- Asia Pacifico (Mumbai)
- Asia Pacifico (Seoul)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)



- Asia Pacifico (Tokyo)
- Canada (Centrale)
- Europa (Francoforte)
- Europa (Stoccolma)
- Europa (Irlanda)
- Europa (Londra)
- Europa (Parigi)
- Sud America (San Paolo)

Nelle seguenti Regioni, per i singoli account è disponibile solo il tipo di configurazione [Gestione host](#):

- Europa (Milano)
- Asia Pacifico (Hong Kong)
- Medio Oriente (Bahrein)
- Cina (Pechino)
- Cina (Ningxia)
- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

Per avere un elenco di tutte le Regioni supportate per Systems Manager, consulta la colonna Regione in [Endpoint del servizio Systems Manager](#) nella Riferimenti generali di Amazon Web Services.

## Nozioni di base su Configurazione rapida

Usa le informazioni contenute in questo argomento per prepararti all'uso di Quick Setup.

### Ruoli e autorizzazioni IAM per Configurazione rapida onboarding

Quick Setup ha lanciato una nuova esperienza di console e una nuova API. Ora puoi interagire con questa API utilizzando la console AWS CLI CloudFormation, e gli SDK. Se accedi alla nuova esperienza, le configurazioni esistenti vengono ricreate utilizzando la nuova API. A seconda del numero di configurazioni esistenti nell'account, questo processo richiede alcuni minuti.

Per utilizzare la nuova console Quick Setup, è necessario disporre delle autorizzazioni per le operazioni seguenti:

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm-quicksetup:*",
 "cloudformation:DescribeStackSetOperation",
 "cloudformation:ListStacks",
 "cloudformation:DescribeStacks",
 "cloudformation:DescribeStackResources",
 "cloudformation:ListStackSetOperations",
 "cloudformation:ListStackInstances",
 "cloudformation:DescribeStackSet",
 "cloudformation:ListStackSets",
 "cloudformation:DescribeStackInstance",
 "cloudformation:DescribeOrganizationsAccess",
 "cloudformation:ActivateOrganizationsAccess",
 "cloudformation:GetTemplate",
 "cloudformation:ListStackSetOperationResults",
 "cloudformation:DescribeStackEvents",
 "cloudformation:UntagResource",
 "ec2:DescribeInstances",
 "ssm:DescribeAutomationExecutions",
 "ssm:GetAutomationExecution",
 "ssm:ListAssociations",
 "ssm:DescribeAssociation",
 "ssm:GetDocument",
 "ssm:ListDocuments",
 "ssm:DescribeDocument",
 "ssm:ListResourceDataSync",
 "ssm:DescribePatchBaselines",
 "ssm:GetPatchBaseline",
 "ssm:DescribeMaintenanceWindows",
 "ssm:DescribeMaintenanceWindowTasks",
 "ssm:GetOpsSummary",
 "organizations:DeregisterDelegatedAdministrator",
 "organizations:DescribeAccount",
 "organizations:DescribeOrganization",
 "organizations:ListDelegatedAdministrators",
 "organizations:ListRoots",
```

```

 "organizations:ListParents",
 "organizations:ListOrganizationalUnitsForParent",
 "organizations:DescribeOrganizationalUnit",
 "organizations:ListAWSServiceAccessForOrganization",
 "s3:GetBucketLocation",
 "s3:ListAllMyBuckets",
 "s3:ListBucket",
 "resource-groups:ListGroups",
 "iam:ListRoles",
 "iam:ListRolePolicies",
 "iam:GetRole",
 "iam:CreatePolicy",
 "organizations:RegisterDelegatedAdministrator",
 "organizations:EnableAWSServiceAccess",
 "cloudformation:TagResource"
],
 "Resource": "*"
},
{
 "Effect": "Allow",
 "Action": [
 "cloudformation:RollbackStack",
 "cloudformation:CreateStack",
 "cloudformation:UpdateStack",
 "cloudformation>DeleteStack"
],
 "Resource": [
 "arn:aws:cloudformation:::stack/StackSet-AWS-QuickSetup-*",
 "arn:aws:cloudformation:::stack/AWS-QuickSetup-*",
 "arn:aws:cloudformation:::type/resource/*",
 "arn:aws:cloudformation:::stack/StackSet-SSMQuickSetup"
]
},
{
 "Effect": "Allow",
 "Action": [
 "cloudformation:CreateStackSet",
 "cloudformation:UpdateStackSet",
 "cloudformation>DeleteStackSet",
 "cloudformation>DeleteStackInstances",
 "cloudformation:CreateStackInstances",
 "cloudformation:StopStackSetOperation"
],
 "Resource": [

```

```

 "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
 "arn:aws:cloudformation:*:*:stackset/SSMQuickSetup",
 "arn:aws:cloudformation:*:*:type/resource/*",
 "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-*:*"
]
},
{
 "Effect": "Allow",
 "Action": [
 "iam:CreateRole",
 "iam>DeleteRole",
 "iam:AttachRolePolicy",
 "iam:DetachRolePolicy",
 "iam:GetRolePolicy",
 "iam:PutRolePolicy"
],
 "Resource": [
 "arn:aws:iam:*:*:role/AWS-QuickSetup-*",
 "arn:aws:iam:*:*:role/service-role/AWS-QuickSetup-*"
]
},
{
 "Effect": "Allow",
 "Action": "iam:PassRole",
 "Resource": "arn:aws:iam:*:111122223333:role/AWS-QuickSetup-*",
 "Condition": {
 "StringEquals": {
 "iam:PassedToService": [
 "ssm-quicksetup.amazonaws.com",
 "cloudformation.amazonaws.com"
]
 }
 }
},
{
 "Effect": "Allow",
 "Action": [
 "ssm>DeleteAssociation",
 "ssm>CreateAssociation",
 "ssm:StartAssociationsOnce"
],
 "Resource": "*"
},
{

```

```

 "Effect": "Allow",
 "Action": "ssm:StartAutomationExecution",
 "Resource": [
 "arn:aws:ssm:*:*:document/AWS-EnableExplorer",
 "arn:aws:ssm:*:*:automation-execution/*"
]
 },
 {
 "Effect": "Allow",
 "Action": [
 "ssm:GetOpsSummary",
 "ssm:CreateResourceDataSync",
 "ssm:UpdateResourceDataSync"
],
 "Resource": "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "iam:CreateServiceLinkedRole"
],
 "Condition": {
 "StringEquals": {
 "iam:AWSServiceName": [
 "accountdiscovery.ssm.amazonaws.com",
 "ssm.amazonaws.com",
 "ssm-quicksetup.amazonaws.com",
 "stacksets.cloudformation.amazonaws.com"
]
 }
 },
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "iam:CreateServiceLinkedRole"
],
 "Resource": "arn:aws:iam:*:*:role/aws-
service-role/stacksets.cloudformation.amazonaws.com/
AWSServiceRoleForCloudFormationStackSetsOrgAdmin"
 }
]

```

```
}
```

Per limitare gli utenti alle autorizzazioni di sola lettura, consenti solo le operazioni `ssm-quicksetup:List*` e `ssm-quicksetup:Get*` relative all'API di Quick Setup.

Durante l'onboarding, Quick Setup crea i seguenti ruoli AWS Identity and Access Management (IAM) per tuo conto:

- `AWS-QuickSetup-LocalExecutionRole`: concede le autorizzazioni CloudFormation per utilizzare qualsiasi modello, escluso il modello di policy di patch, e per creare le risorse necessarie.
- `AWS-QuickSetup-LocalAdministrationRole`— Concede i permessi di assunzione. AWS CloudFormation `AWS-QuickSetup-LocalExecutionRole`
- `AWS-QuickSetup-PatchPolicy-LocalExecutionRole`— Concede le autorizzazioni per AWS CloudFormation utilizzare il modello di policy sulle patch e creare le risorse necessarie.
- `AWS-QuickSetup-PatchPolicy-LocalAdministrationRole`— Concede i permessi di assunzione. AWS CloudFormation `AWS-QuickSetup-PatchPolicy-LocalExecutionRole`

Se stai effettuando l'onboarding di un account di gestione, l'account in cui crei un'organizzazione, crea Quick Setup anche i seguenti ruoli per tuo conto AWS Organizations:

- `AWS-QuickSetup-SSM-RoleForEnablingExplorer`: concede le autorizzazioni al runbook Automation `AWS-EnableExplorer`. Il `AWS-EnableExplorer` runbook configura Explorer, uno strumento in Systems Manager per visualizzare informazioni per più e. Account AWS Regioni AWS
- `AWSServiceRoleForAmazonSSM`— Un ruolo collegato ai servizi che consente l'accesso alle AWS risorse gestite e utilizzate da Systems Manager.
- `AWSServiceRoleForAmazonSSM_AccountDiscovery`— Ruolo collegato ai servizi che concede a Systems Manager l'autorizzazione a chiamare Servizi AWS per scoprire informazioni durante la sincronizzazione dei dati. Account AWS Per ulteriori informazioni, consulta [Usare i ruoli per raccogliere Account AWS informazioni per OpsCenter and Explorer](#).

Quando si effettua l'onboarding di un account di gestione, Quick Setup consente l'accesso affidabile tra le configurazioni AWS Organizations e la distribuzione CloudFormation all'interno dell'organizzazione. Quick Setup Per abilitare l'accesso attendibile, l'account di gestione deve disporre delle autorizzazioni di amministratore. Dopo l'onboarding, non sono più necessarie le

autorizzazioni di amministratore. Per ulteriori informazioni, consulta [Attivazione dell'accesso attendibile con Organizations](#).

Per informazioni sui tipi di AWS Organizations account, consulta la [AWS Organizations terminologia e i concetti](#) nella Guida per l'utente. AWS Organizations

#### Note

Quick Setup utilizza CloudFormation StackSets per distribuire le configurazioni in tutte le regioni Account AWS. Se il numero di account di destinazione moltiplicato per il numero di regioni supera 10.000, la configurazione non viene implementata. Ti consigliamo di esaminare il tuo caso d'uso e di creare configurazioni che utilizzino un minor numero di obiettivi per soddisfare la crescita della tua organizzazione. Le istanze di stack non vengono implementate nell'account di gestione dell'organizzazione. Per maggiori informazioni, consulta [Considerazioni sulla creazione di un set di stack con autorizzazioni gestite dal servizio](#).

Onboarding manuale per lavorare con Configurazione rapida API a livello di programmazione

Quando utilizzi la console per lavorare con Quick Setup, il servizio gestisce le fasi di onboarding per te. Se prevedi di utilizzare gli SDK o i AWS CLI per lavorare con l'Quick Setup API, puoi comunque utilizzare la console per completare le fasi di onboarding in modo da non doverle eseguire manualmente. Tuttavia, alcuni clienti necessitano di completare le fasi di onboarding su Quick Setup in modo programmatico, senza interagire con la console. Se questo metodo si adatta al proprio caso d'uso, è necessario completare le fasi seguenti. Tutti questi passaggi devono essere completati dal tuo account di AWS Organizations gestione.

Per completare l'onboarding manuale per Configurazione rapida

1. Attiva l'accesso affidabile per CloudFormation le organizzazioni. Ciò fornisce all'account di gestione le autorizzazioni necessarie per creare e gestire StackSets l'organizzazione. Puoi utilizzare CloudFormation l'azione `ActivateOrganizationsAccess` API per completare questo passaggio. Per ulteriori informazioni, consulta [ActivateOrganizationsAccess](#) nella documentazione di riferimento dell'API AWS CloudFormation .
2. Abilita l'integrazione di Systems Manager con Organizations. Ciò consente a Systems Manager di creare un ruolo collegato ai servizi in tutti gli account dell'organizzazione. Inoltre, consente a Systems Manager di eseguire operazioni per conto dell'utente all'interno dell'organizzazione e

dei relativi account. Puoi utilizzare AWS Organizations l'azione `EnableAWSServiceAccess` API per completare questo passaggio. Il principio del servizio per Systems Manager è `ssm.amazonaws.com`. Per ulteriori informazioni, consulta [EnableAWSServiceAccess](#) l'AWS Organizations API Reference.

3. Creare il ruolo IAM richiesto per Explorer. Ciò consente a Quick Setup di creare pannelli di controllo per le configurazioni in modo da poter visualizzare gli stati di implementazione e associazione. Crea un ruolo IAM e collega la policy gestita `AWSSystemsManagerEnableExplorerExecutionPolicy`. Modificare la policy di attendibilità affinché il ruolo corrisponda a quanto segue. Sostituisci ciascuno *account ID* con le tue informazioni.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "ssm.amazonaws.com"
 },
 "Action": "sts:AssumeRole",
 "Condition": {
 "StringEquals": {
 "aws:SourceAccount": "111122223333"
 },
 "ArnLike": {
 "aws:SourceArn": "arn:*:ssm:*:111122223333:automation-
execution/*"
 }
 }
 }
]
}
```

4. Aggiorna l'impostazione del servizio Quick Setup per Explorer. È possibile utilizzare l'azione API `UpdateServiceSettings` di Quick Setup per completare questo passaggio. Specifica l'ARN per il ruolo IAM creato nel passaggio precedente per il parametro di richiesta `ExplorerEnablingRoleArn`. Per ulteriori informazioni, consulta [UpdateServiceSettings](#) nella documentazione di riferimento dell'API Quick Setup.



5. Crea i ruoli IAM richiesti CloudFormation StackSets da utilizzare. È necessario creare un ruolo di esecuzione e un ruolo di amministrazione.
  - a. Creare il ruolo di esecuzione. Al ruolo di esecuzione va associata almeno una delle politiche gestite, `AWSQuickSetupDeploymentRolePolicy` o `AWSQuickSetupPatchPolicyDeploymentRolePolicy`. Se stai creando solo configurazioni di policy di patch, è possibile utilizzare la policy gestita `AWSQuickSetupPatchPolicyDeploymentRolePolicy`. Tutte le altre configurazioni utilizzano la policy `AWSQuickSetupDeploymentRolePolicy`. Modificare la policy di attendibilità affinché il ruolo corrisponda a quanto segue. Sostituisci ogni *account ID* *administration role name* mano con le tue informazioni.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "AWS": "arn:aws:iam::111122223333:role/administration
role name"
 },
 "Action": "sts:AssumeRole"
 }
]
}
```

- b. Crea il ruolo di amministrazione. È necessario che la policy autorizzata corrisponda a quanto segue. Sostituisci ciascuna *account ID* *execution role name* mano con le tue informazioni.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Action": [
 "sts:AssumeRole"
]
 }
]
}
```

```

],
 "Resource": "arn:*:iam:*:111122223333:role/execution role
name",
 "Effect": "Allow"
 }
]
}

```

Modificare la policy di attendibilità affinché il ruolo corrisponda a quanto segue. Sostituisci ognuna *account ID* con le tue informazioni.

JSON

```

{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "cloudformation.amazonaws.com"
 },
 "Action": "sts:AssumeRole",
 "Condition": {
 "StringEquals": {
 "aws:SourceAccount": "111122223333"
 },
 "ArnLike": {
 "aws:SourceArn":
 "arn:aws:cloudformation:*:111122223333:stackset/AWS-QuickSetup-*"
 }
 }
 }
]
}

```

## Configurazione per Assume il ruolo per Systems Manager

Per creare un ruolo da assumere per Systems Manager Quick Setup:

Systems Manager Quick Setup richiede un ruolo che consenta a Systems Manager di eseguire azioni in modo sicuro sull'account. Questo ruolo concede a Systems Manager le autorizzazioni necessarie per eseguire comandi sulle istanze e configurare le istanze EC2, i ruoli IAM e altre risorse di Systems Manager per conto dell'utente.

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, scegli **Policy**, quindi **Crea policy**
3. Aggiungi la `SsmOnboardingInlinePolicy` policy utilizzando il codice JSON riportato di seguito. Questa policy abilita le azioni necessarie per allegare le autorizzazioni del profilo dell'istanza alle istanze specificate. Ad esempio, consente di creare profili di istanza e associarli alle istanze EC2.
4. Dopo aver completato questo passaggio, nel riquadro di navigazione, scegli **Ruoli**, quindi scegli **Crea ruolo**.
5. Per il tipo di entità **attendibile**, mantienilo come predefinito (servizio).
6. In **Caso d'uso**, scegli **Systems Manager**, quindi scegli **Avanti**.
7. Nella **pagina Aggiungi autorizzazioni**:
8. Aggiungi la policy `SsmOnboardingInlinePolicy`
9. Seleziona **Next (Successivo)**.
10. Per **Nome ruolo**, inserisci un nome descrittivo (ad esempio, `AmazonSSMRoleForAutomationAssumeQuickSetup`).
11. (Facoltativo) Aggiungi tag per identificare e organizzare il ruolo.
12. Scegliere **Crea ruolo**.

### Important

Il ruolo deve includere un rapporto di fiducia con `ssm.amazonaws.com`. Questo viene configurato automaticamente quando si seleziona Systems Manager come servizio nel passaggio 4.

Dopo aver creato il ruolo, è possibile selezionarlo durante la configurazione di Quick Setup. Il ruolo consente a Systems Manager di gestire le istanze EC2, i ruoli IAM e altre risorse di Systems Manager ed eseguire comandi per conto dell'utente mantenendo la sicurezza tramite autorizzazioni specifiche e limitate.

Policy di autorizzazione

### **SsmOnboardingInlinePolicy**

La seguente politica definisce le autorizzazioni per Systems Manager Quick Setup:

```
{
 "Version": "2012-10-17"
,
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iam:CreateInstanceProfile",
 "iam:ListInstanceProfilesForRole",
 "ec2:DescribeIamInstanceProfileAssociations",
 "iam:GetInstanceProfile",
 "iam:AddRoleToInstanceProfile"
],
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "ec2:AssociateIamInstanceProfile"
],
 "Resource": "arn:aws:ec2:*:*:instance/*",
 "Condition": {
 "Null": {
 "ec2:InstanceProfile": "true"
 },
 "ArnLike": {
 "ec2:NewInstanceProfile": "arn:aws:iam:*:*:instance-profile/[INSTANCE_PROFILE_ROLE_NAME]"
 }
 }
 },
 {
 "Effect": "Allow",
```

```

 "Action": "iam:PassRole",
 "Resource": "arn:aws:iam::*:role/[INSTANCE_PROFILE_ROLE_NAME]",
 "Condition": {
 "StringEquals": {
 "iam:PassedToService": "ec2.amazonaws.com"
 }
 }
 }
]
}

```

## Relazioni di trust

Questo viene aggiunto automaticamente tramite i passaggi precedenti

```

{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "ssm.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
]
}

```

## Utilizzo di un amministratore delegato per Configurazione rapida

Dopo aver registrato un account amministratore delegato per Quick Setup, gli utenti con le autorizzazioni appropriate in tale account possono creare, aggiornare, visualizzare ed eliminare i gestori di configurazione destinati alle unità organizzative all'interno della struttura. AWS Organizations Questo account amministratore delegato può anche organizzare i gestori di configurazione creati precedentemente dall'account di gestione dell'organizzazione.

Solo l'account di gestione di un'organizzazione è in grado di registrare un account nell'organizzazione come amministratore delegato. Quando si registra un account come amministratore delegato per Quick Setup, questo account diventa anche amministratore delegato per AWS CloudFormation StackSets e Systems Manager Explorer. Questi servizi sono necessari per implementare e monitorare le configurazioni. Quick Setup

 Note

Attualmente, il tipo di configurazione della policy sulle patch non è supportato dall'amministratore delegato per Quick Setup. Le configurazioni delle policy di patch per un'organizzazione devono essere create e gestite nell'account di gestione dell'organizzazione. Per ulteriori informazioni, consulta [Creazione di una policy di patch](#).

I seguenti argomenti descrivono come registrare e annullare la registrazione di un amministratore delegato per Quick Setup.

### Registrazione di un amministratore delegato per Quick Setup

Per registrare un amministratore delegato per Quick Setup, attenersi alla procedura descritta di seguito.

Per registrare un amministratore delegato per Quick Setup

1. Accedi al tuo account AWS Organizations di gestione.
2. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
3. Nel pannello di navigazione, scegli Quick Setup.
4. Seleziona Impostazioni.
5. Nella sezione Amministratore delegato per Quick Setup, verifica di aver configurato le opzioni di accesso al servizio e al ruolo collegato al servizio necessarie. Se necessario, scegli i pulsanti Crea ruolo e Abilitazione dell'accesso per configurare queste opzioni.
6. Per Account ID, inserisci l' Account AWS ID. Questo account deve essere un account membro in AWS Organizations.
7. Scegliere Registra amministratore delegato.

### Annullare la registrazione di un amministratore delegato per Quick Setup

Utilizzare la procedura seguente per annullare la registrazione di un amministratore delegato per Quick Setup.

Per annullare la registrazione di un amministratore delegato di Quick Setup

1. Accedi al tuo account AWS Organizations di gestione.

2. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
3. Nel pannello di navigazione, scegli Quick Setup.
4. Seleziona Impostazioni.
5. Nella sezione Amministratore delegato per Quick Setup, scegli Annulla registrazione dal menu a discesa delle Operazioni.
6. Seleziona Conferma.

## Learn (Guida) Configurazione rapida terminologia e dettagli

Quick Setup visualizza i risultati di tutti i gestori di configurazione che hai creato Regioni AWS nella tabella Gestori di configurazione nella Quick Setup home page. In questa pagina, è possibile utilizzare View details (Visualizza dettagli) per visualizzare i dettagli di ciascuna configurazione, eliminare le configurazioni dal menu a discesa Actions (Operazioni) o utilizzare Create (Crea) per creare configurazioni. La tabella Gestori di configurazione contiene le informazioni seguenti:

- Nome: il nome del gestore di configurazione, se fornito al momento della creazione.
- Tipo di configurazione: il tipo di configurazione scelto durante la creazione della configurazione.
- Versione: la versione del tipo di configurazione attualmente distribuita.
- Unità organizzative: mostra le unità organizzative in cui viene implementata la configurazione, se scegli una serie di destinazioni Personalizzate. Le unità organizzative e le destinazioni personalizzate sono disponibili solo per l'account di gestione dell'organizzazione. L'account di gestione è l'account utilizzato per creare un'organizzazione in AWS Organizations.
- Tipo di implementazione: indica se l'implementazione si applica all'intera organizzazione (Organizational) o solo al tuo account (Local).
- Regioni: le Regioni in cui viene implementata la configurazione, se scegli una serie di destinazioni Personalizzate o destinazioni all'interno dell'Account corrente.
- Stato di distribuzione: lo stato di distribuzione indica se l'istanza di destinazione o dello stack è stata distribuita AWS CloudFormation correttamente. Le istanze di destinazione o di stack contengono le opzioni di configurazione scelte durante la creazione della configurazione.
- Association status (Stato associazione): lo stato dell'associazione è lo stato di tutte le associazioni create dalla configurazione. Tutte le associazioni per tutte le destinazioni devono essere eseguite correttamente, altrimenti lo stato è Failed (Non riuscito).

Quick Setup crea ed esegue un'associazione di State Manager per ogni destinazione di configurazione. State Manager è uno strumento di AWS Systems Manager.

Per visualizzare le configurazioni implementate nella regione attualmente esplorata, seleziona la scheda Configurazioni.

### Dettagli di configurazione

Nella pagina Configuration details (Dettagli configurazione) vengono visualizzate informazioni sull'implementazione della configurazione e sulle relative associazioni. Da questa pagina è possibile modificare le opzioni di configurazione, aggiornare le destinazioni o eliminare la configurazione. È possibile anche visualizzare i dettagli dell'implementazione di ciascuna configurazione per ottenere ulteriori informazioni sulle associazioni.

A seconda del tipo di configurazione, vengono visualizzati uno o più dei seguenti grafici di stato:

#### Stato dell'implementazione della configurazione

Visualizza il numero di implementazioni riuscite, non riuscite o in sospeso. Le implementazioni si verificano negli account e nelle regioni di destinazione specificati che contengono i nodi interessati dalla configurazione.

#### Stato dell'associazione della configurazione

Visualizza il numero di associazioni State Manager riuscite, non riuscite o in sospeso. Quick Setup crea un'associazione in ogni implementazione per le opzioni di configurazione selezionate.

#### Stato di configurazione

Visualizza il numero di operazioni eseguite in base al tipo di configurazione e il relativo stato corrente.

#### Conformità delle risorse

Visualizza il numero di risorse conformi alla policy specificata per la configurazione.

Nella tabella Dettagli di configurazione vengono visualizzate informazioni sull'implementazione della configurazione. È possibile visualizzare ulteriori dettagli su ogni implementazione selezionando l'implementazione e scegliendo View details (Visualizza dettagli). Nella pagina dei dettagli di ciascuna implementazione vengono visualizzate le associazioni implementate sui nodi di quella implementazione.



## Modifica ed eliminazione della configurazione

È possibile modificare le opzioni di una configurazione dalla pagina Configuration details (Dettagli configurazione) scegliendo Actions (Operazioni) e poi Edit configuration options (Modifica opzioni di configurazione). Quando si aggiungono nuove opzioni alla configurazione, Quick Setup esegue le implementazioni e crea nuove associazioni. Quando si rimuovono opzioni da una configurazione, Quick Setup esegue le implementazioni e rimuove tutte le associazioni correlate.

### Note

È possibile modificare le configurazioni di Quick Setup per il proprio account in qualsiasi momento. Per modificare la configurazione di una Organizzazione, Stato configurazione deve essere Riuscito o Non riuscito.

È possibile anche aggiornare le destinazioni incluse nelle configurazioni scegliendo Operazioni e Aggiungi UO, Aggiungi Regioni, Rimuovi UO oppure Rimuovi Regioni. Se il tuo account non è configurato come account di gestione o hai creato la configurazione solo per l'account corrente, non è possibile aggiornare le unità organizzative (UO) di destinazione. La rimozione di una regione o di un'unità organizzativa rimuove le associazioni da tali regioni o unità organizzative.

Periodicamente, Quick Setup rilascia nuove versioni di configurazioni. È possibile selezionare l'opzione Aggiorna configurazione per aggiornare la configurazione alla versione più recente.

Per eliminare una configurazione da Quick Setup, selezionala, quindi seleziona Actions (Operazioni) e poi Delete configuration (Elimina configurazione). In alternativa, è possibile eliminare la configurazione dalla pagina Dettagli di configurazione nel menu a discesa Operazioni e quindi selezionare Elimina configurazione. Quick Setup chiederà quindi di selezionare Rimuovi tutte le unità organizzative e le Regioni. Il completamento di questa operazione potrebbe richiedere un po' di tempo. L'eliminazione di una configurazione elimina anche tutte le associazioni correlate. Questo processo di eliminazione in due fasi rimuove tutte le risorse implementate da tutti gli account e le regioni e quindi elimina la configurazione.

## Conformità di configurazione

È possibile verificare se le istanze sono conformi alle associazioni create dalle configurazioni sia in Explorer sia in Conformità, entrambi strumenti di AWS Systems Manager. Per ulteriori informazioni sulla conformità, consulta [Scopri i dettagli sulla conformità](#). Per ulteriori informazioni sulla visualizzazione della conformità in Explorer, consulta [AWS Systems Manager Explorer](#).

## Utilizzo di Configurazione rapida API per gestire configurazioni e implementazioni

Puoi utilizzare l'API fornita da Quick Setup per creare e gestire configurazioni e implementazioni utilizzando l'SDK AWS CLI o il tuo SDK preferito. Puoi anche utilizzarla CloudFormation per creare una risorsa di gestione della configurazione che distribuisce le configurazioni. Utilizzando l'API, si creano gestori di configurazione che implementino le definizioni di configurazione. Le definizioni di configurazione contengono tutte le informazioni necessarie per implementare un particolare tipo di configurazione. Per ulteriori informazioni sull'utilizzo dell'API Quick Setup, consulta la [Documentazione di riferimento sulla configurazione rapida API](#).

Gli esempi seguenti dimostrano come creare gestori di configurazione utilizzando e. AWS CLI CloudFormation

### AWS CLI

```
aws ssm-quicksetup create-configuration-manager \
--name configuration manager name \
--description Description of your configuration manager
--configuration-definitions JSON string containing configuration definition
```

Di seguito è riportato un esempio di stringa JSON contenente una definizione di configurazione per la policy di patch.

```
{
 "Type": "AWSQuickSetupType-PatchPolicy",
 "LocalDeploymentAdministrationRoleArn": "arn:aws:iam::123456789012:role/AWS-QuickSetup-StackSet-Local-AdministrationRole",
 "LocalDeploymentExecutionRoleName": "AWS-QuickSetup-StackSet-Local-ExecutionRole",
 "Parameters": {
 "ConfigurationOptionsInstallNextInterval": "true",
 "ConfigurationOptionsInstallValue": "cron(0 2 ? * SAT#1 *)",
 "ConfigurationOptionsPatchOperation": "ScanAndInstall",
 "ConfigurationOptionsScanNextInterval": "1 * * ? * *",
 "HasDeletedBaseline": "false",
 "IsPolicyAttachAllowed": "true",
 "OutputBucketRegion": "",
 "OutputBucketName": "aws-ssm-us-east-1",
 "PatchBaselineUseDefault": "custom",
 "PatchPolicyName": "dev-patch-policy",
 "RateControlConcurrency": "5",
 "RateControlErrorThreshold": "0%",
 "RebootOption": "RebootAfterPatch",
 "Patches": [
 {
 "value": "arn:aws:ssm:us-east-1:123456789012:patchbaseline/pb-0cb0c4966f86b059b",
 "label": "AWS-AlmaLinuxDefaultPatchBaseline",
 "description": "Default Patch Baseline for Alma Linux Provided by AWS.",
 "disabled": false
 },
 {
 "value": "arn:aws:ssm:us-east-1:123456789012:patchbaseline/pb-0be8c61cde3be63f3",
 "label": "AWS-AmazonLinux2DefaultPatchBaseline",
 "description": "Baseline containing all Security and Bugfix updates approved"
 }
]
 }
}
```

```
for Amazon Linux 2 instances\", \"disabled\":false}, \"AMAZON_LINUX_2023\":{ \"value
\": \"arn:aws:ssm:us-east-1:123456789012:patchbaseline/pb-05c9c9bf778d4c4d0\",
\"label\": \"AWS-AmazonLinux2023DefaultPatchBaseline\", \"description\": \"Default
Patch Baseline for Amazon Linux 2023 Provided by AWS.\", \"disabled\":false},
\"DEBIAN\":{ \"value\": \"arn:aws:ssm:us-east-1:123456789012:patchbaseline/
pb-09a5f8eb62bde80b1\", \"label\": \"AWS-DebianDefaultPatchBaseline\", \"description
\": \"Default Patch Baseline for Debian Provided by AWS.\", \"disabled\":false},
\"MACOS\":{ \"value\": \"arn:aws:ssm:us-east-1:123456789012:patchbaseline/
pb-0ee4f94581368c0d4\", \"label\": \"AWS-MacOSDefaultPatchBaseline\", \"description
\": \"Default Patch Baseline for MacOS Provided by AWS.\", \"disabled\":false},
\"ORACLE_LINUX\":{ \"value\": \"arn:aws:ssm:us-east-1:123456789012:patchbaseline/
pb-06bff38e95fe85c02\", \"label\": \"AWS-OracleLinuxDefaultPatchBaseline\",
\"description\": \"Default Patch Baseline for Oracle Linux Server Provided
by AWS.\", \"disabled\":false}, \"REDHAT_ENTERPRISE_LINUX\":{ \"value\":
\"arn:aws:ssm:us-east-1:123456789012:patchbaseline/pb-0cbb3a633de00f07c\",
\"label\": \"AWS-RedHatDefaultPatchBaseline\", \"description\": \"Default Patch
Baseline for Redhat Enterprise Linux Provided by AWS.\", \"disabled\":false},
\"ROCKY_LINUX\":{ \"value\": \"arn:aws:ssm:us-east-1:123456789012:patchbaseline/
pb-03ec98bc512aa3ac0\", \"label\": \"AWS-RockyLinuxDefaultPatchBaseline\",
\"description\": \"Default Patch Baseline for Rocky Linux Provided by AWS.\",
\"disabled\":false}, \"UBUNTU\":{ \"value\": \"pb-06e3563bd35503f2b\", \"label\":
\"custom-UbuntuServer-Blog-Baseline\", \"description\": \"Default Patch Baseline
for Ubuntu Provided by AWS.\", \"disabled\":false}, \"WINDOWS\":{ \"value\":
\"pb-016889927b2bb8542\", \"label\": \"custom-WindowsServer-Blog-Baseline\",
\"disabled\":false}}\", \"TargetInstances\": \"\", \"TargetOrganizationalUnits\": \"ou-9utf-
example\", \"TargetRegions\": \"us-east-1, us-
east-2\", \"TargetTagKey\": \"Patch\", \"TargetTagValue\": \"true\", \"TargetType\": \"Tags\"}}' \
```

## CloudFormation

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
 SSMQuickSetupTestConfigurationManager:
 Type: "AWS::SSMQuickSetup::ConfigurationManager"
 Properties:
 Name: "MyQuickSetup"
 Description: "Test configuration manager"
 ConfigurationDefinitions:
 - Type: "AWSQuickSetupType-CFGRecording"
 Parameters:
 TargetAccounts:
 Ref: AWS::AccountId
 TargetRegions:
```

```
Ref: AWS::Region
LocalDeploymentAdministrationRoleArn: !Sub "arn:aws:iam::
${AWS::AccountId}:role/AWS-QuickSetup-StackSet-ContractTest-AdministrationRole"
LocalDeploymentExecutionRoleName: "AWS-QuickSetup-StackSet-ContractTest-
ExecutionRole"
Tags:
 foo1: "bar1"
```

## Supportata Configurazione rapida tipi di configurazione

### Tipi di configurazioni supportati

Quick Setup illustra la configurazione delle best practice operative per diversi Systems Manager e altri sistemi e Servizi AWS la distribuzione automatica di tali configurazioni. Il pannello di controllo Quick Setup consente di visualizzare una visualizzazione in tempo reale dello stato di distribuzione della configurazione.

È possibile Quick Setup utilizzarlo singolarmente Account AWS o su più aree geografiche Account AWS integrandosi con. AWS Organizations L'utilizzo Quick Setup su più account aiuta a garantire che l'organizzazione mantenga configurazioni coerenti.

Quick Setup fornisce supporto per i seguenti tipi di configurazione.

- [Configura la gestione degli host di Amazon EC2 utilizzando Configurazione rapida](#)
- [Impostare la configurazione predefinita di gestione dell'host per un'organizzazione utilizzando Configurazione rapida](#)
- [Crea un AWS Config registratore di configurazione utilizzando Configurazione rapida](#)
- [Implementazione AWS Config pacchetto di conformità utilizzando Configurazione rapida](#)
- [Configurare l'applicazione di patch per le istanze in un'organizzazione utilizzando un Configurazione rapida politica sulle patch](#)
- [Configurazione dell'organizzazione di Change Manager](#)
- [Configura DevOps Guru usando Configurazione rapida](#)
- [Implementa i pacchetti Distributor tramite Quick Setup](#)
- [Arresta e avvia automaticamente le istanze EC2 in base a una pianificazione utilizzando Configurazione rapida](#)
- [Configurazione dell'organizzazione di OpsCenter](#)

- [Configura Esploratore di risorse AWS utilizzo di Configurazione rapida](#)

Configura la gestione degli host di Amazon EC2 utilizzando Configurazione rapida

Utilizzalo Quick Setup per configurare rapidamente i ruoli di sicurezza richiesti e gli strumenti di Systems Manager di uso comune sulle tue istanze Amazon Elastic Compute Cloud (Amazon EC2). Puoi utilizzarlo Quick Setup in un singolo account o su più account e integrandoti Regioni AWS con AWS Organizations. Questi strumenti consentono di gestire e monitorare lo stato delle istanze fornendo al contempo le autorizzazioni minime necessarie per iniziare.

Se non hai familiarità con i servizi e le funzionalità di Systems Manager, consigliamo di consultare la Guida per l'utente di AWS Systems Manager prima di creare una configurazione con Quick Setup. Per ulteriori informazioni su Systems Manager, consulta la Guida per l'utente di [Cosa è AWS Systems Manager?](#).

 Important

Quick Setup potrebbe non essere lo strumento giusto da utilizzare per la gestione di EC2 se si applica una delle seguenti condizioni:

- Stai cercando di creare un'istanza EC2 per la prima volta per provare le funzionalità. AWS
- Sei ancora alle prime armi con la gestione delle istanze EC2.

Consigliamo invece di esplorare il seguente contenuto:

- [Nozioni di base su Amazon EC2](#)
- [Avvio di un'istanza tramite la nuova procedura guidata di avvio dell'istanza](#) nella Guida per l'utente di Amazon EC2
- [Tutorial: nozioni di base sulle istanze Linux di Amazon EC2](#) nella Guida per l'utente di Amazon EC2

Se hai già familiarità con la gestione delle istanze EC2 e desideri semplificare la configurazione e la gestione per più istanze EC2, utilizza Quick Setup. A prescindere che la tua organizzazione disponga di decine, migliaia o milioni di istanze EC2, utilizza la seguente procedura Quick Setup per configurare più opzioni contemporaneamente.

 Note

Questo tipo di configurazione consente di impostare più opzioni per un'intera organizzazione definita in AWS Organizations, solo alcuni account e regioni organizzativi o un singolo account. Una di queste opzioni consiste nel verificare la presenza di aggiornamenti e applicarli all'SSM Agent ogni due settimane. Se sei un amministratore dell'organizzazione, è possibile anche scegliere di aggiornare tutte le istanze EC2 della tua organizzazione con aggiornamenti dell'agente ogni due settimane utilizzando il tipo di configurazione di gestione host predefinita. Per informazioni, consulta [Impostare la configurazione predefinita di gestione dell'host per un'organizzazione utilizzando Configurazione rapida](#).

## Configurazione delle opzioni di gestione host per le istanze EC2

Per configurare la gestione degli host, esegui le seguenti attività nella AWS Systems Manager Quick Setup console.

Per aprire la pagina di configurazione di gestione host

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Quick Setup.
3. Nella scheda Gestione host, scegli Crea.

 Tip

Se hai già una o più configurazioni nel tuo account, scegli prima la scheda Libreria o il pulsante Crea nella sezione Configurazioni per visualizzare le schede.

## Per configurare le opzioni di gestione host di Systems Manager

- Per configurare la funzionalità di Systems Manager, nella sezione Opzioni di configurazione, scegli le opzioni nel gruppo Systems Manager che desideri abilitare per la configurazione:

## Aggiorna l'agente Systems Manager (SSM) ogni due settimane

Consente a Systems Manager di verificare ogni due settimane la presenza di una nuova versione dell'agente. Se è presente una nuova versione, Systems Manager aggiorna automaticamente l'agente sul nodo gestito alla versione più recente rilasciata. Quick Setup non installa l'agente sulle istanze su cui non è già presente. Per informazioni su quali AMIs hanno SSM Agent preinstallato, consulta [Trova AMI con il Agente SSM preinstallato](#).

Ti invitiamo a scegliere questa opzione per assicurarti che i tuoi nodi eseguano sempre la versione più aggiornata di SSM Agent. Per ulteriori informazioni su SSM Agent, incluse quelle su come installare manualmente l'agente, consulta [Lavorare con Agente SSM](#).

## Raccolta dei dati di inventario dalle istanze ogni 30 minuti

Abilita Quick Setup per configurare la raccolta dei seguenti tipi di metadati:

- AWS componenti: driver EC2, agenti, versioni e altro ancora.
- Applicazioni: nomi delle applicazioni, editori, versioni e altro.
- Dettagli del nodo: nome del sistema, nome dei sistemi operativi, versione del sistema operativo, ultimo avvio, DNS, dominio, gruppo di lavoro, architettura del sistema operativo e altro.
- Configurazione di rete: indirizzo IP, indirizzo MAC, DNS, gateway, maschera di sottorete e altro.
- Servizi: nome, nome visualizzato, stato, servizi dipendenti, tipo di servizio, tipo di avvio e altro (solo nodi Windows Server).
- Ruoli Windows: nome, nome visualizzato, percorso, tipo di funzionalità, stato installato e altro (solo nodi Windows Server).
- Aggiornamenti di Windows: ID hotfix, installato da, data di installazione e altro (solo nodi Windows Server).

Per ulteriori informazioni sull'inventario, consulta [AWS Systems Manager Inventory](#).

### Note

Il completamento dell'opzione Raccolta Inventory può richiedere fino a 10 minuti, anche se sono stati selezionati solo pochi nodi.

## Scansione giornaliera delle istanze per rilevare patch mancanti

Consente Patch Manager di scansionare i nodi ogni giorno e generare un report nella pagina Conformità. Il report mostra il numero di nodi conformi alla patch secondo la baseline delle patch predefinita. Il report include un elenco di ciascun nodo e il relativo stato di conformità.

Per informazioni sulle operazioni di applicazione di patch e le baseline delle patch, consulta [AWS Systems Manager Patch Manager](#).

Per informazioni sulla conformità delle patch, consulta la pagina [Compliance](#) (Conformità) di Systems Manager.

Per informazioni sull'applicazione di patch ai nodi gestiti in più account e regioni con un'unica configurazione, consulta [Configurazioni delle policy sulle patch in Configurazione rapida](#) e [Configurare l'applicazione di patch per le istanze in un'organizzazione utilizzando un Configurazione rapida politica sulle patch](#).

### Important

Systems Manager supporta diversi metodi di scansione dei nodi gestiti al fine di verificare la conformità delle patch. Se implementi più metodi alla volta, le informazioni sulla conformità delle patch visualizzate rappresentano sempre il risultato della scansione più recente. I risultati delle scansioni precedenti vengono sovrascritti. Se i metodi di scansione utilizzano baseline delle patch diverse, con diverse regole di approvazione, le informazioni sulla conformità delle patch possono cambiare in modo imprevisto. Per ulteriori informazioni, consulta [Identificazione dell'esecuzione che ha creato i dati di conformità delle patch](#).

Per configurare le opzioni di gestione degli CloudWatch host di Amazon

- Per configurare CloudWatch la funzionalità, nella sezione Opzioni di configurazione, scegli le opzioni del CloudWatch gruppo Amazon che desideri abilitare per la tua configurazione:



## Installa e configura l' CloudWatch agente

Installa la configurazione di base dell' CloudWatch agente unificato sulle tue istanze Amazon EC2. L'agente raccoglie metriche e file di registro dalle tue istanze per Amazon. CloudWatch. Queste informazioni sono consolidate in modo da poter determinare rapidamente lo stato delle istanze. Per ulteriori informazioni sulla configurazione di base dell' CloudWatch agente, consulta i set di metriche predefiniti [CloudWatch dell'agente](#). Potrebbero essere addebitati costi aggiuntivi. Per ulteriori informazioni, consulta i prezzi di [Amazon CloudWatch](#).

### Aggiorna l' CloudWatch agente una volta ogni 30 giorni

Consente a Systems Manager di verificare ogni 30 giorni la presenza di una nuova versione dell' CloudWatch agente. Se è presente una nuova versione, Systems Manager aggiorna l'agente sull'istanza. Ti invitiamo a scegliere questa opzione per assicurarti che sulle tue istanze sia sempre in esecuzione la versione più aggiornata dell' CloudWatch agente.

### Per configurare le opzioni di gestione host dell'agente di avvio di Amazon EC2

- Per configurare la funzionalità dell'agente di avvio di Amazon EC2, nella sezione Opzioni di configurazione, scegli le opzioni nel gruppo Agente di avvio di Amazon EC2 che desideri abilitare per la configurazione:

### Aggiorna l'agente di avvio EC2 una volta ogni 30 giorni

Consenti a Systems Manager di verificare ogni 30 giorni la presenza di una nuova versione dell'agente di avvio installato sull'istanza. Se è presente una nuova versione, Systems Manager aggiorna l'agente sull'istanza. Ti invitiamo a scegliere questa opzione per assicurarti che sulle tue istanze sia sempre in esecuzione la versione più aggiornata del launch agent applicabile. Per le istanze Windows di Amazon EC2, questa opzione supporta EC2Launch, EC2Launch v2 ed EC2Config. Per le istanze Linux di Amazon EC2, questa opzione supporta cloud-init. Per le istanze Mac di Amazon EC2, questa opzione supporta ec2-macos-init. Quick Setup non supporta l'aggiornamento degli agenti di avvio installati su sistemi operativi non supportati dall'agente di avvio o su AL2023.

Per ulteriori informazioni su questi agenti di inizializzazione, consulta i seguenti argomenti:

- [Configurare un'istanza Windows tramite EC2Launch v2](#)

- [Configurare un'istanza Windows tramite EC2Launch](#)
- [Configurare un'istanza Windows tramite il servizio EC2Config](#)
- [Documentazione cloud-init](#)
- [ec2-macos-init](#)

Per selezionare le istanze EC2 da aggiornare in base alla configurazione di gestione host

- Nella sezione Targets (Destinazioni), scegli il metodo per determinare gli account e le regioni in cui deve essere implementata la configurazione:

 Note

Non è possibile creare più configurazioni di gestione host Quick Setup che hanno come destinazione la stessa Regione AWS.

## Entire organization

La configurazione viene distribuita a tutte le unità organizzative (OU) e all' Regioni AWS interno dell'organizzazione.

 Note

L'intera organizzazione è disponibile solo se nella configurazione della gestione host è presente un account di gestione dell'organizzazione.

## Custom

1. Nella sezione Unità organizzative di destinazione, seleziona le unità organizzative in cui desideri implementare questa configurazione di gestione host.
2. Nella sezione Regioni di destinazione, seleziona le regioni in cui desideri implementare la configurazione della gestione host.

## Current account

Scegli una delle opzioni della regione e segui i passaggi corrispondenti.

## Regione attuale

Scegli come indirizzare solo le istanze nella regione corrente:

- Tutte le istanze: la configurazione di gestione host si rivolge automaticamente a tutti gli EC2 nella regione corrente.
- Tag: scegli Aggiungi e inserisci la chiave e il valore opzionale che vengono aggiunti alle istanze da destinare.
- Gruppo di risorse: per Gruppo di risorse, seleziona un gruppo di risorse esistente che contenga le istanze EC2 da destinare.
- Manuale: nella sezione Istanze, seleziona la casella di controllo di ogni istanza EC2 da destinare.

## Scegliere le regioni

Scegli come indirizzare le istanze nella regione specificata scegliendo una delle seguenti opzioni:

- Tutte le istanze: tutte le istanze nelle regioni specificate sono destinate.
- Tag: scegli Aggiungi e inserisci la chiave e il valore facoltativi che sono stati aggiunti alle istanze da destinare.

Nella sezione Regioni di destinazione, seleziona le regioni in cui desideri implementare la configurazione della gestione host.

## Come specificare un'opzione di profilo dell'istanza

- Solo intere organizzazioni e destinazioni personalizzate.

Nella sezione Opzioni del profilo dell'istanza, scegliere se aggiungere i criteri IAM richiesti ai profili dell'istanza esistenti collegati alle istanze oppure consentire a Quick Setup di creare i criteri IAM e i profili dell'istanza con le autorizzazioni necessarie per la configurazione scelta.

Dopo aver specificato tutte le scelte di configurazione, scegli Crea.

## Impostare la configurazione predefinita di gestione dell'host per un'organizzazione utilizzando Configurazione rapida

Con Quick Setup, puoi attivare la configurazione predefinita della gestione degli host per tutti gli account e le regioni che sono stati aggiunti alla tua organizzazione in AWS Organizations. Ciò garantisce che l'SSM Agent sia sempre aggiornato su tutte le istanze Amazon Elastic Compute Cloud (EC2) dell'organizzazione e che possa connettersi a Systems Manager.

### Prima di iniziare

Assicurati che siano soddisfatti i seguenti requisiti prima di abilitare questa impostazione.

- L'ultima versione di SSM Agent è già installata su tutte le istanze EC2 da gestire nell'organizzazione.
- Le istanze EC2 da gestire deve utilizzare la versione 2 del servizio di metadati delle istanze (IMDSv2).
- Hai effettuato l'accesso all'account di gestione della tua organizzazione, come specificato in AWS Organizations, utilizzando un'identità AWS Identity and Access Management (IAM) (utente, ruolo o gruppo) con autorizzazioni di amministratore.

### Uso del ruolo di gestione delle istanze EC2 predefinito

La configurazione di gestione host predefinita utilizza l'impostazione del servizio `default-ec2-instance-management-role` per Systems Manager. Si tratta di un ruolo con autorizzazioni che desideri rendere disponibili a tutti gli account dell'organizzazione per consentire la comunicazione tra l'istanza SSM Agent e il servizio Systems Manager nel cloud.

Se hai già impostato questo ruolo utilizzando il comando della CLI [update-service-setting](#), la configurazione di gestione host predefinita utilizza tale ruolo. Se non hai ancora impostato questo ruolo, Quick Setup lo creerà e lo applicherà per tuo conto.

Per verificare se questo ruolo è già stato specificato per la tua organizzazione, utilizza il comando [get-service-setting](#).

### Abilita gli aggiornamenti automatici di Agente SSM ogni due settimane

Utilizza la procedura seguente per abilitare l'opzione di configurazione predefinita della gestione dell'host per l'intera AWS Organizations organizzazione.

Per abilitare gli aggiornamenti automatici di Agente SSM ogni due settimane

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Quick Setup.
3. Nella scheda Configurazione di gestione host predefinita, scegli Crea.

 Tip

Se disponi già di una o più configurazioni nel tuo account, scegli prima la scheda Libreria o il pulsante Crea nella sezione Configurazioni per visualizzare le schede.

4. Nella sezione Opzioni di configurazione, seleziona Abilita gli aggiornamenti automatici di SSM Agent ogni due settimane.
5. Scegli Crea

Crea un AWS Config registratore di configurazione utilizzando Configurazione rapida

Con Quick Setup, puoi creare rapidamente un registratore di configurazione alimentato da AWS Config. Utilizza il registratore della configurazione per rilevare le modifiche alle configurazioni delle risorse e acquisire tali modifiche come elementi di configurazione. Se non hai familiarità con AWS Config, ti consigliamo di saperne di più sul servizio esaminando il contenuto della Guida per gli AWS Config sviluppatori prima di creare una configurazione con Quick Setup. Per ulteriori informazioni AWS Config, consulta [What is AWS Config?](#) nella Guida per AWS Config gli sviluppatori.

Per impostazione predefinita, il registratore di configurazione registra tutte le risorse supportate nel luogo in Regione AWS cui AWS Config è in esecuzione. È possibile personalizzare la configurazione in modo che vengano registrati solo i tipi di risorse specificati. Per ulteriori informazioni, consulta [Selezione delle risorse da AWS Config registrare](#) nella AWS Config Developer Guide.

Ti vengono addebitati i costi di utilizzo del servizio quando AWS Config inizia a registrare le configurazioni. Per informazioni sui prezzi, consulta [Prezzi di AWS Config](#).

 Note

Se hai già creato un registratore di configurazione, Quick Setup non interrompe la registrazione né apporta modifiche ai tipi di risorse che stai già registrando. Se scegli di registrare altri tipi di risorse utilizzando Quick Setup, il servizio li aggiunge ai

gruppi di registratori esistenti. Eliminazione del Quick Setup Registrazione di Config Il tipo di configurazione non interrompe il registratore di configurazione. Le modifiche continuano a essere registrate e vengono applicate le tariffe di utilizzo del servizio fino a quando non si arresta il registratore di configurazione. Per ulteriori informazioni sulla gestione del registratore di configurazione, consulta [Gestione del registratore della configurazione](#) nella AWS Config Guida per gli sviluppatori.

Per configurare AWS Config la registrazione, esegui le seguenti operazioni nella AWS Systems Manager console.

Per configurare AWS Config registrazione con Configurazione rapida

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Quick Setup.
3. Nella scheda Registrazione di Config, scegli Crea.

 Tip

Se hai già una o più configurazioni nel tuo account, scegli prima la scheda Libreria o il pulsante Crea nella sezione Configurazioni per visualizzare le schede.

4. Nella sezione Opzioni di configurazione, procedi come segue:
  - a. Per Scegli i tipi di AWS risorse da registrare, specifica se registrare tutte le risorse supportate o solo i tipi di risorse scelti.
  - b. Con Impostazione di consegna, è possibile specificare se creare un nuovo bucket Amazon Simple Storage Service (Amazon S3) o scegliere un bucket esistente a cui inviare snapshot di configurazione.
  - c. Per le opzioni di notifica, scegli l'opzione di notifica che preferisci. AWS Config utilizza Amazon Simple Notification Service (Amazon SNS) per notificarti AWS Config eventi importanti relativi alle tue risorse. Se scegli l'opzione Usa argomenti SNS esistenti, devi fornire l' Account AWS ID e il nome dell'argomento Amazon SNS esistente nell'account che desideri utilizzare. Se si sceglie come target più Regioni AWS, i nomi degli argomenti devono essere identici in ogni regione.

5. Nella Pianificazione, scegliere la frequenza con cui si desidera che Quick Setup corregga le modifiche apportate alle risorse diverse dalla configurazione. LaDefaultviene eseguita una volta. Se non vuoiQuick Setupper correggere le modifiche apportate alle risorse diverse dalla configurazione, scegliereDisabilita correzioneUNDERPersonalizza.
6. Nella sezione Targets (Destinazioni), è possibile scegliere una delle seguenti opzioni per identificare gli account e le regioni per la registrazione.

 Note

Quando viene utilizzato un singolo account, le opzioni per lavorare con organizzazioni e unità organizzative (UO) non sono disponibili. Puoi scegliere se applicare questa configurazione Regioni AWS a tutti gli elementi del tuo account o solo alle regioni selezionate.

- Entire organization (Tutta l'organizzazione): tutti gli account e le regioni dell'organizzazione.
  - Custom (Personalizzato): solo le unità organizzative e le regioni specificate.
    - Nella sezione dell'Unità organizzative di destinazione, è possibile selezionare le unità organizzative in cui desideri autorizzare la registrazione.
    - Nella sezione Target Regions (Regioni target), è possibile selezionare le regioni in cui desideri autorizzare la registrazione.
  - Current account (Account corrente): vengono scelte come destinazione solo le regioni specificate nell'account a cui si è attualmente connessi. Seleziona una delle seguenti opzioni:
    - Current Region (Regione corrente): vengono scelti come destinazione solo i nodi gestiti nella regione selezionata nella console.
    - Choose Regions (Scelta delle Regioni): scegli le singole regioni a cui applicare la configurazione di registrazione.
7. Scegli Crea.

## Implementazione AWS Config pacchetto di conformità utilizzando Configurazione rapida

Un pacchetto di conformità è un insieme di regole e azioni correttive AWS Config . Con Quick Setup, è possibile distribuire un pacchetto di conformità come singola entità in un account e uno Regione AWS attraverso un'organizzazione in AWS Organizations. Ciò consente di gestire la conformità

della configurazione delle AWS risorse su larga scala, dalla definizione delle policy all'audit e alla rendicontazione aggregata, utilizzando un framework e un modello di packaging comuni.

Per distribuire i pacchetti di conformità, esegui le seguenti attività nella console. AWS Systems Manager Quick Setup

 Note

È necessario abilitare AWS Config la registrazione prima di distribuire questa configurazione. Per ulteriori informazioni, consulta [Pacchetti di conformità](#) nella AWS Config Guida per gli sviluppatori.

Per distribuire i pacchetti di conformità con Configurazione rapida

1. Apri la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Quick Setup.
3. Nella scheda Pacchetti di conformità, scegli Crea.

 Tip

Se hai già una o più configurazioni nel tuo account, scegli prima la scheda Libreria o il pulsante Crea nella sezione Configurazioni per visualizzare le schede.

4. Nella sezione Scegli i pacchetti di conformità, scegli i pacchetti di conformità che desideri implementare.
5. Nella Pianificazione, scegliere la frequenza con cui si desidera che Quick Setup corregga le modifiche apportate alle risorse diverse dalla configurazione. La Default viene eseguita una volta. Se non vuoi Quick Setup per correggere le modifiche apportate alle risorse diverse dalla configurazione, scegli Disabilitato sotto Personalizza.
6. Nella sezione Target, scegli se distribuire i pacchetti di conformità all'intera organizzazione, ad alcuni Regioni AWS o all'account a cui hai attualmente effettuato l'accesso.

Se si sceglie **Intero organizzazione** Continuare con la fase 8.

Se si sceglie **Personalizza** Continuare con la fase 7.



7. Nella **Regioni** target selezionare le caselle di controllo delle Regioni in cui si desidera distribuire i pacchetti di conformità.
8. Scegli **Crea**.

Configurare l'applicazione di patch per le istanze in un'organizzazione utilizzando un'Configurazione rapida politica sulle patch

Con Quick Setup, puoi creare policy di patch basate su Patch Manager. Una policy di patch definisce la pianificazione e baseline da utilizzare quando si applicano automaticamente le patch alle istanze Amazon Elastic Compute Cloud (Amazon EC2) e ad altri nodi gestiti. Con una singola configurazione delle policy di patch, è possibile definire l'applicazione di patch per tutti gli account in tutte le Regioni AWS dell'organizzazione, per Regioni e account selezionati o per una singola coppia account-Regione. Per ulteriori informazioni sulle policy di patch, consulta [Configurazioni delle policy sulle patch in Configurazione rapida](#).

### Prerequisito

Per definire una policy di patch per un nodo tramite Quick Setup, il nodo deve essere un nodo gestito. Per ulteriori informazioni sulla gestione dei nodi, consulta la pagina [Configurazione della console unificata di Systems Manager per un'organizzazione](#).

#### Important

Metodi di scansione della conformità delle patch: Systems Manager supporta diversi metodi di scansione dei nodi gestiti al fine di verificare la conformità delle patch. Se implementi più metodi alla volta, le informazioni sulla conformità delle patch visualizzate rappresentano sempre il risultato della scansione più recente. I risultati delle scansioni precedenti vengono sovrascritti. Se i metodi di scansione utilizzano baseline delle patch diverse, con diverse regole di approvazione, le informazioni sulla conformità delle patch possono cambiare in modo imprevisto. Per ulteriori informazioni, consulta [Identificazione dell'esecuzione che ha creato i dati di conformità delle patch](#).

Stato di conformità dell'associazione e policy di patch: lo stato di applicazione di patch per un nodo gestito soggetto a una policy Quick Setup di patch corrisponde allo stato dell'esecuzione dell'associazione State Manager per quel nodo. Quando lo stato di esecuzione dell'associazione è **Compliant**, anche lo stato di applicazione di patch per il nodo gestito viene contrassegnato come **Compliant**. Quando lo stato di esecuzione

dell'associazione è Non-Compliant, anche lo stato di applicazione di patch per il nodo gestito viene contrassegnato come Non-Compliant.

## Regioni supportate per le configurazioni delle policy di patch

Le configurazioni delle policy di patch in Quick Setup sono attualmente supportate nelle seguenti regioni:

- Stati Uniti orientali (Ohio) (us-east-2)
- Stati Uniti orientali (Virginia settentrionale) (us-east-1)
- Stati Uniti occidentali (California settentrionale) (us-west-1)
- Stati Uniti occidentali (Oregon) (us-west-2)
- Asia Pacifico (Mumbai) (ap-south-1)
- Asia Pacifico (Seoul) (ap-northeast-2)
- Asia Pacifico (Singapore) (ap-southeast-1)
- Asia Pacifico (Sydney) (ap-southeast-2)
- Asia Pacifico (Tokyo) (ap-northeast-1)
- Canada (Centrale) (ca-central-1)
- Europa (Francoforte) (eu-central-1)
- Europa (Irlanda) (eu-west-1)
- Europa (Londra) (eu-west-2)
- Europa (Parigi) (eu-west-3)
- Europa (Stoccolma) (eu-north-1)
- Sud America (San Paolo) (sa-east-1)

## Autorizzazioni per il bucket S3 con policy di patch

Quando crei una policy di patch, Quick Setup crea un bucket Amazon S3 che contiene un file denominato `baseline_overrides.json`. Questo file memorizza le informazioni sulle baseline delle patch che hai specificato per la tua policy di patch.

Il nome del bucket S3 segue il formato `aws-quicksetup-patchpolicy-account-id-quick-setup-configuration-id`.

Ad esempio, `aws-quicksetup-patchpolicy-123456789012-abcde`

Se stai creando una policy di patch per un'organizzazione, il bucket viene creato nell'account di gestione dell'organizzazione.

Esistono due casi d'uso in cui è necessario fornire ad altre AWS risorse l'autorizzazione per accedere a questo bucket S3 utilizzando le politiche AWS Identity and Access Management (IAM):

- [Caso 1: utilizza il tuo profilo di istanza o il tuo ruolo di servizio con i tuoi nodi gestiti anziché quello fornito da Configurazione rapida](#)
- [Caso 2: utilizzo degli endpoint VPC per la connessione a Systems Manager](#)

La policy di autorizzazione necessaria in entrambi i casi si trova nella sezione in basso, [Autorizzazioni politiche per Configurazione rapida Bucket S3](#).

Caso 1: utilizza il tuo profilo di istanza o il tuo ruolo di servizio con i tuoi nodi gestiti anziché quello fornito da Configurazione rapida

Le configurazioni delle policy di patch includono un'opzione Aggiungi le policy IAM richieste ai profili dell'istanza esistenti collegati alle tue istanze.

Se non scegli questa opzione ma desideri applicare patch Quick Setup ai tuoi nodi gestiti utilizzando questa politica di patch, devi assicurarti che siano implementati quanto segue:

- La policy gestita IAM AmazonSSMManagedInstanceCore deve essere collegata al [profilo dell'istanza IAM](#) o al [ruolo di servizio IAM](#) utilizzato per fornire le autorizzazioni Systems Manager ai nodi gestiti.
- È necessario aggiungere le autorizzazioni per accedere al bucket di policy della patch come policy in linea per il profilo dell'istanza IAM o il ruolo di servizio IAM. È possibile fornire l'accesso con caratteri jolly a tutti i bucket `aws-quicksetup-patchpolicy` o solo al bucket specifico creato per la tua organizzazione o il tuo account, come mostrato negli esempi di codice precedenti.
- È necessario etichettare il profilo dell'istanza IAM o il ruolo di servizio IAM con la seguente coppia chiave-valore.

Key: `QSConfigId-quick-setup-configuration-id`, Value: `quick-setup-configuration-id`

*quick-setup-configuration-id* rappresenta il valore del parametro applicato allo AWS CloudFormation stack utilizzato nella creazione della configurazione della politica di patch. Per recuperare questo ID, procedi come segue:

1. Apri la CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
2. Seleziona il nome dello stack utilizzato per creare la policy di patch. Il nome è in un formato come StackSet-AWS-QuickSetup-PatchPolicy-LA-q4bkg-52cd2f06-d0f9-499e-9818-d887cEXAMPLE.
3. Scegli la scheda Parametri.
4. Nell'elenco Parametri, nella colonna Chiave, individua la chiave QSConfigurationId. Nella colonna Valore relativa alla riga corrispondente, individua l'ID di configurazione, ad esempio abcde.

In questo esempio, per applicare il tag al profilo dell'istanza o al ruolo di servizio, la chiave è QSConfigId-abcde e il valore è abcde.

Per informazioni sull'aggiunta di tag a un ruolo IAM, consulta [Tagging IAM roles](#) e [Managing tags on instance profiles \(AWS CLI o AWS API\)](#) nella IAM User Guide.

## Caso 2: utilizzo degli endpoint VPC per la connessione a Systems Manager

Se utilizzi endpoint VPC per connetterti a Systems Manager, la policy di endpoint VPC per S3 deve consentire l'accesso al bucket S3 della policy di patch di Quick Setup.

Per informazioni sull'aggiunta di autorizzazioni a una policy di endpoint VPC per S3, consulta [Controllo dell'accesso da endpoint VPC con policy di bucket](#) nella Guida per l'utente di Amazon S3.

## Autorizzazioni politiche per Configurazione rapida Bucket S3

È possibile fornire l'accesso con caratteri jolly a tutti i bucket aws-quicksetup-patchpolicy o solo al bucket specifico creato per la tua organizzazione o il tuo account. Per fornire le autorizzazioni necessarie per i due casi descritti di seguito, utilizza uno dei due formati.

### All patch policy buckets

JSON

```
{
```

```

"Version": "2012-10-17",
"Statement": [
 {
 "Sid": "AccessToAllPatchPolicyRelatedBuckets",
 "Effect": "Allow",
 "Action": "s3:GetObject",
 "Resource": "arn:aws:s3::aws-quicksetup-patchpolicy-*"
 }
]
}

```

## Specific patch policy bucket

### JSON

```

{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "AccessToMyPatchPolicyRelatedBucket",
 "Effect": "Allow",
 "Action": "s3:GetObject",
 "Resource": "arn:aws:s3::aws-quicksetup-patchpolicy-111122223333-quick-setup-configuration-id"
 }
]
}

```

#### Note

Dopo aver creato la configurazione della policy di patch, è possibile individuare il nome completo del tuo bucket nella console S3. Ad esempio, `aws-quicksetup-patchpolicy-123456789012-abcde`

ID casuali della baseline delle patch nelle operazioni relative alle policy delle patch

Le operazioni di applicazione delle patch per le politiche di patch utilizzano il `BaselineOverride` parametro nel documento `AWS-RunPatchBaseline` SSM Command.

Quando utilizzi AWS-RunPatchBaseline per applicare le patch al di fuori di una policy di patch, è possibile utilizzare BaselineOverride per specificare un elenco di baseline delle patch da utilizzare durante l'operazione che sono diverse dai valori predefiniti specificati. È possibile creare questo elenco in un file denominato `baseline_overrides.json` e aggiungerlo manualmente a un bucket Amazon S3 di tua proprietà, come spiegato in [Utilizzo del BaselineOverride parametro](#).

Per le operazioni di applicazione di patch basate su policy di patch, tuttavia, Systems Manager crea automaticamente un bucket S3 e vi aggiunge un file `baseline_overrides.json`. Quindi, ogni volta che Quick Setup esegue un'operazione di applicazione di patch (utilizzando lo strumento Run Command), il sistema genera un ID casuale per ogni baseline delle patch. Questo ID è diverso per ogni operazione di applicazione di patch basata su una policy di patch e la baseline delle patch che rappresenta non è memorizzata o accessibile all'utente nel suo account.

Di conseguenza, l'ID della baseline delle patch selezionata nella configurazione nei log di applicazione delle patch. Questo vale sia per le baseline delle patch AWS gestite che per le baseline delle patch personalizzate che potresti aver selezionato. L'ID di base riportato nel log è invece quello generato per la specifica operazione di applicazione di patch.

Inoltre, se tenti di visualizzare i dettagli in Patch Manager relativi a una baseline delle patch generata con un ID casuale, il sistema segnala che la baseline delle patch non esiste. Questo comportamento è previsto e può essere ignorato.

## Creazione di una policy di patch

Per creare una policy di patch, segui la procedura seguente nella console di Systems Manager.

Per creare una policy sulle patch con Configurazione rapida

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.

Se stai configurando l'applicazione di patch per un'organizzazione, assicurati di aver effettuato l'accesso al relativo account di gestione. Non è possibile configurare la policy utilizzando l'account amministratore delegato o un account membro.

2. Nel pannello di navigazione, scegli Quick Setup.
3. Nella scheda Patch Manager (Gestore patch), scegli Create (Crea).

 Tip

Se hai già una o più configurazioni nel tuo account, scegli prima la scheda Libreria o il pulsante Crea nella sezione Configurazioni per visualizzare le schede.

4. In Configuration name (Nome configurazione), immetti un nome per identificare la policy di patch.
5. Nella sezione Scanning and installation (Scansione e installazione), in Patch operation (Operazione di patch), scegli se la policy di patch deve eseguire l'operazione Scan (Scansione) o Scan and install (Esegui scansione e installa) sulle patch delle destinazioni specificate.
6. In Pianificazione della scansione, scegli Utilizza le impostazioni predefinite consigliate o Pianificazione di scansione personalizzata. La pianificazione predefinita della scansione eseguirà l'analisi delle destinazioni ogni giorno alle 01:00 UTC.
  - Se scegli Pianificazione di scansione personalizzata, seleziona Frequenza di scansione.
  - Se scegli Daily (Giornaliero), inserisci l'ora, in UTC, in cui desideri scansionare le destinazioni.
  - Se scegli Espressione Cron personalizzata, inserisci la pianificazione come Espressione Cron (). Per ulteriori informazioni sulla formattazione delle espressioni CRON per Systems Manager, consulta [Riferimento: espressioni Cron e della frequenza per Systems Manager](#).

Inoltre, seleziona Wait to scan targets until first CRON interval (Attendi per analizzare le destinazioni fino al primo intervallo CRON). Per impostazione predefinita, Patch Manager esegue immediatamente la scansione dei nodi non appena diventano destinazioni.
7. Se scegli Scansione e installazione (Esegui scansione e installa), seleziona la Installation schedule (Pianificazione dell'installazione) da utilizzare durante l'installazione delle patch per le destinazioni specificate. Se scegli Use recommended defaults (Usa le impostazioni predefinite consigliate), Patch Manager esegue l'installazione settimanale delle patch la domenica alle 02:00 UTC.
  - Se scegli Custom install schedule (Pianificazione dell'installazione personalizzata), seleziona la Installation Frequency (Frequenza di installazione).
  - Se scegli Daily (Giornaliero), inserisci l'ora, in UTC, in cui desideri installare gli aggiornamenti nelle destinazioni.
  - Se scegli Custom CRON Expression (Espressione CRON personalizzata), inserisci la pianificazione come CRON expression (Espressione CRON). Per ulteriori informazioni sulla formattazione delle espressioni CRON per Systems Manager, consulta [Riferimento: espressioni Cron e della frequenza per Systems Manager](#).

Inoltre, deseleziona Wait to install updates until first CRON interval (Attendi per installare gli aggiornamenti fino al primo intervallo CRON) per installare immediatamente gli aggiornamenti sui nodi non appena diventano destinazioni. Per impostazione predefinita, Patch Manager attende il primo intervallo CRON per installare gli aggiornamenti.

- Scegli Reboot if needed (Riavvia se necessario) per riavviare i nodi dopo l'installazione della patch. L'operazione di riavvio è consigliata, ma può causare problemi di disponibilità.
8. Nella sezione Baseline delle patch, scegli le baseline delle patch da utilizzare per la scansione e l'aggiornamento delle destinazioni.

Per impostazione predefinita, Patch Manager utilizza le baseline delle patch predefinite. Per ulteriori informazioni, consulta [Baseline predefinite](#).

Se scegli la baseline della patch personalizzata, modifica la baseline della patch selezionata per i sistemi operativi per i quali non desideri utilizzare una baseline di patch predefinita AWS .

#### Note

Quando utilizzi endpoint VPC per connetterti a Systems Manager, assicurati che la policy degli endpoint VPC per S3 consenta l'accesso a questo bucket S3. Per ulteriori informazioni, consulta [Autorizzazioni per il bucket S3 con policy di patch](#).

#### Important

Quando utilizzi una [configurazione della policy di patch](#) in Quick Setup, gli aggiornamenti apportati alle baseline delle patch personalizzate vengono sincronizzati con Quick Setup una volta ogni ora.

Quando si elimina una baseline delle patch personalizzata a cui si fa riferimento in una policy di patch, viene visualizzato un banner nella pagina Dettagli di configurazione di Quick Setup relativa alla policy di patch. Il banner informa che la policy di patch fa riferimento a una baseline delle patch che non esiste più, di conseguenza le successive operazioni di applicazione di patch avranno esito negativo. In questo caso, torna alla pagina Configurazioni di Quick Setup, seleziona la configurazione Patch Manager e scegli Operazioni, Modifica configurazione. Il nome della baseline delle patch eliminata viene evidenziato ed è necessario selezionare una nuova baseline delle patch per il sistema operativo interessato.



9. (Facoltativo) Nella sezione Archiviazione di log delle applicazioni di patch, seleziona **Scrivi output nel bucket S3** per archiviare i log delle operazioni di applicazione di patch in un bucket Amazon S3.

 **Note**

Se stai configurando una policy di patch per un'organizzazione, l'account di gestione dell'organizzazione deve disporre almeno di autorizzazioni di sola lettura per questo bucket. Tutte le unità organizzative incluse nella policy devono disporre dell'accesso in scrittura al bucket. Per informazioni sulla concessione dell'accesso al bucket a diversi account, consulta [Esempio 2: il proprietario del bucket concede autorizzazioni per il bucket multi-account](#) nella Guida per l'utente di Amazon Simple Storage Service.

10. Scegli **Sfoglia S3** per selezionare il bucket in cui desideri archiviare l'output del log delle patch. L'account di gestione deve disporre dell'accesso in lettura a questo bucket. Tutti gli account e le destinazioni non gestionali configurati nella sezione **Targets (Destinazioni)** devono disporre dell'accesso in scrittura al bucket S3 fornito per la registrazione.
11. Nella sezione **Targets (Destinazioni)**, scegli una delle seguenti opzioni per identificare gli account e le regioni interessate da questa operazione della policy di patch.

 **Note**

Quando viene utilizzato un singolo account, le opzioni per lavorare con organizzazioni e unità organizzative (UO) non sono disponibili. È possibile decidere di applicare questa configurazione a tutte le Regioni AWS dell'account o solo alle Regioni selezionate. Quando viene precedentemente specificata una regione di residenza per l'account senza aver effettuato l'onboarding alla nuova esperienza della console Quick Setup, non sarà possibile escludere tale regione dalla configurazione dei **Targets (Destinazioni)**.

- **Entire organization (Tutta l'organizzazione)**: tutti gli account e le regioni dell'organizzazione.
- **Custom (Personalizzato)**: solo le unità organizzative e le regioni specificate.
  - Nella sezione **Target OUs (Unità organizzative di destinazione)**, seleziona le unità organizzative per cui desideri configurare la policy di patch.
  - Nella sezione **Target Regions (Regioni target)**, seleziona le regioni in cui desideri applicare la policy di patch.

- **Current account (Account corrente):** vengono scelte come destinazione solo le regioni specificate nell'account a cui si è attualmente connessi. Seleziona una delle seguenti opzioni:
    - **Current Region (Regione corrente):** vengono scelti come destinazione solo i nodi gestiti nella regione selezionata nella console.
    - **Choose Regions (Scelta delle Regioni):** scegli le singole regioni a cui applicare la policy di patch.
12. In **Choose how you want to target instances (Scegli come vorresti indirizzare le istanze)**, scegli una delle opzioni seguenti per identificare i nodi a cui applicare la patch:
- **Tutti i nodi gestiti:** tutti i nodi gestiti nelle UO e nelle Regioni selezionate.
  - **Specify the resource group (Specifica il gruppo di risorse):** scegli il nome di un gruppo di risorse dall'elenco per indirizzare le risorse associate.

 **Note**

Attualmente, la selezione dei gruppi di risorse è supportata solo per le configurazioni di account singoli. Per applicare patch alle risorse in più account, scegli un'opzione di destinazione diversa.

- **Specify a node tag (Specifica il tag nodo):** l'applicazione di patch si applica solo ai nodi contrassegnati con la coppia chiave-valore specificata in tutti gli account e le regioni di destinazione.
- **Manual (Manuale):** scegli manualmente i nodi gestiti tra tutti gli account e le regioni specificati da un elenco.

 **Note**

Al momento, questa opzione supporta solo istanze Amazon EC2. Puoi aggiungere un massimo di 25 istanze manualmente in una configurazione di policy di patch.

13. Nella sezione **Rate control (Controllo velocità)** esegui le operazioni seguenti:

- In **Concurrency (Simultaneità)**, inserisci un numero o una percentuale di nodi su cui eseguire contemporaneamente la policy di patch.
- In **Error threshold (Soglia di errore)**, inserisci il numero o la percentuale di nodi in cui è possibile che si verifichi un errore prima che la policy di patch abbia esito negativo.

14. (Facoltativo) Seleziona la casella di controllo Aggiungi policy IAM richieste ai profili dell'istanza esistenti collegati alle istanze.

Questa selezione applica le policy IAM create da questa configurazione di Quick Setup ai nodi a cui è già associato un profilo dell'istanza (istanze EC2) o un ruolo di servizio (nodi attivati da sistemi ibridi). Questa selezione è consigliata quando i nodi gestiti dispongono già di un profilo dell'istanza o di un ruolo di servizio associato, ma non contengono tutte le autorizzazioni necessarie per l'utilizzo di Systems Manager.

La selezione è valida per i nodi gestiti creati successivamente negli account e nelle regioni a cui si applica questa configurazione della policy di patch.

 Important

Se non selezioni questa casella di controllo ma desideri che Quick Setup applichi le patch ai nodi gestiti utilizzando questa policy di patch, devi procedere come segue:

Aggiungi le autorizzazioni al [profilo dell'istanza IAM](#) o al [ruolo di servizio IAM](#) per accedere al bucket S3 creato per la policy di patch

Assegna un tag al profilo dell'istanza IAM o al ruolo di servizio IAM con una coppia chiave-valore specifica.

Per informazioni, consulta [Caso 1: utilizza il tuo profilo di istanza o il tuo ruolo di servizio con i tuoi nodi gestiti anziché quello fornito da Configurazione rapida](#).

15. Scegli Crea.

Per esaminare lo stato di applicazione di patch dopo la loro creazione, accedi alla configurazione dalla pagina [Quick Setup](#).

## Configura DevOps Guru usando Configurazione rapida

Puoi configurare rapidamente le opzioni DevOps Guru utilizzando. Quick Setup Amazon DevOps Guru è un servizio basato sull'apprendimento automatico (ML) che semplifica il miglioramento delle prestazioni operative e della disponibilità di un'applicazione. DevOpsGuru rileva comportamenti diversi dai normali schemi operativi in modo da poter identificare i problemi operativi molto prima che abbiano un impatto sui clienti. DevOpsGuru acquisisce automaticamente i dati operativi dalle tue AWS applicazioni e fornisce un'unica dashboard per visualizzare i problemi nei tuoi dati operativi. Puoi iniziare con DevOps Guru per migliorare la disponibilità e l'affidabilità delle applicazioni senza alcuna configurazione manuale o esperienza di apprendimento automatico.

La configurazione di DevOps Guru con Quick Setup è disponibile nei seguenti campi: Regioni AWS

- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti orientali (Ohio)
- Stati Uniti occidentali (Oregon)
- Europa (Francoforte)
- Europa (Irlanda)
- Europa (Stoccolma)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Tokyo)

Per informazioni sui prezzi, consulta i prezzi di [Amazon DevOps Guru](#).

Per configurare DevOps Guru, esegui le seguenti attività nella AWS Systems Manager Quick Setup console.

Per configurare DevOps Guru con Configurazione rapida

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Quick Setup.
3. Sulla scheda DevOps Guru, scegli Crea.

 Tip

Se hai già una o più configurazioni nel tuo account, scegli prima la scheda Libreria o il pulsante Crea nella sezione Configurazioni per visualizzare le schede.

4. Nelle Opzioni di configurazione, scegliere la sezione AWS Tipi di risorse che desideri analizzare e preferenze di notifica.

Se non selezioni l'opzione Analizza tutte le AWS risorse in tutti gli account della mia organizzazione, puoi scegliere AWS le risorse da analizzare in un secondo momento nella console DevOps Guru. DevOpsGuru analizza diversi tipi di AWS risorse (come i bucket Amazon Simple Storage Service (Amazon S3) e le istanze Amazon Elastic Compute Cloud (Amazon

EC2)), che sono suddivisi in due gruppi di prezzi. Paghi per il AWS ore risorsa analizzate, per ogni risorsa attiva. Una risorsa è attiva solo se produce parametri, eventi o voci di log entro un'ora. La tariffa addebitata per un tipo di risorsa specifico dipende dal gruppo di prezzi AWS .

Se selezioni l'opzione **Abilita notifiche SNS**, viene creato un argomento Amazon Simple Notification Service (Amazon SNS) Account AWS in ciascuna delle unità organizzative (OU) a cui ti rivolgi con la tua configurazione. DevOpsGuru utilizza l'argomento per informarti su importanti eventi dedicati a DevOps Guru, come la creazione di nuove informazioni. Se non abiliti questa opzione, puoi aggiungere un argomento in un secondo momento nella console DevOps Guru.

Se selezioni l' **AWS Systems Manager OpsItems** opzione **Abilita**, verranno creati elementi di lavoro operativi (OpsItems) per gli EventBridge eventi Amazon correlati e gli CloudWatch allarmi Amazon.

5. Nella Pianificazione, scegliere la frequenza con cui si desidera che Quick Setup corregga le modifiche apportate alle risorse diverse dalla configurazione. LaDefaultviene eseguita una volta. Se non vuoi Quick Setup per correggere le modifiche apportate alle risorse diverse dalla configurazione, scegli **Disabilitato** sotto **Personalizza**.
6. Nella sezione **Obiettivi**, scegli se consentire a DevOps Guru di analizzare le risorse in alcune delle tue unità organizzative (OU) o nell'account a cui sei attualmente connesso.

Se scegli **Personalizza**, continua con la fase 8.

Se si sceglie **Current account** (Account corrente), continuare con la fase 9.

7. Nelle sezioni **OU di Target** e **Regioni di Target**, seleziona le caselle di controllo delle OU e delle Regioni in cui desideri utilizzare DevOps Guru.
8. Scegli le regioni in cui desideri utilizzare DevOps Guru nell'account corrente.
9. Scegli **Create** (Crea).

Implementa i pacchetti Distributor tramite Quick Setup

Distributor è uno strumento in AWS Systems Manager. A Distributor è una raccolta di software o di asset installabili che possono essere distribuiti come una singola entità. Con Quick Setup, è possibile distribuire un Distributor pacchetto in un'azienda Regione AWS o Account AWS all'interno di un'organizzazione in AWS Organizations. Attualmente, è possibile distribuire solo l'agente EC2Launch v2, il pacchetto di utilità Amazon Elastic File System (Amazon EFS) e CloudWatch

l'agente Amazon. Quick Setup Per ulteriori informazioni su Distributor, consultare [AWS Systems Manager Distributor](#).

Per distribuire i Distributor pacchetti, esegui le seguenti attività nella console. AWS Systems Manager Quick Setup

Per distribuireDistributorPacchetti conQuick Setup

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Quick Setup.
3. Nella scheda Distributore, scegli Crea.

 Tip

Se hai già una o più configurazioni nel tuo account, scegli prima la scheda Libreria o il pulsante Crea nella sezione Configurazioni per visualizzare le schede.

4. NellaOpzioni di configurazione, selezionare il pacchetto che si desidera distribuire.
5. Nella sezione Destinazioni, scegli se implementare il pacchetto all'intera organizzazione, ad alcune unità organizzative (UO) o all'account a cui hai fatto attualmente l'accesso.

Se si sceglieIntero organizzazioneContinuare con la fase 8.

Se scegli Personalizza, continua con la fase 7.

6. Nella sezione UO di destinazione, seleziona le caselle di controllo delle UO e delle Regioni in cui si desidera implementare il pacchetto.
7. Scegli Create (Crea).

Arresta e avvia automaticamente le istanze EC2 in base a una pianificazione utilizzando Configurazione rapida

ConQuick Setup, puoi configurare Resource Scheduler per automatizzare l'avvio e l'arresto delle istanze Amazon Elastic Compute Cloud (Amazon EC2).

Questa configurazione di Quick Setup consente di ridurre i costi operativi avviando e interrompendo le istanze in base alla pianificazione specificata. Ciò consente di evitare costi superflui per l'esecuzione di istanze, quando non sono necessarie.

Ad esempio, attualmente potresti lasciare le tue istanze costantemente in esecuzione, anche se vengono utilizzate solo 10 ore al giorno per 5 giorni alla settimana. È possibile invece pianificare l'interruzione delle istanze ogni giorno dopo l'orario lavorativo, con un risparmio del 70% dal momento che il tempo di esecuzione si riduce da 168 ore a 50 ore. L'uso di Quick Setup non prevede alcun costo. Tuttavia, i costi possono essere addebitati in base alle risorse configurate e ai limiti di utilizzo senza costi per i servizi utilizzati per configurare il servizio.

Utilizzando Resource Scheduler, puoi scegliere di arrestare e avviare automaticamente le istanze su più Regioni AWS istanze e in base a una pianificazione definita. Account AWS La configurazione di Quick Setup è destinata alle istanze Amazon EC2 che utilizzano la chiave tag e il valore specificati. Solo le istanze con un tag corrispondente al valore specificato nella configurazione vengono interrotte o avviate da Pianificatore risorse. Tieni presente che se i volumi Amazon EBS collegati all'istanza sono crittografati, devi aggiungere le autorizzazioni richieste per la AWS KMS chiave al ruolo IAM affinché Resource Scheduler possa avviare l'istanza.

### Numero massimo di istanze per configurazione

Una configurazione singola supporta la pianificazione di un massimo di 5.000 istanze per Regione. Se necessiti di più di 5.000 istanze in una determinata Regione, devi creare più configurazioni. Assegna di conseguenza i tag alle istanze, in modo che ogni configurazione gestisca fino a 5.000 istanze. Durante la creazione di molteplici configurazioni di Quick Setup nel Pianificatore risorse, devi specificare valori di chiave di tag diversi. Ad esempio, una configurazione può utilizzare la chiave tag Environment con il valore Production, mentre un'altra utilizza Environment e Development.

### Comportamenti di pianificazione

I seguenti punti descrivono determinati comportamenti delle configurazioni di pianificazione:

- Pianificatore risorse avvia le istanze contrassegnate solo se si trovano nello stato Stopped. Allo stesso modo, le istanze vengono interrotte solo se si trovano nello stato running. Pianificatore risorse opera su un modello basato su eventi e avvia o arresta le istanze solo nei momenti specificati. Si supponga, ad esempio, di creare una pianificazione che avvia le istanze alle ore 09:00. Pianificatore risorse avvia tutte le istanze associate al tag specificato che si trovano nello stato Stopped alle 09:00. Se le istanze vengono interrotte manualmente in un secondo momento, Pianificatore risorse non le riavvierà per mantenere lo stato Running. Analogamente, se un'istanza viene avviata manualmente dopo essere stata interrotta in base alla pianificazione, Pianificatore risorse non interromperà nuovamente l'istanza.
- Se crei una pianificazione con un'ora di inizio successiva alle 24 ore rispetto all'ora di fine, la funzione Pianificazione risorse presuppone che le istanze vengano eseguite durante la notte. Si

supponga, ad esempio, di creare una pianificazione che avvia le istanze alle 21:00 e le interrompe alle 07:00. Pianificatore risorse avvia tutte le istanze associate al tag specificato che si trovano nello stato `Stopped` alle 21:00 e le interrompe alle 07:00 del giorno successivo. Per gli orari notturni, l'ora di inizio si applica ai giorni selezionati per la pianificazione. Tuttavia, l'orario di interruzione si applica al giorno successivo alla pianificazione.

- Quando crei una configurazione di pianificazione, lo stato corrente delle istanze potrebbe essere modificato per soddisfare i requisiti della pianificazione.

Ad esempio, supponiamo che oggi sia mercoledì e che tu specifichi una pianificazione per l'inizio delle istanze gestite alle 9:00 e l'interruzione alle 17:00 solo il martedì e il giovedì. Poiché l'ora corrente non rientra negli orari prescritti per l'esecuzione delle istanze, queste verranno interrotte dopo la creazione della configurazione. Le istanze non verranno rieseguite fino alla successiva ora prescritta, le 9:00 di giovedì.

Se le istanze sono attualmente in uno stato `Stopped` e si specifica una pianificazione in base alla quale verranno eseguite all'ora corrente, Pianificazione risorse le avvia dopo la creazione della configurazione.

Quando elimini la configurazione, le istanze non vengono più interrotte e avviate secondo la pianificazione precedentemente definita. In rari casi, le istanze potrebbero non interrompersi o avviarsi correttamente a causa di errori nelle operazioni API.

Per configurare la pianificazione per le istanze Amazon EC2, esegui le seguenti attività nella console AWS Systems Manager Quick Setup

Per configurare la pianificazione delle istanze con Configurazione rapida

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Quick Setup.
3. Nella scheda Pianificazione risorse, scegli Crea.

 Tip

Se hai già una o più configurazioni nel tuo account, scegli prima la scheda Libreria o il pulsante Crea nella sezione Configurazioni per visualizzare le schede.



4. Nella sezione Instance tag (Tag dell'istanza), specifica la chiave tag e il valore applicati alle istanze da associare alla pianificazione.
5. Nella sezione Schedule options (Opzioni di pianificazione), specifica il fuso orario, i giorni e gli orari in cui desideri avviare e interrompere le istanze.
6. Nella sezione Destinazioni, scegli se configurare la pianificazione per un gruppo Personalizzato di unità organizzative (UO) o per l'Account attuale a cui hai effettuato l'accesso:
  - Custom (Personalizzato): nella sezione Target OUs (Unità organizzative di destinazione), seleziona le unità organizzative in cui desideri configurare la pianificazione. Successivamente, nella sezione Target Regions (Regioni target), seleziona le regioni in cui desideri configurare la pianificazione.
  - Account corrente: seleziona Regione corrente o Scelta delle Regioni. Se hai selezionato Choose Regions (Scelta delle Regioni), scegli le Target Regions (Regioni target) in cui desideri configurare la pianificazione.
7. Verifica le informazioni relative alla pianificazione nella sezione Summary (Riepilogo).
8. Scegli Create (Crea).

## Configura Esploratore di risorse AWS utilizzo di Configurazione rapida

Con Quick Setup, puoi configurarlo rapidamente Esploratore di risorse AWS per cercare e scoprire risorse all'interno della tua organizzazione Account AWS o in un'intera AWS organizzazione. È possibile cercare le risorse utilizzando i metadati come nomi, tag e ID. Esploratore di risorse AWS fornisce risposte rapide alle query di ricerca utilizzando gli indici. Resource Explorer crea e gestisce indici utilizzando una varietà di fonti di dati per raccogliere informazioni sulle risorse nel tuo Account AWS.

Quick Setup per Resource Explorer automatizza il processo di configurazione dell'indice. Per ulteriori informazioni su Esploratore di risorse AWS, vedi [Che cos'è Esploratore di risorse AWS?](#) nella Guida Esploratore di risorse AWS per l'utente.

Durante Quick Setup, Resource Explorer esegue le seguenti operazioni:

- Crea un indice Regione AWS in ogni tuo file Account AWS.
- Aggiorna l'indice nella regione specificata come indice di aggregazione per l'account.
- Crea una vista predefinita nella regione dell'indice di aggregazione. Questa vista non ha filtri, quindi restituisce tutte le risorse trovate nell'indice.

## Autorizzazioni minime

Per eseguire le fasi della seguente procedura, è necessario avere le seguenti autorizzazioni:

- Azione: `resource-explorer-2:*` – Risorsa: nessuna risorsa specifica (\*)
- Azione: `iam:CreateServiceLinkedRole` – Risorsa: nessuna risorsa specifica (\*)

Per configurare Resource Explorer

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Quick Setup.
3. Nella scheda Resource Explorer, scegli Crea.
4. Nella sezione Regione dell'indice di aggregazione, scegli la regione in cui desideri contenere l'indice di aggregazione. È necessario selezionare la regione appropriata per la posizione geografica degli utenti.
5. (Facoltativo) Seleziona la casella di controllo Sostituisci gli indici di aggregazione esistenti in regioni diverse da quella selezionata sopra.
6. Nella sezione Destinazioni, scegli l'organizzazione di destinazione o le unità organizzative (UO) specifiche contenenti le risorse da scoprire.
7. Nella sezione Regioni, scegli quali regioni includere nella configurazione.
8. Rivedi il riepilogo della configurazione e scegli Create (Crea).

Nella pagina Resource Explorer, è possibile monitorare lo stato della configurazione.

## Risoluzione dei problemi Configurazione rapida results

Utilizza le informazioni seguenti per risolvere i problemi relativi a Quick Setup, uno strumento di AWS Systems Manager. Questo argomento include attività specifiche per risolvere i problemi in base al tipo di problema di Quick Setup.

Problema: implementazione non riuscita

Una distribuzione ha esito negativo se lo CloudFormation stack set ha esito negativo durante la creazione. Per esaminare un errore di implementazione, segui la seguente procedura:

1. Passare alla [console AWS CloudFormation](#).

2. Scegli lo stack creato dalla configurazione di Quick Setup. Stack name (Nome stack) include QuickSetup seguito dal tipo di configurazione scelto, ad esempio SSMHostMgmt.

 Note

CloudFormation a volte elimina le distribuzioni di stack non riuscite. Se lo stack non è disponibile nella tabella Stacks (Stack), scegli Deleted (Eliminato) dall'elenco dei filtri.

3. Controlla Status (Stato) e Status reason (Motivo dello stato). Per ulteriori informazioni sugli stati dello stack, consulta [Codici di stato dello stack](#) nella Guida per l'utente di AWS CloudFormation .
4. Per individuare il passaggio esatto non riuscito, controlla la scheda Events (Eventi) e rivedi lo Status (Stato) di ciascun evento.
5. Consulta la sezione [Risoluzione dei problemi](#) nella Guida per l'utente di AWS CloudFormation .
6. Se non riesci a risolvere l'errore di distribuzione utilizzando la procedura di CloudFormation risoluzione dei problemi, elimina la configurazione e riconfigurala.

#### Problema: associazione non riuscita

Se una delle associazioni ha riportato un errore durante la configurazione, nella tabella Configuration details (Dettagli configurazione) della pagina Configuration details (Dettagli configurazione) della configurazione in Configuration status (Stato configurazione) sarà visualizzato Failed (Non riuscito). Segui la seguente procedura per risolvere i problemi di un'associazione non riuscita.

1. Nella tabella Configuration details (Dettagli configurazione), scegli la configurazione non riuscita e quindi seleziona View Details (Visualizza dettagli).
2. Copia l'Association name (Nome associazione).
3. Vai a State Manager e incolla il nome dell'associazione nel campo di ricerca.
4. Scegliere l'associazione, quindi scegliere la scheda Execution history (Cronologia esecuzione).
5. In Execution ID (ID esecuzione), scegliere l'esecuzione dell'associazione non riuscita.
6. La pagina Association execution targets (Target di esecuzione dell'associazione) elenca tutti i nodi in cui è stata eseguita l'associazione. Scegliere il pulsante Output per un'esecuzione che non è stata eseguita.

7. Nella pagina Output, scegliere Step - Output (Fase - Output) per visualizzare il messaggio di errore per tale fase nell'esecuzione del comando. Ogni fase può visualizzare un messaggio di errore diverso. Esamina i messaggi di errore per tutte le fasi per risolvere il problema.

Se la visualizzazione dell'output della fase non aiuta a risolvere il problema, è possibile provare a ricreare l'associazione. Per ricreare l'associazione, elimina prima quella non riuscita in State Manager. Dopo aver eliminato l'associazione, modifica la configurazione e scegli l'opzione eliminata, quindi seleziona Update (Aggiorna).

#### Note

Per esaminare le associazioni con stato Failed (Non riuscito) per la configurazione di una Organization (Organizzazione), è necessario accedere all'account con l'associazione non riuscita e utilizzare la seguente procedura di associazione non riuscita descritta in precedenza. LaID associazionenon è un collegamento ipertestuale all'account di destinazione quando si visualizzano i risultati dall'account di gestione.

#### Problema: stato di deviazione

Quando si visualizza la pagina dei dettagli di una configurazione, è possibile visualizzare lo stato di deviazione di ciascuna implementazione. La deviazione della configurazione si verifica ogni volta che un utente apporta modifiche a un servizio o a funzionalità in conflitto con le selezioni effettuate tramite Quick Setup. Se un'associazione viene modificata dopo la configurazione iniziale, nella tabella viene visualizzata un'icona di avviso che indica il numero di elementi che sono stati deviati. È possibile determinare cosa ha causato la deviazione passando il mouse sull'icona.

Quando un'associazione viene eliminata in State Manager, le implementazioni correlate visualizzano un avviso di deviazione. Per risolvere questo problema, modifica la configurazione e scegli l'opzione che è stata rimossa quando l'associazione è stata eliminata. Scegli Update (Aggiorna) e attendi il completamento dell'implementazione.

## AWS Systems Manager strumenti applicativi

Gli strumenti applicativi sono una suite di funzionalità che consentono di gestire al meglio le applicazioni in esecuzione in AWS.

## Argomenti

- [AWS AppConfig](#)
- [AWS Systems Manager Application Manager](#)
- [AWS Systems Manager Parameter Store](#)

## AWS AppConfig

Le informazioni su sono state spostate in guide AWS AppConfig separate. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [AWS AppConfig Guida per l'utente](#)
- [AWS AppConfig Documentazione di riferimento delle API](#)

## AWS Systems Manager Application Manager

### Note

AWS Systems Manager Application Manager non è più aperto a nuovi clienti. Per funzionalità simili a AWS Systems Manager Application Manager, esplora le alternative [AWS Systems Manager Application Manager modifica della disponibilità](#).

Application Manager aiuta DevOps gli ingegneri a indagare e risolvere i problemi con AWS le loro risorse nel contesto delle loro applicazioni e dei cluster. Application Manager aggrega le informazioni operative provenienti da più strumenti Servizi AWS e Systems Manager in un unico strumento. Console di gestione AWS

In Application Manager, un'applicazione è un gruppo logico di AWS risorse che si desidera utilizzare come un'unità. Questo gruppo logico può rappresentare versioni diverse di un'applicazione, limiti di proprietà per operatori o ambienti per sviluppatori, per citarne alcuni. L'assistenza di Application Manager per i cluster container include sia i cluster di Amazon Elastic Kubernetes Service (Amazon EKS) che di Amazon Elastic Container Service (Amazon ECS).

La prima volta che si apre Application Manager, viene visualizzata la pagina Cosa Application Manager può fare per te. Quando scegli Inizia, importa Application Manager automaticamente i metadati sulle risorse che sono stati creati in altri strumenti Servizi AWS o in Systems Manager. Application Manager quindi visualizza tali risorse in un elenco raggruppato per categorie predefinite.

Per le Applicazioni, l'elenco include quanto segue:

- AWS CloudFormation pile
- applicazioni personalizzate;
- AWS Launch Wizard applicazioni
- AppRegistry applicazioni
- AWS applicazioni SAP Enterprise Workload
- Cluster Amazon ECS;
- Cluster Amazon EKS

Dopo aver [impostato](#) Servizi AWS e configurato gli strumenti di Systems Manager, Application Manager visualizza i seguenti tipi di informazioni sulle risorse:

- Informazioni sullo stato attuale e sullo stato di integrità di Amazon EC2 Auto Scaling per le istanze Amazon Elastic Compute Cloud (Amazon EC2) disponibili nell'applicazione
- Allarmi forniti da Amazon CloudWatch
- Informazioni sulla conformità fornite da AWS Config e State Manager (un componente di Systems Manager)
- Informazioni sul cluster Kubernetes fornite da Amazon EKS;
- Dati di registro forniti da AWS CloudTrail e Amazon CloudWatch Logs
- OpsItems fornito da Systems Manager OpsCenter
- Dettagli delle risorse forniti da Servizi AWS che li ospita.
- Informazioni sui cluster di container fornite da Amazon ECS.

Per risolvere i problemi relativi a componenti o risorse, Application Manager fornisce inoltre runbook che è possibile associare alle applicazioni. Per iniziare a utilizzare Application Manager, apri la [console di Systems Manager](#). Nel pannello di navigazione, scegli Application Manager.

## Quali sono i vantaggi dell'utilizzo Application Manager?

Application Manager riduce il tempo impiegato DevOps dagli ingegneri per rilevare e analizzare i problemi con AWS le risorse. A tale scopo, Application Manager visualizza molti tipi di informazioni operative nel contesto di un'applicazione in un'unica console. Application Manager riduce inoltre il

tempo necessario per risolvere i problemi fornendo runbook che eseguono attività di riparazione comuni sulle risorse. AWS

## Quali sono le caratteristiche di Application Manager?

Application Manager ha le funzionalità seguenti:

- Importa le tue AWS risorse automaticamente

Durante la configurazione iniziale, puoi scegliere di importare e visualizzare Application Manager automaticamente le risorse presenti nel tuo Account AWS sistema basate su CloudFormation stack, AWS Resource Groups implementazioni Launch Wizard, AppRegistry applicazioni e cluster Amazon ECS e Amazon EKS. Il sistema visualizza queste risorse in categorie di applicazioni o cluster predefinite. Successivamente, ogni volta che nuove risorse di questo tipo vengono aggiunte al tuo Account AWS, vengono visualizzate Application Manager automaticamente le nuove risorse nelle categorie predefinite di applicazioni e cluster.

- Crea o modifica CloudFormation stack e modelli

Application Manager ti aiuta a fornire e gestire le risorse per le tue applicazioni integrandoti con [CloudFormation](#). Puoi creare, modificare ed eliminare CloudFormation modelli e stack in. Application Manager include anche una libreria di modelli in cui è possibile clonare, creare e archiviare modelli. Application Manager CloudFormation visualizza le stesse informazioni sullo stato corrente di uno stack. I modelli e gli aggiornamenti dei modelli vengono archiviati in Systems Manager fino al provisioning dello stack, momento in cui vengono visualizzate anche le modifiche CloudFormation.

- Visualizzazione delle informazioni relative alle istanze nel contesto di un'applicazione

Application Manager si integra con Amazon Elastic Compute Cloud (Amazon EC2) per visualizzare informazioni relative alle istanze nel contesto di un'applicazione. Application Manager visualizza lo stato dell'istanza e lo stato di integrità di Amazon EC2 Auto Scaling per un'applicazione selezionata in un formato grafico. La scheda Istanze include inoltre una tabella con le seguenti informazioni per ogni istanza dell'applicazione.

- Stato dell'istanza (Pending [In attesa], Stopping [In arresto], Running [In esecuzione], Stopped [Arrestata])
- Stato ping per SSM Agent
- Stato e nome dell'ultimo runbook Automation Systems Manager elaborato nell'istanza
- Conteggio degli allarmi di Amazon CloudWatch Logs per stato.

- ALARM: il parametro o l'espressione non rientra nella soglia definita.
- OK: il parametro o l'espressione rientra nella soglia definita.
- INSUFFICIENT\_DATA: l'allarme è stato appena attivato, il parametro non è disponibile o la quantità di dati non è sufficiente affinché il parametro determini lo stato dell'allarme.
- Integrità del gruppo Auto Scaling per i gruppi padre e singoli
- Visualizzazione di parametri operativi e allarmi per un'applicazione o un cluster

Application Manager si integra con [Amazon CloudWatch](#) per fornire metriche operative e allarmi in tempo reale per un'applicazione o un cluster. È possibile esplorare la struttura delle applicazioni per visualizzare gli allarmi a livello di ciascun componente o visualizzare gli allarmi per un singolo cluster.

- Visualizzazione dei dati di log per un'applicazione

Application Manager si integra con [Amazon CloudWatch Logs](#) per fornire dati di registro nel contesto dell'applicazione senza dover uscire da Systems Manager.

- Visualizzazione e gestione di OpsItems per un'applicazione o un cluster

Application Manager si integra con [AWS Systems Manager OpsCenter](#) per fornire un elenco di elementi di lavoro operativi (OpsItems) per le applicazioni e i cluster. L'elenco riflette gli OpsItems generati automaticamente e creati manualmente. È possibile visualizzare i dettagli relativi alla risorsa che ha creato un OpsItem e lo stato, la fonte e la gravità dell'OpsItem.

- Visualizzazione dei dati di conformità delle risorse per un'applicazione o un cluster

Application Manager si integra con [AWS Config](#) per fornire dettagli relativi alla conformità e alla cronologia delle risorse di AWS in base alle regole specificate. Application Manager si integra anche con [AWS Systems Manager State Manager](#) per fornire informazioni di conformità sullo stato che si desidera mantenere per le istanze di Amazon Elastic Compute Cloud (Amazon EC2).

- Visualizzazione delle informazioni sull'infrastruttura cluster di Amazon ECS e Amazon EKS

Application Manager si integra con [Amazon ECS](#) e [Amazon EKS](#) per fornire informazioni sullo stato di integrità delle infrastrutture cluster e una visualizzazione del runtime (tempo di esecuzione) dei componenti delle risorse di calcolo, rete e archiviazione in un cluster.

Tuttavia, non è possibile gestire o visualizzare informazioni sulle operazioni relative ai pod o container o di Amazon EKS su Application Manager. È possibile gestire e visualizzare solo le informazioni sulle operazioni relative all'infrastruttura che ospita le risorse di Amazon EKS.



- Visualizzazione dei dettagli sui costi delle risorse per un'applicazione

Application Manager è integrato con AWS Cost Explorer, una funzionalità di Gestione costi e fatturazione AWS, tramite il widget Cost. Dopo aver abilitato Cost Explorer nella console di gestione fatturazione e costi, il widget Cost (Costi) in Application Manager mostra i dati di costo per una specifica applicazione o componente dell'applicazione non container. È possibile utilizzare i filtri nel widget per visualizzare i dati dei costi in base a diversi periodi di tempo, granularità e tipi di costo in grafici a barre o a linee.

- Visualizzazione di informazioni dettagliate sulle risorse in un'unica console

Scegli un nome di risorsa elencato su Application Manager e visualizza le informazioni contestuali e le informazioni sulle operazioni relative a tale risorsa senza dovere uscire da Systems Manager.

- Ricezione di aggiornamenti automatici per risorse e applicazioni

Se si apportano modifiche a una risorsa in una console di servizio e tale risorsa fa parte di un'applicazione su Application Manager, Systems Manager visualizza automaticamente tali modifiche. Ad esempio, se si aggiorna uno stack nella CloudFormation console e lo stack fa parte di un'Application Manager applicazione, gli aggiornamenti dello stack si riflettono automaticamente in Application Manager.

- Individuazione automatica delle applicazioni di Launch Wizard

Application Manager è integrato con [AWS Launch Wizard](#). Se è stato utilizzato Launch Wizard per implementare risorse per un'applicazione, Application Manager può importarli e visualizzarli automaticamente in una sezione di Launch Wizard.

- Monitora le risorse delle applicazioni in Application Manager ingresso utilizzando CloudWatch Application Insights

Application Manager si integra con Amazon CloudWatch Application Insights. Application Insights identifica e configura i log, i parametri chiave e gli allarmi tra le risorse dell'applicazione e stack tecnologico. Application Insights controlla in modo continuo i parametri e i log per rilevare e correlare anomalie ed errori. Quando il sistema rileva errori o anomalie, Application Insights genera CloudWatch eventi che puoi utilizzare per impostare notifiche o intraprendere azioni. È possibile abilitare e visualizzare Approfondimenti sulle applicazioni nelle schede Panoramica e Monitoraggio su Application Manager. Per ulteriori informazioni su Application Insights, consulta [What is Amazon CloudWatch Application Insights](#) nella Amazon CloudWatch User Guide.

- Risoluzione dei problemi relativi ai runbook

Application Manager include runbook predefiniti di Systems Manager per risolvere problemi comuni con le risorse. AWS Puoi eseguire un runbook su tutte le risorse di un'applicazione senza dover uscire da Application Manager.

## L'utilizzo è a pagamento Application Manager?

Application Manager è disponibile senza costi aggiuntivi.

## A cosa servono le quote delle risorse Application Manager?

È possibile visualizzare le quote per tutti gli strumenti di Systems Manager nella sezione [Service Quotas di Systems Manager](#) nella Riferimenti generali di Amazon Web Services. Salvo dove diversamente specificato, ogni quota si applica a una regione specifica.

## AWS Systems Manager Application Manager modifica della disponibilità

AWS Systems Manager Application Manager non è più aperto a nuovi clienti. SSM Application Manager è una funzionalità di console che consente ai DevOps team di definire o scoprire automaticamente le applicazioni, associare AWS risorse a tali applicazioni, applicare tag per la gestione delle risorse e monitorare lo stato delle applicazioni.

Fino a nuovo avviso, Application Manager i clienti SSM esistenti possono continuare a utilizzare il servizio normalmente con account esistenti. Durante questo periodo, AWS manterranno la disponibilità e le prestazioni del servizio e continueranno a offrire supporto tramite i canali di AWS supporto. AWS non aggiungerà nuove funzionalità né espanderà il servizio in nuove regioni.

Abbiamo identificato diverse alternative a SSM Application Manager a seconda del caso d'uso. AWS Console for SAP Applications, Tagging, AWS Resource Groups e AWS Resource Explorer sono disponibili senza costi aggiuntivi. Per i casi d'uso relativi all'osservabilità, Amazon CloudWatch Application Signals è un servizio a pagamento che include un livello gratuito.

### Alternative a Application Manager

#### AWS Console per applicazioni SAP

Se il tuo caso d'uso principale è la gestione HANA-based delle applicazioni SAP AWS, utilizza AWS Console for SAP Applications. Questa esperienza centralizzata offre una visualizzazione incentrata sulle applicazioni per registrare e gestire le applicazioni SAP in esecuzione su. HANA-based AWS La console offre un dashboard unificato per visualizzare le applicazioni SAP

registrate, comprendere la configurazione della zona di destinazione e ottenere visibilità sulle risorse consumate dai carichi di lavoro SAP. Dalla pagina dei dettagli dell'applicazione, puoi visualizzare la topologia dell'applicazione, le risorse associate ed eseguire operazioni, inclusa la convalida automatica e con riconoscimento delle applicazioni. start/stop Per saperne di più, consulta l'annuncio della [AWS Console for SAP Applications](#).

## Assegnazione di tag

Se il tuo caso d'uso principale è l'assegnazione di metadati alle risorse, aggiungi tag utilizzando chiavi di tag definite dal cliente (ad esempio, applicazione, progetto o carico di lavoro) al tuo account. Il tagging è la base su cui si AWS Systems Manager basa non solo, ma anche molti altri strumenti di AWS gestione (servizi come Resource Groups, Resource Explorer, Cost Explorer, CloudWatch, Config e Security Hub utilizzano tutti i tag per organizzare e filtrare le risorse). Stabilendo innanzitutto una strategia di tagging, si ottiene la flessibilità necessaria per adottare altre alternative nel tempo. Ad esempio, dopo aver taggato le risorse, puoi utilizzare i gruppi di risorse per creare un raggruppamento logico per le operazioni e la visibilità all'interno del tuo account e cercare le risorse contrassegnate in più regioni e tra account utilizzando AWS Resource Explorer. AWS Per saperne di più, consulta [Best practice per la codifica delle risorse. AWS](#)

## AWS Gruppi di risorse

Se il tuo caso d'uso principale è l'organizzazione e la gestione delle risorse, utilizza i gruppi di AWS risorse per stabilire raggruppamenti permanenti e denominati in base ai tag in una singola regione. I gruppi di risorse consentono di organizzare le risorse per applicazione, ambiente o qualsiasi altra categoria basata su tag, semplificando la gestione e il funzionamento dei carichi di lavoro. Per ulteriori informazioni, consulta la Guida per l'utente dei gruppi di [AWS risorse](#).

## AWS Esploratore di risorse

Se il tuo caso d'uso principale è l'individuazione delle risorse, utilizza AWS Resource Explorer per cercare e scoprire una raccolta di risorse per tag, per più regioni e per più account. Resource Explorer offre una visualizzazione unificata delle AWS risorse, consentendoti di cercare e filtrare per proprietà, tra cui tag, tipo di risorsa e regione. Per ulteriori informazioni, consulta la Guida [per l'utente di](#) AWS Resource Explorer.

## Mappa CloudWatch delle applicazioni Amazon Application Signals

Se il tuo caso d'uso principale è l'osservabilità a livello di applicazione, utilizza Amazon CloudWatch Application Signals per il rilevamento automatico delle applicazioni con supporto per più regioni e più account. Application Signals è un servizio a pagamento che include un livello gratuito e fornisce una visione completa dello stato, delle prestazioni e delle dipendenze dell'applicazione. Per saperne di più, consulta la Guida [per l'utente di](#) Application Signals.

 Note

I `awsApplication` tag e i gruppi di AppManager risorse creati tramite SSM Application Manager persistono a tempo indeterminato e possono continuare a essere utilizzati per il raggruppamento delle risorse, l'allocazione dei costi e il filtro. I clienti possono utilizzare i gruppi di AppManager risorse e i `awsApplication` tag esistenti in combinazione con le alternative consigliate (Resource Groups, Resource Explorer, Application Signals). Non è necessario rimuovere o sostituire questo tag come parte della transizione alla modalità di manutenzione.

## Domande frequenti

## È AWS Systems ManagerApplication Manager chiuso?

No, AWS Systems ManagerApplication Manager sta entrando in modalità manutenzione. AWS continuerà a mantenere la disponibilità del servizio e a offrire AWS supporto tramite i canali di assistenza. AWS non aggiungerà nuove funzionalità né estenderà il servizio ad altre regioni. A partire dal 30 luglio 2026, gli account che non sono stati utilizzati in precedenza non AWS Systems ManagerApplication Manager saranno più in grado di accedere al servizio; i clienti esistenti non sono interessati.

## Le mie AWS Systems ManagerApplication Manager applicazioni esistenti continueranno a funzionare?

Sì, AWS Systems ManagerApplication Manager le applicazioni esistenti continueranno a funzionare come oggi. Non vi è alcuna interruzione della configurazione corrente e non è richiesta alcuna azione da parte dell'utente. Nessuna API è interessata da questa modifica. Application Managerutilizza solo le API SSM esistenti.

## Quali alternative possono esplorare i clienti?

I clienti possono esplorare diverse alternative a seconda dei casi d'uso: AWS Console for SAP Applications, Tagging, AWS Resource Groups, Resource Explorer e, per i casi d'uso di osservabilità, Amazon CloudWatch Application Signals Application Map. AWS

## Esiste una strategia di tagging o una convenzione di denominazione delle chiavi consigliata per sostituire AWSApplication? AppManager

Non esiste un'unica chiave tag obbligatoria, che offre ai clienti la flessibilità di selezionare la propria chiave tag personalizzata per il loro caso d'uso. Le convenzioni più comuni includono

applicazioni, progetti o carichi di lavoro. I gruppi di AppManager risorse e i `awsApplication` tag rimangono utilizzabili anche per i clienti esistenti e non devono essere rimossi o sostituiti. Parallelamente al passaggio Application Manager alla modalità di manutenzione, `awsApplication` si passa anche alla modalità di manutenzione.

Se hai altre domande, contattaci tramite il Centro [AWS assistenza](#).

## Argomenti

- [Impostazione di servizi correlati](#)
- [Configurazione delle autorizzazioni per Systems Manager Application Manager](#)
- [Aggiunta di applicazioni e cluster di container ad Application Manager](#)
- [Utilizzo delle applicazioni](#)

## Impostazione di servizi correlati

Application Manager visualizza risorse e informazioni provenienti da altri strumenti Servizi AWS e da Systems Manager. Per massimizzare la quantità di informazioni sulle operazioni visualizzate su Application Manager, si consiglia di impostare e configurare questi altri servizi o strumenti prima dell'utilizzo di Application Manager.

## Argomenti

- [Impostazione delle attività per l'importazione di risorse](#)
- [Impostazione delle attività per visualizzare le informazioni sulle operazioni relative alle risorse](#)

## Impostazione delle attività per l'importazione di risorse

Le seguenti attività di configurazione consentono di visualizzare AWS le risorse in Application Manager. Al termine di ciascuna di queste attività, Systems Manager può importare automaticamente le risorse in Application Manager. Dopo aver importato le risorse, è possibile creare applicazioni su Application Manager e spostare le risorse importate in esse. In questo modo è possibile visualizzare le informazioni sulle operazioni nel contesto di un'applicazione.

(Facoltativo) Organizza AWS le tue risorse utilizzando i tag

Puoi assegnare metadati alle tue AWS risorse sotto forma di tag. Ogni tag è un'etichetta composta da una chiave e da un valore definiti dall'utente. Con i tag è possibile gestire,

identificare, organizzare, cercare e filtrare le risorse. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri.

(Facoltativo) Organizza le risorse utilizzando AWS [AWS Resource Groups](#)

È possibile utilizzare i gruppi di risorse per organizzare le AWS risorse. I gruppi di risorse semplificano la gestione, il monitoraggio e l'automatizzazione delle attività per numeri elevati di risorse per volta.

Application Manager importa automaticamente tutti i gruppi di risorse e li elenca nella categoria Custom applications (Applicazioni personalizzate).

(Facoltativo) Configura e distribuisce AWS le tue risorse utilizzando [AWS CloudFormation](#)

CloudFormation consente di creare e fornire implementazioni AWS dell'infrastruttura in modo prevedibile e ripetuto. Ti aiuta a utilizzare gli Servizi AWS , quali Amazon EC2, Amazon Elastic Block Store (Amazon EBS), Amazon Simple Notification Service (Amazon SNS), Elastic Load Balancing e AWS Auto Scaling. Con CloudFormation, puoi creare applicazioni affidabili, scalabili e convenienti nel cloud senza preoccuparti di creare e configurare l'infrastruttura sottostante. AWS

Application Manager importa automaticamente tutte le CloudFormation risorse e le elenca nella categoria stack. CloudFormation Puoi creare CloudFormation pile e modelli in. Application Manager Le modifiche allo stack e al modello vengono sincronizzate automaticamente tra e Application Manager. CloudFormation Inoltre, puoi creare applicazioni su Application Manager e spostarvi stack. In questo modo è possibile visualizzare le informazioni sulle operazioni per le risorse negli stack nel contesto di un'applicazione. Per informazioni sui prezzi, consultare [Prezzi di CloudFormation](#).

(Facoltativo) Configura e distribuisce le tue applicazioni utilizzando AWS Launch Wizard

Launch Wizard ti guida nel processo di dimensionamento, configurazione e distribuzione AWS delle risorse per applicazioni di terze parti senza la necessità di identificare e fornire manualmente le singole risorse. AWS

Application Manager importa automaticamente tutte le risorse di Launch Wizard e le elenca nella categoria Launch Wizard. Per ulteriori informazioni AWS Launch Wizard, vedere [Guida introduttiva a SQL Server. AWS Launch Wizard](#) Launch Wizard è disponibile senza costi aggiuntivi. I costi sono calcolati solo per le AWS risorse messe a disposizione per l'esecuzione della soluzione.

## (Facoltativo) Configurazione e implementazione delle applicazioni containerizzate utilizzando [Amazon ECS](#) e [Amazon EKS](#)

Amazon Elastic Container Service (Amazon ECS) è un servizio rapido e altamente scalabile di gestione dei container che semplifica l'eseguire, arrestare e gestire container in un cluster. I container sono definiti in una definizione di attività utilizzata per eseguire singoli processi o processi all'interno di un servizio.

Amazon EKS è un servizio gestito che aiuta a eseguire Kubernetes su AWS senza bisogno di installare, utilizzare e mantenere il proprio piano di controllo o nodi di Kubernetes. Kubernetes è un sistema open source per automatizzare l'implementazione, il dimensionamento e la gestione di applicazioni containerizzate.

Application Manager importa automaticamente tutte le risorse dell'infrastruttura Amazon ECS e Amazon EKS e le elenca nella scheda Container clusters (Cluster di container). Tuttavia, non è possibile gestire o visualizzare informazioni sulle operazioni relative ai pod o container o di Amazon EKS su Application Manager. È possibile gestire e visualizzare solo le informazioni sulle operazioni relative all'infrastruttura che ospita le risorse di Amazon EKS. Per informazioni sui prezzi, consulta [Prezzi di Amazon ECS](#) e [Prezzi di Amazon EKS](#).

Impostazione delle attività per visualizzare le informazioni sulle operazioni relative alle risorse

Le seguenti attività di impostazione consentono di visualizzare le informazioni sulle operazioni relative alle risorse di AWS su Application Manager.

(Consigliato) Verifica delle [autorizzazioni runbook](#)

È possibile risolvere i problemi con AWS le risorse di Application Manager utilizzando i runbook di Systems Manager Automation. Per utilizzare questo strumento di correzione, è necessario configurare o verificare le autorizzazioni. Per informazioni sui prezzi, consultare [Prezzi di AWS Systems Manager](#).

(Facoltativo) Abilita [Cost Explorer](#)

AWS Cost Explorer è una funzionalità AWS Cost Management che puoi utilizzare per visualizzare i dati sui costi per ulteriori analisi. Quando abiliti Cost Explorer, puoi visualizzare le informazioni sui costi, la cronologia dei costi e l'ottimizzazione dei costi per le risorse dell'applicazione nella console di Application Manager.



(Facoltativo) Imposta e configura i CloudWatch [log](#) e [gli allarmi di Amazon](#)

CloudWatch è un servizio di monitoraggio e gestione che fornisce dati e informazioni fruibili per applicazioni e risorse di AWS infrastruttura ibride e multicloud. Con CloudWatch, puoi raccogliere e accedere a tutti i tuoi dati operativi e prestazionali sotto forma di log e metriche da un'unica piattaforma. Per visualizzare CloudWatch i log e gli allarmi relativi alle risorse in Application Manager, è necessario configurarli e configurarli. CloudWatch Per informazioni sui prezzi, consultare [Prezzi di CloudWatch](#).

 Note

CloudWatch Il supporto per i log si applica solo alle applicazioni, non ai cluster.

(Facoltativo) Impostazione e configurazione di [AWS Config](#)

AWS Config fornisce una visione dettagliata delle risorse associate alle tue Account AWS, incluso come sono configurate, come sono correlate tra loro e come le configurazioni e le loro relazioni sono cambiate nel tempo. È possibile AWS Config utilizzarlo per valutare le impostazioni di configurazione delle AWS risorse. A tale scopo, è possibile creare AWS Config regole, che rappresentano le impostazioni di configurazione ideali. Pur AWS Config tenendo traccia continuamente delle modifiche alla configurazione che si verificano tra le risorse, verifica se tali modifiche violano una qualsiasi delle condizioni delle regole. Se una risorsa viola una regola, AWS Config contrassegna la risorsa e la regola come non conformi. Application Manager visualizza le informazioni sulla conformità sulle regole. AWS Config Per visualizzare questi dati in Application Manager, è necessario impostarli e configurarli AWS Config. Per informazioni sui prezzi, consultare [Prezzi di AWS Config](#).

(Opzionale) Creazione di [associazioni](#) di State Manager

È possibile utilizzare lo State Manager di Systems Manager per creare una configurazione da assegnare ai nodi gestiti. La configurazione, denominata associazione, definisce lo stato che si desidera mantenere nei propri nodi. Per visualizzare i dati di conformità delle associazioni su Application Manager, è necessario configurare uno o più associazioni di State Manager. State Manager è offerto senza alcun costo aggiuntivo.

(Facoltativo) Impostazione e configurazione di [OpsCenter](#)

È possibile visualizzare gli elementi di lavoro operativi (OpsItems) sulle tue risorse su Application Manager tramite OpsCenter. Puoi configurare Amazon CloudWatch e Amazon in modo che inviino automaticamente EventBridge OpsItems a OpsCenter in base ad allarmi ed eventi. È inoltre



possibile inserire OpsItems manualmente. Per informazioni sui prezzi, consultare [Prezzi di AWS Systems Manager](#).

## Configurazione delle autorizzazioni per Systems Manager Application Manager

Puoi utilizzare tutte le funzionalità Application Manager se la tua entità AWS Identity and Access Management (IAM) (ad esempio un utente, un gruppo o un ruolo) ha accesso alle operazioni API elencate in questo argomento. Le operazioni API sono separate in due tabelle per poter comprendere le diverse funzioni che svolgono.

La tabella seguente elenca le operazioni API chiamate da Systems Manager se si sceglie una risorsa su Application Manager, perché si desidera visualizzare i dettagli della risorsa. Ad esempio, se Application Manager elenca un gruppo di Amazon EC2 Auto Scaling e, se si sceglie quel gruppo per visualizzarne i dettagli, Systems Manager richiama le operazioni API di `autoscaling:DescribeAutoScalingGroups`. Se non si hanno gruppi Auto Scaling nel proprio account, questa operazione API non viene richiamata da Application Manager.

### Solo dettagli sulla risorsa

```
acm:DescribeCertificate
acm:ListTagsForCertificate
autoscaling:DescribeAutoScalingGroups
cloudfront:GetDistribution
cloudfront:ListTagsForResource
cloudtrail:DescribeTrails
cloudtrail:ListTags
cloudtrail:LookupEvents
codebuild:BatchGetProjects
codepipeline:GetPipeline
codepipeline:ListTagsForResource
dynamodb:DescribeTable
dynamodb:ListTagsOfResource
ec2:DescribeAddresses
ec2:DescribeCustomerGateways
ec2:DescribeHosts
ec2:DescribeInternetGateways
ec2:DescribeNetworkAcls
ec2:DescribeNetworkInterfaces
ec2:DescribeRouteTables
ec2:DescribeSecurityGroups
```

## Solo dettagli sulla risorsa

```
ec2:DescribeSubnets
ec2:DescribeVolumes
ec2:DescribeVpcs
ec2:DescribeVpnConnections
ec2:DescribeVpnGateways
elasticbeanstalk:DescribeApplications
elasticbeanstalk:ListTagsForResource
elasticloadbalancing:DescribeInstanceHealth
elasticloadbalancing:DescribeListeners
elasticloadbalancing:DescribeLoadBalancers
elasticloadbalancing:DescribeTags
iam:GetGroup
iam:GetPolicy
iam:GetRole
iam:GetUser
lambda:GetFunction
rds:DescribeDBClusters
rds:DescribeDBInstances
rds:DescribeDBSecurityGroups
rds:DescribeDBSnapshots
rds:DescribeDBSubnetGroups
rds:DescribeEventSubscriptions
rds:ListTagsForResource
redshift:DescribeClusterParameters
redshift:DescribeClusterSecurityGroups
redshift:DescribeClusterSnapshots
redshift:DescribeClusterSubnetGroups
redshift:DescribeClusters
s3:GetBucketTagging
```

La tabella seguente elenca le operazioni API utilizzate da Systems Manager per apportare modifiche alle applicazioni e risorse elencate su Application Manager o per visualizzare le informazioni sulle operazioni per un'applicazione o una risorsa selezionata.

## Azioni e dettagli dell'applicazione

```
applicationinsights:CreateApplication
applicationinsights:DescribeApplication
```

## Azioni e dettagli dell'applicazione

```
applicationinsights:ListProblems
ce:GetCostAndUsage
ce:GetTags
ce:ListCostAllocationTags
ce:UpdateCostAllocationTagsStatus
cloudformation:CreateStack
cloudformation>DeleteStack
cloudformation:DescribeStackDriftDetectionStatus
cloudformation:DescribeStackEvents
cloudformation:DescribeStacks
cloudformation:DetectStackDrift
cloudformation:GetTemplate
cloudformation:GetTemplateSummary
cloudformation:ListStacks
cloudformation:UpdateStack
cloudwatch:DescribeAlarms
cloudwatch:DescribeInsightRules
cloudwatch:DisableAlarmActions
cloudwatch:EnableAlarmActions
cloudwatch:GetMetricData
cloudwatch:ListTagsForResource
cloudwatch:PutMetricAlarm
config:DescribeComplianceByConfigRule
config:DescribeComplianceByResource
config:DescribeConfigRules
config:DescribeRemediationConfigurations
config:GetComplianceDetailsByConfigRule
config:GetComplianceDetailsByResource
config:GetResourceConfigHistory
config:ListDiscoveredResources
config:PutRemediationConfigurations
config:SelectResourceConfig
config:StartConfigRulesEvaluation
config:StartRemediationExecution
ec2:DescribeInstances
ecs:DescribeCapacityProviders
ecs:DescribeClusters
ecs:DescribeContainerInstances
ecs:ListClusters
ecs:ListContainerInstances
ecs:TagResource
eks:DescribeCluster
```

## Azioni e dettagli dell'applicazione

```
eks:DescribeFargateProfile
eks:DescribeNodegroup
eks:ListClusters
eks:ListFargateProfiles
eks:ListNodegroups
eks:TagResource
iam:CreateServiceLinkedRole
iam:ListRoles
logs:DescribeLogGroups
resource-groups:CreateGroup
resource-groups>DeleteGroup
resource-groups:GetGroup
resource-groups:GetGroupQuery
resource-groups:GetTags
resource-groups:ListGroupResources
resource-groups:ListGroups
resource-groups:Tag
resource-groups:Untag
resource-groups:UpdateGroup
s3:ListAllMyBuckets
s3:ListBucket
s3:ListBucketVersions
servicecatalog:GetApplication
servicecatalog:ListApplications
sns:CreateTopic
sns:ListSubscriptionsByTopic
sns:ListTopics
sns:Subscribe
ssm:AddTagsToResource
ssm:CreateDocument
ssm:CreateOpsMetadata
ssm>DeleteDocument
ssm>DeleteOpsMetadata
ssm:DescribeAssociation
ssm:DescribeAutomationExecutions
ssm:DescribeDocument
ssm:DescribeDocumentPermission
ssm:GetDocument
ssm:GetInventory
ssm:GetOpsMetadata
ssm:GetOpsSummary
ssm:GetServiceSetting
```

## Azioni e dettagli dell'applicazione

```
ssm:ListAssociations
ssm:ListComplianceItems
ssm:ListDocuments
ssm:ListDocumentVersions
ssm:ListOpsMetadata
ssm:ListResourceComplianceSummaries
ssm:ListTagsForResource
ssm:ModifyDocumentPermission
ssm:RemoveTagsFromResource
ssm:StartAssociationsOnce
ssm:StartAutomationExecution
ssm:UpdateDocument
ssm:UpdateDocumentDefaultVersion
ssm:UpdateOpsItem
ssm:UpdateOpsMetadata
ssm:UpdateServiceSetting
tag:GetTagKeys
tag:GetTagValues
tag:TagResources
tag:UntagResources
```

### Esempio di politica per tutti Application Manager autorizzazioni

Per configurare le autorizzazioni di Application Manager per entità IAM (ad esempio un utente, un gruppo o un ruolo), crea una policy IAM utilizzando l'esempio seguente. Questo esempio di policy include tutte le operazioni API utilizzate da Application Manager.

### JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "acm:DescribeCertificate",
 "acm:ListTagsForCertificate",
 "applicationinsights:CreateApplication",
```

```
"applicationinsights:DescribeApplication",
"applicationinsights:ListProblems",
"autoscaling:DescribeAutoScalingGroups",
"ce:GetCostAndUsage",
"ce:GetTags",
"ce:ListCostAllocationTags",
"ce:UpdateCostAllocationTagsStatus",
"cloudformation:CreateStack",
"cloudformation:DeleteStack",
"cloudformation:DescribeStackDriftDetectionStatus",
"cloudformation:DescribeStackEvents",
"cloudformation:DescribeStacks",
"cloudformation:DetectStackDrift",
"cloudformation:GetTemplate",
"cloudformation:GetTemplateSummary",
"cloudformation:ListStacks",
"cloudformation:ListStackResources",
"cloudformation:UpdateStack",
"cloudfront:GetDistribution",
"cloudfront:ListTagsForResource",
"cloudtrail:DescribeTrails",
"cloudtrail:ListTags",
"cloudtrail:LookupEvents",
"cloudwatch:DescribeAlarms",
"cloudwatch:DescribeInsightRules",
"cloudwatch:DisableAlarmActions",
"cloudwatch:EnableAlarmActions",
"cloudwatch:GetMetricData",
"cloudwatch:ListTagsForResource",
"cloudwatch:PutMetricAlarm",
"codebuild:BatchGetProjects",
"codepipeline:GetPipeline",
"codepipeline:ListTagsForResource",
"config:DescribeComplianceByConfigRule",
"config:DescribeComplianceByResource",
"config:DescribeConfigRules",
"config:DescribeRemediationConfigurations",
"config:GetComplianceDetailsByConfigRule",
"config:GetComplianceDetailsByResource",
"config:GetResourceConfigHistory",
"config:ListDiscoveredResources",
"config:PutRemediationConfigurations",
"config:SelectResourceConfig",
"config:StartConfigRulesEvaluation",
```

```
"config:StartRemediationExecution",
"dynamodb:DescribeTable",
"dynamodb:ListTagsOfResource",
"ec2:DescribeAddresses",
"ec2:DescribeCustomerGateways",
"ec2:DescribeHosts",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeVolumes",
"ec2:DescribeVpcs",
"ec2:DescribeVpnConnections",
"ec2:DescribeVpnGateways",
"ecs:DescribeCapacityProviders",
"ecs:DescribeClusters",
"ecs:DescribeContainerInstances",
"ecs:ListClusters",
"ecs:ListContainerInstances",
"ecs:TagResource",
"eks:DescribeCluster",
"eks:DescribeFargateProfile",
"eks:DescribeNodegroup",
"eks:ListClusters",
"eks:ListFargateProfiles",
"eks:ListNodegroups",
"eks:TagResource",
"elasticbeanstalk:DescribeApplications",
"elasticbeanstalk:ListTagsForResource",
"elasticloadbalancing:DescribeInstanceHealth",
"elasticloadbalancing:DescribeListeners",
"elasticloadbalancing:DescribeLoadBalancers",
"elasticloadbalancing:DescribeTags",
"iam:CreateServiceLinkedRole",
"iam:GetGroup",
"iam:GetPolicy",
"iam:GetRole",
"iam:GetUser",
"iam:ListRoles",
"lambda:GetFunction",
"logs:DescribeLogGroups",
```

```
"rds:DescribeDBClusters",
"rds:DescribeDBInstances",
"rds:DescribeDBSecurityGroups",
"rds:DescribeDBSnapshots",
"rds:DescribeDBSubnetGroups",
"rds:DescribeEventSubscriptions",
"rds:ListTagsForResource",
"redshift:DescribeClusterParameters",
"redshift:DescribeClusters",
"redshift:DescribeClusterSecurityGroups",
"redshift:DescribeClusterSnapshots",
"redshift:DescribeClusterSubnetGroups",
"resource-groups:CreateGroup",
"resource-groups>DeleteGroup",
"resource-groups:GetGroup",
"resource-groups:GetGroupQuery",
"resource-groups:GetTags",
"resource-groups:ListGroupResources",
"resource-groups:ListGroups",
"resource-groups:Tag",
"resource-groups:Untag",
"resource-groups:UpdateGroup",
"s3:GetBucketTagging",
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:ListBucketVersions",
"servicecatalog:GetApplication",
"servicecatalog:ListApplications",
"sns:CreateTopic",
"sns:ListSubscriptionsByTopic",
"sns:ListTopics",
"sns:Subscribe",
"ssm:AddTagsToResource",
"ssm:CreateDocument",
"ssm:CreateOpsMetadata",
"ssm>DeleteDocument",
"ssm>DeleteOpsMetadata",
"ssm:DescribeAssociation",
"ssm:DescribeAutomationExecutions",
"ssm:DescribeDocument",
"ssm:DescribeDocumentPermission",
"ssm:GetDocument",
"ssm:GetInventory",
"ssm:GetOpsMetadata",
```



```

 "ssm:GetOpsSummary",
 "ssm:GetServiceSetting",
 "ssm:ListAssociations",
 "ssm:ListComplianceItems",
 "ssm:ListDocuments",
 "ssm:ListDocumentVersions",
 "ssm:ListOpsMetadata",
 "ssm:ListResourceComplianceSummaries",
 "ssm:ListTagsForResource",
 "ssm:ModifyDocumentPermission",
 "ssm:RemoveTagsFromResource",
 "ssm:StartAssociationsOnce",
 "ssm:StartAutomationExecution",
 "ssm:UpdateDocument",
 "ssm:UpdateDocumentDefaultVersion",
 "ssm:UpdateOpsMetadata",
 "ssm:UpdateOpsItem",
 "ssm:UpdateServiceSetting",
 "tag:GetResources",
 "tag:GetTagKeys",
 "tag:GetTagValues",
 "tag:TagResources",
 "tag:UntagResources"
],
 "Resource": "*"
}
]
}

```

### Note

È possibile limitare la capacità di un utente di apportare modifiche alle applicazioni e alle risorse in Application Manager rimuovendo le operazioni API seguenti dalla policy di autorizzazione IAM collegata al relativo utente, gruppo o ruolo. La rimozione di queste operazioni crea un'esperienza in sola lettura su Application Manager. Di seguito sono elencate tutte le API che consentono agli utenti di apportare modifiche all'applicazione o a qualsiasi altra risorsa correlata.

```

applicationinsights:CreateApplication
ce:UpdateCostAllocationTagsStatus

```

```
cloudformation:CreateStack
cloudformation>DeleteStack
cloudformation:UpdateStack
cloudwatch:DisableAlarmActions
cloudwatch:EnableAlarmActions
cloudwatch:PutMetricAlarm
config:PutRemediationConfigurations
config:StartConfigRulesEvaluation
config:StartRemediationExecution
ecs:TagResource
eks:TagResource
iam:CreateServiceLinkedRole
resource-groups:CreateGroup
resource-groups>DeleteGroup
resource-groups:Tag
resource-groups:Untag
resource-groups:UpdateGroup
sns:CreateTopic
sns:Subscribe
ssm:AddTagsToResource
ssm:CreateDocument
ssm:CreateOpsMetadata
ssm>DeleteDocument
ssm>DeleteOpsMetadata
ssm:ModifyDocumentPermission
ssm:RemoveTagsFromResource
ssm:StartAssociationsOnce
ssm:StartAutomationExecution
ssm:UpdateDocument
ssm:UpdateDocumentDefaultVersion
ssm:UpdateOpsMetadata
ssm:UpdateOpsItem
ssm:UpdateServiceSetting
tag:TagResources
tag:UntagResources
```

Per informazioni sulla creazione e sulla modifica di policy IAM, consultare [Creazione di policy IAM](#) nella Guida per l'utente di IAM. Per informazioni su come assegnare questa policy a un'entità IAM (come un utente, un gruppo o un ruolo), consulta la pagina [Aggiunta e rimozione di autorizzazioni per le identità IAM](#).

## Aggiunta di applicazioni e cluster di container ad Application Manager

Application Manager è un componente di AWS Systems Manager. In Application Manager, un'applicazione è un gruppo logico di AWS risorse che si desidera utilizzare come unità. Questo gruppo logico può rappresentare versioni diverse di un'applicazione, limiti di proprietà per operatori o ambienti sviluppatore, per citarne alcuni.

La prima volta che si apre Application Manager, viene visualizzata la pagina Cosa Application Manager può fare per te. Quando si sceglie Nozioni di base, Application Manager vengono importati automaticamente i metadati relativi alle risorse create in altri Servizi AWS o strumenti di Systems Manager. Application Manager, quindi, visualizza tali risorse in un elenco raggruppato per categorie predefinite.

Per le Applicazioni, l'elenco include quanto segue:

- AWS CloudFormation pile
- applicazioni personalizzate;
- AWS Launch Wizard applicazioni
- AppRegistry applicazioni
- AWS applicazioni SAP Enterprise Workload
- Cluster Amazon ECS;
- Cluster Amazon EKS.

Al termine dell'importazione, è possibile visualizzare le informazioni sulle operazioni relative a un'applicazione o a una risorsa specifica in queste categorie predefinite. In alternativa, se si desidera fornire più contesto su una raccolta di risorse, è possibile creare manualmente un'applicazione su Application Manager. È quindi possibile aggiungere risorse o gruppi di risorse in tale applicazione. Dopo aver creato un'applicazione su Application Manager, è possibile visualizzare le informazioni sulle operazioni relative alla risorsa nel contesto di un'applicazione.

### Creazione di un'applicazione su Application Manager

Utilizza la procedura seguente per creare un'applicazione su Application Manager e aggiungere risorse a quell'applicazione.

## Per creare un'applicazione in Application Manager

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Application Manager.
3. Scegli Crea applicazione.
4. Scegli un'opzione dall'elenco a discesa e completa i campi nella pagina visualizzata.

## Utilizzo delle applicazioni

Application Manager è un componente di AWS Systems Manager. Questa sezione include argomenti con cui è possibile utilizzare le applicazioni di Application Manager e a visualizzare le informazioni sulle operazioni relative alle risorse di AWS .

### Indice

- [Panoramica delle applicazioni in Application Manager](#)
- [Gestione delle istanze EC2 delle applicazioni](#)
- [Visualizzazione delle risorse associate all'applicazione](#)
- [Gestione della conformità delle applicazioni](#)
- [Utilizzo di CloudWatch Application Insights per monitorare un'applicazione](#)
- [Visualizzazione OpsItems per un'applicazione](#)
- [Gestione dei log delle applicazioni](#)
- [Utilizza i runbook Automation per correggere i problemi delle applicazioni](#)
- [Aggiungi tag alle risorse in Application Manager](#)
- [Lavorare con CloudFormation modelli e impilabili Application Manager](#)
- [Lavorare con i cluster in Application Manager](#)

## Panoramica delle applicazioni in Application Manager

In Application Manager, un componente di AWS Systems Manager, la scheda Overview mostra un riepilogo degli CloudWatch allarmi di Amazon, degli elementi di lavoro operativi (OpsItems), di CloudWatch Application Insights e della cronologia dei runbook. Scegli Visualizza tutto per qualsiasi scheda per aprire la scheda corrispondente in cui è possibile visualizzare tutte le informazioni sull'applicazione, gli allarmi, OpsItems o la cronologia dei runbook.

## Informazioni su Application Insights

CloudWatch Application Insights identifica e configura metriche, log e allarmi chiave tra le risorse applicative e lo stack tecnologico. Application Insights controlla in modo continuo i parametri e i log per rilevare e correlare anomalie ed errori. Quando il sistema rileva errori o anomalie, Application Insights genera CloudWatch eventi che è possibile utilizzare per impostare notifiche o intraprendere azioni. Se scegli il pulsante Modifica configurazione nella scheda Monitoraggio, il sistema apre la console di CloudWatch Application Insights. Per ulteriori informazioni su Application Insights, consulta [What is Amazon CloudWatch Application Insights](#) nella Amazon CloudWatch User Guide.

## Informazioni su Cost Explorer

Application Manager è integrato con AWS Cost Explorer, una funzionalità di [AWS Cost Management](#), tramite il widget Costo e la scheda Costo. Dopo aver abilitato Cost Explorer nella console di Gestione dei costi, il widget Costi nella scheda Costi in Application Manager mostra i dati di costo per una specifica applicazione o componente di applicazione non container. È possibile utilizzare i filtri nel widget o la scheda per visualizzare i dati dei costi in base a diversi periodi di tempo, livelli di granularità e tipi di costo in un grafico a barre o a linee.

È possibile abilitare questa funzionalità scegliendo il pulsante Vai alla console di gestione dei AWS costi. Per impostazione predefinita, i dati vengono filtrati negli ultimi tre mesi. Per un'applicazione non container, se si sceglie il tasto Visualizza tutto in questa sezione, Application Manager aprirà la scheda Risorse. Per le applicazioni container, il tasto Visualizza tutto aprirà la console AWS Cost Explorer .

## Operazioni che è possibile eseguire in questa pagina

Puoi attivare e accedere alle informazioni sui seguenti widget nella scheda Panoramica di questa pagina. Quando un widget è abilitato, scegli Visualizza tutto per visualizzare i dettagli dell'applicazione specifici per quell'area.

- Nella sezione Approfondimenti e allarmi, scegli un numero del livello di gravità per aprire la scheda Monitoraggio, all'interno della quale puoi visualizzare maggiori dettagli sugli allarmi della gravità scelta.
- Nella sezione Costo, scegli Visualizza tutto per aprire la scheda Risorse e visualizzare i dati di costo per un'applicazione o per un componente specifico.
- Nella sezione Conformità, scegli Visualizza tutto per aprire la scheda Conformità, in cui puoi visualizzare le informazioni sulla conformità AWS Config e State Manager le associazioni.

 Note

Per visualizzare i dettagli di conformità delle patch, scegli direttamente la scheda Conformità. Puoi quindi visualizzare i dettagli di conformità delle patch per i nodi gestiti utilizzati dall'applicazione selezionata.

- Nella sezione Runbook, scegliere un runbook per aprirlo nella pagina Documenti di Systems Manager in cui è possibile visualizzare ulteriori dettagli sul documento.
- Nella OpsItemssezione, scegli una severità per aprire la OpsItemsscheda in cui puoi visualizzare tutta OpsItems la severità scelta.
- Scegliere un pulsante Visualizza tutto per aprire la scheda corrispondente. È possibile visualizzare tutti gli allarmi o OpsItems le voci della cronologia del runbook dell'applicazione.

Per aprire la scheda Panoramica

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Application Manager.
3. Nella sezione Applicazioni, scegli una categoria. Se si desidera aprire un'applicazione creata manualmente in Application Manager, scegliere Applicazioni personalizzate.
4. Scegli l'applicazione nell'elenco. Application Manager apre la scheda Panoramica.

Gestione delle istanze EC2 delle applicazioni

Application Manager si integra con Amazon Elastic Compute Cloud (Amazon EC2) per visualizzare informazioni relative alle istanze nel contesto di un'applicazione. Application Manager visualizza lo stato dell'istanza e lo stato di integrità di Dimensionamento automatico Amazon EC2 per un'applicazione selezionata in un formato grafico. La scheda Istanze include inoltre una tabella con le seguenti informazioni per ogni istanza dell'applicazione:

- Stato dell'istanza (Pending [In attesa], Stopping [In arresto], Running [In esecuzione], Stopped [Arrestata])
- Stato ping per SSM Agent
- Stato e nome del runbook più recente di Automazione Systems Manager elaborato nell'istanza
- Un numero di allarmi Amazon CloudWatch Logs per stato.

- **ALARM:** il parametro o l'espressione non rientra nella soglia definita.
- **OK:** il parametro o l'espressione rientra nella soglia definita.
- **INSUFFICIENT\_DATA:** l'allarme è stato appena attivato, il parametro non è disponibile o la quantità di dati non è sufficiente affinché il parametro determini lo stato dell'allarme.
- Integrità del gruppo Auto Scaling per i gruppi padre e singoli

Se scegli un'istanza nella tabella All instances (Tutte le istanze), Application Manager mostra le relative informazioni in quattro schede:

- **Details (Dettagli):** tutti i dettagli dell'istanza Amazon EC2, tra cui Amazon Machine Image (AMI), informazioni sul DNS, informazioni sull'indirizzo IP e altro ancora.
- **Health (Integrità):** lo stato attuale fornito dai controlli sullo stato del sistema EC2 e delle istanze.
- **Cronologia delle esecuzioni:** log di esecuzione per i runbook di automazione Systems Manager e le chiamate API elaborate dall'istanza.
- **CloudWatch allarmi:** il nome, lo stato e altro per tutti gli CloudWatch allarmi generati dall'istanza.

Operazioni che è possibile eseguire in questa pagina

In questa pagina è possibile eseguire le seguenti operazioni:

- Avviare, interrompere e terminare le istanze.
- Applica una ricetta Chef.
- Collegare o scollegare le istanze da un gruppo Auto Scaling.
- Abilita gli aggiornamenti automatici per SSM Agent.

Per aprire la scheda Instances (Istanze)

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Application Manager.
3. Nella sezione Applicazioni, scegli una categoria. Se vuoi aprire un'applicazione creata manualmente in Application Manager, scegli Applicazioni personalizzate.
4. Scegliere l'applicazione nell'elenco. Application Manager apre la scheda Panoramica.
5. Selezionare la scheda Instances (Istanze).

## Visualizzazione dei dettagli dell'applicazione

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Application Manager.
3. Nella sezione Applicazioni, scegli una categoria. Se vuoi aprire un'applicazione creata manualmente in Application Manager, scegli Applicazioni personalizzate.
4. Scegliere l'applicazione nell'elenco. Application Manager apre la scheda Panoramica.
5. Selezionare la scheda Instances (Istanze).
6. Scegli il pulsante accanto all'istanza di cui desideri visualizzare i dettagli.
7. Controlla i dettagli dell'istanza nella parte inferiore della pagina.

## Per aggiornare automaticamente SSM Agent

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Application Manager.
3. Nella sezione Applicazioni, scegli una categoria. Se vuoi aprire un'applicazione creata manualmente in Application Manager, scegli Applicazioni personalizzate.
4. Scegliere l'applicazione nell'elenco. Application Manager apre la scheda Panoramica.
5. Selezionare la scheda Instances (Istanze).
6. Nel menu a discesa Operazioni dell'agente, scegli Configura aggiornamento di SSM Agent.
7. Scegli Tutte le istanze per configurare gli aggiornamenti automatici di SSM Agent per tutte le istanze gestite. In alternativa, scegli Istanza per configurare gli aggiornamenti di SSM Agent di automazione per una singola istanza dell'applicazione.
8. Seleziona l'interruttore Abilita aggiornamento automatico.
9. Nel menu a discesa Specifica la pianificazione, scegli la pianificazione che desideri utilizzare per gli aggiornamenti di SSM Agent.
10. Selezionare Configura.

## Visualizzazione delle risorse associate all'applicazione

In Application Manager, un componente di AWS Systems Manager, la scheda Risorse mostra le AWS risorse dell'applicazione. Se si sceglie un componente di primo livello, questa pagina visualizza tutte



le risorse per tale componente e gli eventuali sottocomponenti. Se si sceglie un sottocomponente, questa pagina mostra solo le risorse assegnate a tale sottocomponente.

Operazioni che è possibile eseguire in questa pagina

In questa pagina è possibile eseguire le seguenti operazioni:

- Scegli il nome di una risorsa per visualizzarne le informazioni, inclusi i dettagli forniti dalla console in cui è stata creata, i tag, gli CloudWatch allarmi Amazon, AWS Config i dettagli e le informazioni di AWS CloudTrail registro.
- Scegliere il pulsante di opzione accanto al nome di una risorsa. Quindi, scegli il pulsante Resource timeline per aprire la AWS Config console in cui puoi visualizzare le informazioni sulla conformità relative a una risorsa selezionata.
- Se abilitata AWS Cost Explorer, la sezione Cost Explorer mostra i dati sui costi per una specifica applicazione o componente dell'applicazione non contenitore. È possibile abilitare questa funzionalità scegliendo il pulsante Vai alla console di gestione dei AWS costi. Utilizza i filtri in questa sezione per visualizzare le informazioni sui costi della tua applicazione.

Per aprire la scheda Risorse

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Application Manager.
3. Nella sezione Applicazioni, scegli una categoria. Se si desidera aprire un'applicazione creata manualmente in Application Manager, scegliere Applicazioni personalizzate.
4. Scegliere l'applicazione nell'elenco. Application Manager apre la scheda Overview (Panoramica).
5. Scegli la scheda Risorse.

Gestione della conformità delle applicazioni

In Application Manager, un componente di AWS Systems Manager, la pagina Configurazioni visualizza informazioni sulla conformità [AWS Config](#) delle risorse e delle regole di configurazione. Questa pagina mostra anche informazioni sulla conformità delle AWS Systems Manager [State Manager](#) associazioni. È possibile scegliere una risorsa, una regola o un'associazione per aprire la console corrispondente per ulteriori informazioni. Questa pagina visualizza le informazioni sulla conformità degli ultimi 90 giorni.

## Operazioni che è possibile eseguire in questa pagina

In questa pagina è possibile eseguire le seguenti operazioni:

- Scegli il nome di una risorsa per aprire la AWS Config console in cui è possibile visualizzare le informazioni sulla conformità relative a una risorsa selezionata.
- Scegliere il pulsante di opzione accanto al nome di una risorsa. Quindi, scegli il pulsante Cronologia delle risorse per aprire la AWS Config console in cui puoi visualizzare le informazioni sulla conformità relative a una risorsa selezionata.
- Nella sezione Config conformità alle regole è possibile eseguire le seguenti operazioni:
  - Scegli il nome di una regola per aprire la AWS Config console in cui puoi visualizzare le informazioni su quella regola.
  - Scegli Aggiungi regole per aprire la AWS Config console in cui puoi creare una regola.
  - Scegli il pulsante di opzione accanto al nome di una regola, scegliere Operazioni e quindi scegli Gestisci correzione per modificare l'azione di correzione per una regola.
  - Scegli il pulsante di opzione accanto al nome di una regola, scegli Azioni, quindi scegli Re-evaluatedi AWS Config eseguire un controllo di conformità sulla regola selezionata.
- Nella sezione Conformità delle associazioni è possibile eseguire le seguenti operazioni:
  - Scegli un nome di associazione per aprire la pagina Associazioni in cui è possibile visualizzare le informazioni relative a tale associazione.
  - Scegli Crea associazione per aprire State Manager di Systems Manager in cui è possibile creare un'associazione.
  - Scegli il pulsante di opzione accanto al nome di un'associazione e scegli Applica associazione per avviare immediatamente tutte le operazioni specificate nell'associazione.

## Apri la scheda Conformità

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Application Manager.
3. Nella sezione Applicazioni, scegli una categoria. Se si desidera aprire un'applicazione creata manualmente in Application Manager, scegliere Applicazioni personalizzate.
4. Scegli l'applicazione nell'elenco. Application Manager apre la scheda Panoramica.
5. Scegli la scheda Conformità.

## Utilizzo di CloudWatch Application Insights per monitorare un'applicazione

In Application Manager, un componente di AWS Systems Manager, la scheda Monitoraggio mostra Amazon CloudWatch Application Insights e i dettagli degli allarmi per le risorse in un'applicazione.

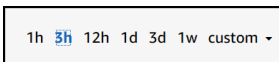
### Informazioni su Application Insights

CloudWatch Application Insights identifica e imposta le metriche, i log e gli allarmi chiave nelle risorse applicative e nello stack tecnologico. Application Insights controlla in modo continuo i parametri e i log per rilevare e correlare anomalie ed errori. Quando il sistema rileva errori o anomalie, Application Insights genera CloudWatch eventi che puoi utilizzare per impostare notifiche o intraprendere azioni. Se scegli il pulsante Modifica configurazione nella scheda Monitoraggio, il sistema apre la console di CloudWatch Application Insights. Per ulteriori informazioni su Application Insights, consulta [What is Amazon CloudWatch Application Insights](#) nella Amazon CloudWatch User Guide.

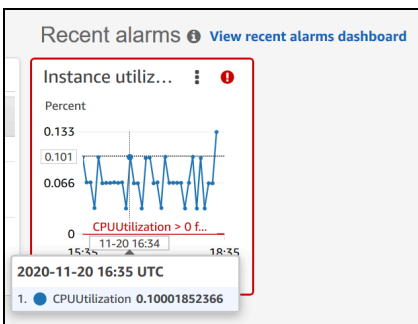
Operazioni che è possibile eseguire in questa pagina

In questa pagina è possibile eseguire le seguenti operazioni:

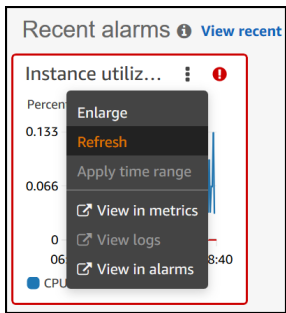
- Scegli un nome di servizio nella sezione Allarmi per AWS servizio per CloudWatch aprire il servizio e l'allarme selezionati.
- Regola il periodo di tempo per i dati visualizzati nei widget nella sezione Allarmi recenti selezionando uno dei valori predefiniti del periodo di tempo. È possibile scegliere personalizzato per definire il periodo di tempo.



- Passa il cursore su un widget nella sezione Allarmi recenti per visualizzare un popup di dati per un periodo specifico.



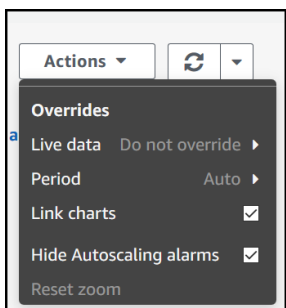
- Scegli il menu delle opzioni in un widget per visualizzare le opzioni di visualizzazione. Scegli Ingrandisci per espandere un widget. Scegli Aggiorna per aggiornare i dati in un widget. Seleziona un intervallo nella visualizzazione dei dati di un widget per visualizzare un intervallo di tempo specifico. È quindi possibile scegliere Applica intervallo di tempo.



- Scegli il menu Operazioni per visualizzare le opzioni di Sostituzione dei dati degli allarmi che includono quanto segue:
  - Scegliere se il widget visualizza i dati in tempo reale. I dati in tempo reale sono dati pubblicati nell'ultimo minuto che non sono stati completamente aggregati. Se i dati in tempo reale sono disattivati, vengono visualizzati solo i punti dati con un periodo di aggregazione di almeno un minuto nel passato. Ad esempio, quando si utilizzano periodi di 5 minuti, il punto dati per le 12:35 verrà aggregato dalle 12:35 alle 12:40 e visualizzato alle 12:41.

Se i dati in tempo reale sono attivati, il punto dati più recente viene visualizzato non appena i dati vengono pubblicati nell'intervallo di aggregazione corrispondente. Ogni volta che si aggiorna la visualizzazione, il punto dati più recente potrebbe cambiare se vengono pubblicati nuovi dati all'interno di tale periodo di aggregazione.

- Specifica un periodo di tempo per i dati in tempo reale.
- Collega i grafici nella sezione Allarmi recenti in modo che, quando ingrandisci o rimpicciolisci un grafico, l'altro grafico si ingrandisce o rimpicciolisce allo stesso tempo. È possibile scollegare i grafici per limitare l'ingrandimento a un solo grafico.
- Nascondi gli allarmi Auto Scaling.



Per aprire il Monitoraggio linguetta

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.

2. Nel pannello di navigazione, scegli Application Manager.
3. Nella sezione Applicazioni, scegli una categoria. Se si desidera aprire un'applicazione creata manualmente in Application Manager, scegliere Applicazioni personalizzate.
4. Scegli l'applicazione nell'elenco. Application Manager apre la scheda Panoramica.
5. Scegli la scheda Monitoraggio.

## Visualizzazione OpsItems per un'applicazione

In Application Manager, un componente di AWS Systems Manager, la OpsItemsscheda visualizza gli elementi di lavoro operativi (OpsItems) per le risorse nell'applicazione selezionata. Puoi configurare Systems Manager OpsCenter per creare automaticamente OpsItems da Amazon CloudWatch allarmi ed EventBridge eventi Amazon. È anche possibile creare manualmente OpsItems.

### Operazioni che è possibile eseguire in questa scheda

In questa pagina è possibile eseguire le seguenti operazioni:

- Filtraggio dell'elenco di OpsItems utilizzando il campo di ricerca. È possibile filtrare per nome, ID, ID fonte o gravità di OpsItem. Inoltre è possibile filtrare l'elenco in base allo stato. OpsItems supporta i seguenti stati: aperto, in corso, aperto e in corso, risolto oppure tutti.
- Modifica lo stato di un OpsItem scegliendo il pulsante di opzione accanto a esso e scegliendo un'opzione nel menu Impostazione dello stato.
- Apri OpsCenter di Systems Manager per creare un OpsItem scegliendo Crea OpsItem.

### Per aprire la scheda OpsItems

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Application Manager.
3. Nella sezione Applicazioni, scegli una categoria. Se si desidera aprire un'applicazione creata manualmente in Application Manager, scegliere Applicazioni personalizzate.
4. Scegliere l'applicazione nell'elenco. Application Manager apre la scheda Overview (Panoramica).
5. Scegli la scheda OpsItems.

## Gestione dei log delle applicazioni

In Application Manager, un componente di AWS Systems Manager, la scheda Logs mostra un elenco di gruppi di log di Amazon CloudWatch Logs.

Operazioni che è possibile eseguire in questa scheda

In questa pagina è possibile eseguire le seguenti operazioni:

- Scegli il nome di un gruppo di log per aprirlo in CloudWatch Logs. È quindi possibile scegliere un flusso di log per visualizzare i log di una risorsa nel contesto di un'applicazione.
- Scegli Crea gruppi di log per creare un gruppo di log in CloudWatch Logs.

Per aprire la scheda Log

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Application Manager.
3. Nella sezione Applicazioni, scegli una categoria. Se si desidera aprire un'applicazione creata manualmente in Application Manager, scegliere Applicazioni personalizzate.
4. Scegliere l'applicazione nell'elenco. Application Manager apre la scheda Overview (Panoramica).
5. Scegli la scheda Log.

Utilizza i runbook Automation per correggere i problemi delle applicazioni

È possibile risolvere i problemi con le AWS risorse utilizzando i runbook di Application Manager Automation. Un runbook di automazione definisce le azioni che Systems Manager esegue sulle istanze gestite e su altre AWS risorse quando viene eseguita un'automazione. L'automazione è uno strumento di AWS Systems Manager. Un runbook contiene una o più fasi che si eseguono in ordine sequenziale. Ogni fase è riferita a una singola operazione. L'output di una fase può essere utilizzato come input in una fase successiva.

Quando si sceglie Avvia runbook da un'applicazione o cluster di Application Manager, il sistema visualizza un elenco filtrato di runbook disponibili in base al tipo di risorse nell'applicazione o nel cluster. Quando si sceglie il runbook che si desidera avviare, Systems Manager apre la pagina Execute automation document (Esegui il documento di automazione).

Application Manager include i miglioramenti seguenti per l'utilizzo di runbook.

- Se si sceglie il nome di una risorsa in Application Manager e quindi Esegui runbook, il sistema visualizza un elenco filtrato di runbook per quel tipo di risorsa.
- È possibile avviare un'automazione su tutte le risorse dello stesso tipo scegliendo un runbook nell'elenco e quindi scegliendo Esegui per risorse dello stesso tipo.

## Prima di iniziare

Prima di avviare un runbook da Application Manager, effettua le seguenti operazioni:

- Verifica di disporre delle autorizzazioni corrette per l'avvio di runbook. Per ulteriori informazioni, consulta [Configurazione del servizio di automazione](#).
- Rivedi la documentazione relativa alla procedura di automazione relativa all'avvio dei runbook. Per ulteriori informazioni, consulta [Esegui un'operazione automatizzata basata su Systems Manager Automation](#).

## Per avviare un runbook da Application Manager

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Application Manager.
3. Nella sezione Applicazioni, scegli una categoria. Se si desidera aprire un'applicazione creata manualmente in Application Manager, scegliere Applicazioni personalizzate.
4. Scegli l'applicazione nell'elenco. Application Manager apre la scheda Panoramica.
5. Scegli Avvia runbook. Application Manager apre il pop-up del widget di automazione. Per ulteriori informazioni sulle opzioni nel widget di automazione, consulta [Esegui un'operazione automatizzata basata su Systems Manager Automation](#).

## Aggiungi tag alle risorse in Application Manager

Puoi aggiungere o eliminare rapidamente tag su applicazioni e AWS risorse in Application Manager. Utilizzate la seguente procedura per aggiungere o eliminare un tag da un'applicazione e da tutte le AWS risorse in essa contenute.

Per aggiungere o eliminare un tag da un'applicazione e da tutte le risorse nell'applicazione

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.

2. Nel pannello di navigazione, scegli Application Manager.
3. Nella sezione Applicazioni, scegli una categoria. Se si desidera aprire un'applicazione creata manualmente in Application Manager, scegliere Applicazioni personalizzate.
4. Scegliere l'applicazione nell'elenco. Application Manager apre la scheda Overview (Panoramica).
5. Nella sezione Informazioni sull'applicazione, scegli il numero sottostante Tag delle applicazioni. Se all'applicazione non sono assegnati tag, il numero è zero.
6. Per aggiungere un tag, scegli Aggiungi un nuovo tag. Specificare una chiave e un valore facoltativo. Per rimuovere un tag, scegli Rimuovi.
7. Scegli Salva.

Utilizzare la procedura seguente per aggiungere o eliminare un tag da una risorsa specifica in Application Manager.

Per aggiungere o eliminare un tag da una risorsa

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Application Manager.
3. Nella sezione Applicazioni, scegli una categoria. Se si desidera aprire un'applicazione creata manualmente in Application Manager, scegliere Applicazioni personalizzate.
4. Scegliere l'applicazione nell'elenco. Application Manager apre la scheda Overview (Panoramica).
5. Scegli la scheda Risorse.
6. Scegliere un nome per la risorsa.
7. Nella sezione Tag, scegli Modifica.
8. Per aggiungere un tag, scegliere Add new tag (Aggiungi un nuovo tag). Specificare una chiave e un valore facoltativo. Per rimuovere un tag, scegli Rimuovi.
9. Scegliere Save (Salva).

Lavorare con CloudFormation modelli e impilabili Application Manager

Application Manager ti aiuta a fornire e gestire le risorse per le tue applicazioni integrandosi con AWS CloudFormation. È possibile creare, modificare ed eliminare modelli e stack di CloudFormation in Application Manager. Uno stack è una raccolta di risorse di AWS che è possibile gestire come un'unità singola. Ciò significa che puoi creare, aggiornare o eliminare una raccolta di AWS risorse



utilizzando gli CloudFormation stack. Un modello è un file di testo formattato in JSON o YAML che specifica le risorse di cui intendi effettuare il provisioning negli stack.

Application Manager include anche una libreria di modelli in cui è possibile clonare, creare e archiviare modelli. Application Manager CloudFormation visualizza le stesse informazioni sullo stato corrente di uno stack. I modelli e gli aggiornamenti dei modelli vengono archiviati in Systems Manager fino al provisioning dello stack, momento in cui vengono visualizzate anche le modifiche CloudFormation.

Dopo aver creato uno stack in Application Manager, nella pagina degli CloudFormation stack vengono visualizzate informazioni utili a riguardo. Questo include il modello utilizzato per crearlo, un conteggio di [OpsItems](#) per le risorse nello stack, [stato dello stack](#) e [stato di deviazione](#).

### Informazioni su Cost Explorer

Application Manager è integrato con AWS Cost Explorer, una funzionalità di [AWS Cost Management](#), tramite il widget Cost. Dopo aver abilitato Cost Explorer nella console di gestione costi, il widget Costi in Application Manager mostra i dati di costo per una specifica applicazione o componente dell'applicazione non container. È possibile utilizzare i filtri nel widget per visualizzare i dati dei costi in base a diversi periodi di tempo, granularità e tipi di costo in un grafico a barre o a linee.

È possibile abilitare questa funzionalità scegliendo il pulsante [Vai alla console di gestione dei AWS costi](#). Per impostazione predefinita, i dati vengono filtrati negli ultimi tre mesi. Per un'applicazione non container, se si sceglie il tasto [Visualizza tutto](#) in questa sezione, Application Manager aprirà la scheda Risorse. Per le applicazioni container, il tasto [Visualizza tutto](#) aprirà la console AWS Cost Explorer.

#### Note

Esplorazione dei costi utilizza i tag per tenere traccia dei costi delle applicazioni. Se l'applicazione CloudFormation basata su stack non è configurata con la chiave `AppManagerCFNStackKey` tag, Cost Explorer non riesce a presentare dati accurati sui costi in formato. Application Manager Quando il `AppManagerCFNStackKey` tag key non viene rilevato, nella console ti viene richiesto di aggiungere il tag allo CloudFormation stack per abilitare il monitoraggio dei costi. Aggiungendo la chiave di tag, verrà associata al nome della risorsa Amazon (ARN) dello stack e abiliterà il widget Costi per visualizzare dati accurati sui costi.

**⚠ Important**

L'aggiunta del tag `AppManager:CFNStackKey` attiverà un aggiornamento dello stack. Qualsiasi configurazione manuale eseguita dopo l'implementazione originale dello stack non si rifletterà dopo l'aggiunta del tag utente. Per ulteriori informazioni sui comportamenti di aggiornamento delle risorse, consulta [Comportamenti di aggiornamento delle risorse di stack](#) nella Guida per l'utente di AWS CloudFormation

## Prima di iniziare

Utilizzate i seguenti collegamenti per conoscere CloudFormation i concetti prima di creare, modificare o eliminare CloudFormation modelli e stack utilizzando Application Manager

- [Che cos'è AWS CloudFormation?](#)
- [CloudFormation best practice](#)
- [Informazioni sulle nozioni di base dei modelli](#)
- [Utilizzo degli stack di AWS CloudFormation](#)
- [Utilizzo dei modelli di AWS CloudFormation](#)
- [Modelli di esempio](#)

## Argomenti

- [Utilizzo Application Manager da gestire CloudFormation modelli](#)
- [Utilizzo Application Manager da gestire CloudFormation stack](#)

## Utilizzo Application Manager da gestire CloudFormation modelli

Application Manager include una libreria di modelli e altri strumenti per aiutarti a gestire i AWS CloudFormation modelli. Questa sezione include le seguenti informazioni.

## Argomenti

- [Utilizzo della libreria dei modelli](#)
- [Creazione di un modello](#)
- [Modifica di un modello](#)

## Utilizzo della libreria dei modelli

La libreria dei modelli di Application Manager offre strumenti che consentono di visualizzare, creare, modificare, eliminare e clonare i modelli. È inoltre possibile effettuare il provisioning degli stack direttamente dalla libreria dei modelli. I modelli vengono memorizzati come documenti di Systems Manager (SSM) di tipo CloudFormation. Memorizzando i modelli come documenti SSM, è possibile utilizzare i controlli versione per utilizzare versioni diverse di un modello. È anche possibile impostare autorizzazioni e condividere modelli. Dopo aver eseguito correttamente il provisioning di uno stack, lo stack e il modello sono disponibili in Application Manager e CloudFormation.

### Prima di iniziare

Ti consigliamo di leggere i seguenti argomenti per saperne di più sui documenti SSM prima di iniziare a lavorare con CloudFormation i modelli in Application Manager.

- [AWS Systems Manager Documenti di](#)
- [Condivisione di documenti SSM](#)
- [Best practice per documenti SSM condivisi](#)

Per visualizzare la libreria di modelli in Application Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Application Manager.
3. Scegli CloudFormation Template Library.

### Creazione di un modello

La procedura seguente descrive come creare un CloudFormation modello in Application Manager. Quando crei un modello, inserisci i dettagli dello stack del modello in JSON o YAML. Se non hai familiarità con JSON o YAML, puoi utilizzare AWS Infrastructure Composer, uno strumento per creare e modificare visivamente i modelli. Per ulteriori informazioni, consulta [Creare modelli visivamente con Infrastructure Composer](#) nella Guida per l'utente AWS CloudFormation . Per ulteriori informazioni sulla struttura e sintassi di un modello, consulta [Sezioni dei modelli CloudFormation](#) nella Guida per l'utente AWS CloudFormation .

È inoltre possibile creare un modello da più frammenti di modello. I frammenti di modello sono esempi che illustrano come scrivere modelli per una risorsa specifica. Ad esempio, puoi visualizzare

frammenti per istanze Amazon Elastic Compute Cloud (Amazon EC2), domini Amazon Simple Storage Service (Amazon S3), mappature e altro ancora. CloudFormation I frammenti sono raggruppati per risorsa. Puoi trovare i frammenti generici di CloudFormation nella sezione [General template snippets \(frammenti di modello generali\)](#) della Guida per l'utente di AWS CloudFormation .

### Creazione di un modello in CloudFormation Application Manager (console)

Utilizzare la procedura seguente per creare un CloudFormation modello in Application Manager utilizzando il Console di gestione AWS.

Per creare un CloudFormation modello in Application Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Application Manager.
3. Scegli Libreria CloudFormation modelli, quindi scegli Crea modello o scegli un modello esistente e quindi scegli Azioni, Clona.
4. Per Name (Nome), inserire un nome per il modello che consente di identificare le risorse create o lo scopo dello stack.
5. (Facoltativo) Per Version name (Versione nome), inserire un nome o un numero per identificare la versione del modello.
6. Nella sezione Editor di codice, scegli YAML o JSON e quindi inserisci o copia e incolla il codice del modello.
7. (Facoltativo) Nella sezione Tag, applica una o più name/value coppie di chiavi di tag al modello.
8. (Facoltativo) Nella sezione Autorizzazioni, inserisci un Account AWS ID e scegli Aggiungi account. Questa operazione fornisce l'autorizzazione di lettura per il modello. Il proprietario dell'account può effettuare il provisioning e clonare il modello, ma non può modificarlo o eliminarlo.
9. Scegliere Create (Crea). Il modello viene salvato nel servizio documenti di Systems Manager (SSM).

### Creazione di un CloudFormation modello in Application Manager (riga di comando)

Dopo aver creato il contenuto del CloudFormation modello in JSON o YAML, puoi usare AWS Command Line Interface (AWS CLI) o AWS Strumenti per PowerShell per salvare il modello come documento SSM. Sostituisci ogni *example resource placeholder* con le tue informazioni.

## Prima di iniziare

Installa e configura il AWS CLI o il AWS Strumenti per PowerShell se non l'hai già fatto. Per informazioni, consulta le pagine [Installazione o aggiornamento della versione più recente di AWS CLI](#) e [Installazione di AWS Strumenti per PowerShell](#).

## Linux & macOS

```
aws ssm create-document \
 --content file://path/to/template_in_json_or_yaml \
 --name "a_name_for_the_template" \
 --document-type "CloudFormation" \
 --document-format "JSON_or_YAML" \
 --tags "Key=tag-key,Value=tag-value"
```

## Windows

```
aws ssm create-document ^
 --content file://C:\path\to\template_in_json_or_yaml ^
 --name "a_name_for_the_template" ^
 --document-type "CloudFormation" ^
 --document-format "JSON_or_YAML" ^
 --tags "Key=tag-key,Value=tag-value"
```

## PowerShell

```
$json = Get-Content -Path "C:\path\to\template_in_json_or_yaml" | Out-String
New-SSMDocument `
 -Content $json `
 -Name "a_name_for_the_template" `
 -DocumentType "CloudFormation" `
 -DocumentFormat "JSON_or_YAML" `
 -Tags "Key=tag-key,Value=tag-value"
```

Se il comando viene eseguito correttamente, verrà visualizzata una risposta simile alla seguente:

```
{
 "DocumentDescription": {
 "Hash": "c1d9640f15fbdba6deb41af6471d6ace0acc22f213bdd1449f03980358c2d4fb",
 "HashType": "Sha256",
 "Name": "MyTestCFTemplate",
```

```
"Owner": "428427166869",
"CreateDate": "2021-06-04T09:44:18.931000-07:00",
"Status": "Creating",
"DocumentVersion": "1",
"Description": "My test template",
"PlatformTypes": [],
"DocumentType": "CloudFormation",
"SchemaVersion": "1.0",
"LatestVersion": "1",
"DefaultVersion": "1",
"DocumentFormat": "YAML",
"Tags": [
 {
 "Key": "Templates",
 "Value": "Test"
 }
]
```

## Modifica di un modello

Utilizzare la procedura seguente per modificare un CloudFormation modello in Application Manager. Le modifiche al modello sono disponibili CloudFormation dopo aver effettuato il provisioning di uno stack che utilizza il modello aggiornato.

Per modificare un CloudFormation modello in Application Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Application Manager.
3. Scegli CloudFormation Template Library
4. Scegliere un modello e quindi scegliere Actions (Operazioni), Edit (Modifica). Non è possibile modificare il nome di un modello, ma è possibile modificare tutti gli altri dettagli.
5. Scegliere Save (Salva). Il modello viene salvato nel servizio Systems Manager Document.

## Utilizzo Application Manager da gestire CloudFormation stack

Application Manager ti aiuta a fornire e gestire le risorse per le tue applicazioni integrandoti con. AWS CloudFormation Puoi creare, modificare ed eliminare CloudFormation modelli e stack in. Application Manager Uno stack è una raccolta di AWS risorse che puoi gestire come una singola

unità. Ciò significa che puoi creare, aggiornare o eliminare una raccolta di AWS risorse utilizzando CloudFormation gli stack. Un modello è un file di testo formattato in JSON o YAML che specifica le risorse di cui intendi effettuare il provisioning negli stack. Questa sezione include le seguenti informazioni.

## Argomenti

- [Creazione di uno stack](#)
- [Aggiornamento di uno stack](#)

## Creazione di uno stack

Le seguenti procedure descrivono come creare uno CloudFormation stack utilizzando Application Manager. Uno stack si basa su un modello. Quando si crea uno stack, è possibile scegliere un modello esistente oppure crearne uno nuovo. Dopo aver creato lo stack, il sistema tenta immediatamente di creare le risorse identificate nello stack. Dopo che il sistema ha effettuato correttamente il provisioning delle risorse, il modello e lo stack sono disponibili per la visualizzazione e la modifica in Application Manager e CloudFormation.

### Note

L'utilizzo per Application Manager creare uno stack è gratuito, ma ti vengono addebitati i costi relativi AWS alle risorse create nello stack.

## Creazione di una CloudFormation pila utilizzando Application Manager (console)

Utilizza la procedura seguente per creare un nuovo stack utilizzando Application Manager nella Console di gestione AWS.

Per creare una CloudFormation pila

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Application Manager.
3. Scegli Crea applicazione, CloudFormation Stack.
4. Nella sezione Prepare a template (Prepara un modello) scegliere un'opzione. Se scegli Use an existing template (Utilizza un modello esistente), puoi utilizzare le schede disponibili nella

sezione Choose a template (Scegli un modello) per individuare il modello desiderato. Se scegli una delle altre opzioni, completa la procedura guidata per preparare un modello.

5. Seleziona il pulsante accanto al nome del modello, quindi scegli Avanti.
6. Nella pagina Specifica i dettagli del modello, verifica i dettagli del modello per assicurarti che il processo crei le risorse desiderate.
  - (Facoltativo) Nella sezione Tag, applica una o più name/value coppie di chiavi tag al modello.
  - I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente.
  - Scegli Avanti.
7. Sulla pagina Edit stack details (Modifica i dettagli dello stack), per Stack name (Nome dello stack) inserire un nome che ti aiuti a identificare le risorse create dallo stack o il suo scopo.
  - La sezione Parametri include tutti i parametri facoltativi e richiesti specificati nel modello. Inserire uno o più parametri in ogni campo.
  - (Facoltativo) Nella sezione Tag, applica una o più name/value coppie di chiavi tag allo stack.
  - (Facoltativo) Nella sezione Autorizzazioni, specifica un nome di ruolo AWS Identity and Access Management (IAM) o un Amazon Resource Name (ARN) IAM. Il sistema utilizza il ruolo di servizio specificato per creare tutte le risorse specificate nello stack. Se non indichi un ruolo IAM, allora CloudFormation utilizza una sessione temporanea generata dal sistema dalle credenziali utente. Per ulteriori informazioni su questo ruolo IAM, consulta [service role di](#) (ruolo di servizio CloudFormation ) nella Guida per l'utente di AWS CloudFormation .
  - Seleziona Next (Successivo).
8. Nella pagina Review and provision (Revisiona ed effettua il provisioning), rivedi i dettagli dello stack. Scegli un pulsante di Edit (Modifica) in questa pagina per apportare modifiche.
9. Scegli Provision stack (Effettua il provisioning di stack).

Application Manager visualizza la pagina degli CloudFormation stack e lo stato di creazione e distribuzione dello stack. Se CloudFormation non riesce a creare ed eseguire il provisioning dello stack, consulta i seguenti argomenti nella Guida per l'AWS CloudFormation utente.

- [Codici di stato dello stack](#)
- [Risoluzione dei problemi CloudFormation](#)





## PowerShell

```
New-CFNStack `
 -StackName "a_name_for_the_stack" `
 -TemplateURL "ssm-doc://arn:aws:ssm:Region:account_ID:document/template_name" `
```

### Aggiornamento di uno stack

È possibile distribuire gli aggiornamenti su uno CloudFormation stack modificando direttamente lo stack in Application Manager. Con un aggiornamento diretto, è possibile specificare gli aggiornamenti di un modello o parametri di input. Dopo aver salvato e distribuito le modifiche, CloudFormation aggiorna le AWS risorse in base alle modifiche specificate.

Puoi visualizzare in anteprima le modifiche che CloudFormation verranno apportate allo stack prima di aggiornarlo utilizzando i set di modifiche. Per ulteriori informazioni, consulta [Aggiornamento di stack utilizzando i set di modifiche](#) nella Guida per l'utente di AWS CloudFormation .

Per aggiornare uno CloudFormation stack in Application Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Application Manager.
3. Seleziona il pulsante di opzione accanto al nome di un'applicazione, quindi scegli Azioni, Aggiorna stack.
4. Sulla pagina Specify template source (Specifica la fonte del modello), scegliere una delle seguenti opzioni, quindi scegliere Next (Successivo).
  - Scegliere Use the template code currently provisioned in the stack (Utilizza il codice di modello per cui è stato attualmente effettuato il provisioning nello stack) per visualizzare un modello. Utilizza una versione di modello nell'elenco Versions (Versioni), quindi scegliere Next (Successivo).
  - Scegliere Switch to a different template (Passa a un modello diverso) per scegliere o creare un nuovo modello per lo stack.
5. Una volta completate le modifiche al modello, scegliere Next (Successivo).
6. Sulla pagina Edit stack details (Modifica i dettagli dello stack), puoi modificare parametri, tag e autorizzazioni. Non è possibile cambiare il nome di uno stack. Apportare le modifiche, quindi scegliere Next (Successivo).

7. Sulla pagina Review and provision (Revisiona ed effettua il provisioning), rivedere tutti i dettagli dello stack e quindi scegliere Provision stack (Effettua il provisioning dello stack).

## Lavorare con i cluster in Application Manager

Questa sezione include argomenti per aiutarti a lavorare con i cluster di container Amazon Elastic Container Service (Amazon ECS) e Amazon Elastic Kubernetes Service (Amazon EKS) in, un componente di. Application Manager AWS Systems Manager

### Indice

- [Lavorare con Amazon ECS in Application Manager](#)
- [Lavorare con Amazon EKS in Application Manager](#)
- [Utilizzo dei runbook per i cluster](#)

## Lavorare con Amazon ECS in Application Manager

Con Application Manager, puoi visualizzare e gestire la tua infrastruttura di cluster Amazon Elastic Container Service (Amazon ECS). Application Manager applica un tag al tuo cluster Amazon ECS utilizzando l'Amazon Resource Name (ARN) del cluster come valore del tag. Application Manager fornisce una visualizzazione in fase di esecuzione dei componenti delle risorse di calcolo, rete e storage in un cluster.

### Note

Non è possibile gestire o visualizzare informazioni sulle operazioni relative ai container su Application Manager. È possibile gestire e visualizzare solo le informazioni sulle operazioni relative all'infrastruttura che ospita le risorse di Amazon ECS.

## Operazioni che è possibile eseguire in questa pagina

In questa pagina è possibile eseguire le seguenti operazioni:

- Scegliere Manage cluster (Gestisci il cluster) per aprire il cluster in Amazon ECS.
- Scegliere View all (Visualizza tutto) per visualizzare un elenco di risorse nel cluster;
- Scegli Visualizza in CloudWatch per visualizzare gli allarmi delle risorse in Amazon. CloudWatch

- Scegli Manage nodes (Gestisci i nodi) o Manage Fargate profiles (Gestisci profili Fargate) per visualizzare queste risorse in Amazon ECS.
- Scegliere un ID di risorsa per visualizzarne le informazioni dettagliate nella console in cui è stato creato.
- Visualizzazione di un elenco di OpsItems correlati ai cluster.
- Visualizza una cronologia dei runbook eseguiti nei cluster.

## Per aprire un Cluster ECS

1. Aprire la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegliere Application Manager.
3. Nella sezione Container clusters (Cluster di container), scegliere ECS clusters (Cluster di ECS).
4. Scegliere un cluster nell'elenco. Application Manager apre la scheda Overview (Panoramica).

## Lavorare con Amazon EKS in Application Manager

Application Manager si integra con [Amazon Elastic Kubernetes Service](#) (Amazon EKS) per fornire informazioni sullo stato della tua infrastruttura di cluster Amazon EKS. Application Manager applica un tag al tuo cluster Amazon EKS utilizzando l'Amazon Resource Name (ARN) del cluster come valore del tag. Application Manager fornisce una visualizzazione in fase di esecuzione dei componenti delle risorse di calcolo, rete e storage in un cluster.

### Note

Non è possibile gestire o visualizzare informazioni sulle operazioni relative ai pod o container di Amazon EKS su Application Manager. È possibile gestire e visualizzare solo le informazioni sulle operazioni relative all'infrastruttura che ospita le risorse di Amazon EKS.

## Operazioni che è possibile eseguire in questa pagina

In questa pagina è possibile eseguire le seguenti operazioni:

- Scegliere Manage cluster (Gestisci il cluster) per aprire il cluster in Amazon EKS.
- Scegliere View all (Visualizza tutto) per visualizzare un elenco di risorse nel cluster.

- Scegli **Visualizza in CloudWatch** per visualizzare gli allarmi delle risorse in Amazon. CloudWatch
- Scegli **Manage nodes (Gestisci i nodi)** o **Manage Fargate profiles (Gestisci profili Fargate)** per visualizzare queste risorse in Amazon EKS.
- Scegliere un ID di risorsa per visualizzarne le informazioni dettagliate nella console in cui è stato creato.
- Visualizzazione di un elenco di OpsItems correlati ai cluster.
- Visualizza una cronologia dei runbook eseguiti nei cluster.

Per aprire un Cluster EKS applicazione

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegliere **Application Manager**.
3. Nella sezione **Container clusters (Cluster di container)**, scegliere **EKS clusters (Cluster di EKS)**.
4. Scegliere un cluster nell'elenco. Application Manager apre la scheda **Overview (Panoramica)**.

Utilizzo dei runbook per i cluster

È possibile risolvere i problemi relativi alle AWS risorse da Application Manager, uno strumento in AWS Systems Manager, utilizzando i runbook di Systems Manager Automation. Quando si sceglie **Avvia runbook** da un cluster di Application Manager, il sistema visualizza un elenco filtrato di runbook in base al tipo di risorse nell'applicazione o nel cluster. Quando si sceglie il runbook che si desidera avviare, Systems Manager apre la pagina **Execute automation document (Esegui il documento di automazione)**.

Prima di iniziare

Prima di avviare un runbook da Application Manager, effettua le seguenti operazioni:

- Verifica di disporre delle autorizzazioni corrette per l'avvio di runbook. Per ulteriori informazioni, consulta [Configurazione del servizio di automazione](#).
- Rivedi la documentazione relativa alla procedura di automazione relativa all'avvio dei runbook. Per ulteriori informazioni, consulta [Esegui un'operazione automatizzata basata su Systems Manager Automation](#).

- Se intendi avviare i runbook su più risorse contemporaneamente, esamina la documentazione relativa all'utilizzo di destinazioni e controlli frequenza. Per ulteriori informazioni, consulta [Esegui operazioni automatizzate su larga scala](#).

Per avviare un runbook per cluster da Application Manager

1. Aprire la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegliere Application Manager.
3. Nella sezione Cluster di container, scegliere un tipo di container.
4. Scegliere il cluster nell'elenco. Application Manager apre la scheda Overview (Panoramica).
5. Nella scheda Runbooks (Runbook), scegli Start runbook (Avvia runbook). Application Manager apre la pagina Execute automation document (Esegui il documento di automazione) in una nuova scheda. Per ulteriori informazioni sulle opzioni nella pagina Execute automation document (Esegui il documento di automazione), vedi [Esegui un'operazione automatizzata basata su Systems Manager Automation](#).

## AWS Systems Manager Parameter Store

Parameter Store è un archivio dati di configurazione centralizzato per valori denominati parametri. Un parametro è qualsiasi dato memorizzato in Parameter Store, ad esempio un blocco di testo, un elenco di nomi, un AMI ID, una chiave di licenza e così via. Con Parameter Store, è possibile archiviare, organizzare e recuperare in modo sicuro i dati di configurazione su larga scala.

Parameter Store semplifica la gestione della configurazione in tutti gli ambienti. È possibile standardizzare il modo in cui le applicazioni accedono ai dati critici in fase di esecuzione senza codificare i valori o affidarsi a soluzioni di storage frammentate. In questo modo, è possibile mantenere la coerenza, applicare la governance e creare sistemi più sicuri e manutenibili.

Parameter Store supporta i seguenti tipi di parametro:

- **String**

Utilizzate questo tipo per valori di testo normale, come nomi di ambienti, URL degli endpoint o identificatori di risorse.

- **StringList**

Utilizzate questo tipo per un elenco separato da virgole di valori in testo normale. Ad esempio, è possibile memorizzare il valore. subnet-123abc , subnet-456def , subnet-789ghi

• SecureString

Utilizzalo SecureString per i valori di configurazione che richiedono la crittografia, come gli endpoint del servizio e gli identificatori degli account. Per informazioni segrete, come credenziali di database, chiavi API o token, consigliamo di utilizzare questa soluzione che fornisce controlli di sicurezza appositamente progettati AWS Secrets Manager, tra cui la rotazione automatica e la replica tra regioni.

Parameter Storecrittografa i valori utilizzando. AWS Key Management Service

Per ulteriori informazioni sui tipi di parametri, vedere[Riferimento Parameter Store](#).

Dove devo archiviare i dati della mia applicazione?

Utilizzate la seguente tabella per scegliere un servizio per i dati della vostra applicazione.

 Note

Se gestisci credenziali come nomi utente, password o altri segreti, ti consigliamo di utilizzarle. [AWS Secrets Manager](#) Secrets Manager è stato creato appositamente per la gestione di segreti come credenziali di database, chiavi API e segreti supportati forniti da software di terze parti. Per ulteriori informazioni, vedi Che cos'è? [AWS Secrets Manager](#) nella Guida AWS Secrets Manager per l'utente.

| Funzionalità | Parameter Store                                                                                                                         | AWS AppConfig                                                                                                                                                                                    | AWS Secrets Manager                                                                                                                                                       |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Casi d'uso   | <ul style="list-style-type: none"><li>• Configurazione statica</li><li>• Key-value storage senza implement azione o convalida</li></ul> | <ul style="list-style-type: none"><li>• Configurazione delle applicazioni modificat a di frequente</li><li>• Zero-downtime implementazioni</li><li>• esperimenti in fase di esecuzione</li></ul> | <ul style="list-style-type: none"><li>• Credenziali o altri segreti</li><li>• Dati crittografati che richiedono rotazione automatica, accesso tra più account o</li></ul> |

| Funzionalità                | Parameter Store                                                                                                                                                                                                  | AWS AppConfig                                                                                                                                                                            | AWS Secrets Manager                                                                                                                                               |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             |                                                                                                                                                                                                                  |                                                                                                                                                                                          | registrazione di controllo dettagliata                                                                                                                            |
| Dati tipici                 | <ul style="list-style-type: none"> <li>• ID AMI approvati</li> <li>• Variabili di ambiente</li> <li>• URL degli endpoint</li> <li>• Identificatori di risorse</li> <li>• Ottimizzazione dei parametri</li> </ul> | <ul style="list-style-type: none"> <li>• Bandiere delle funzionalità</li> <li>• Interruttori operativi</li> <li>• Parametri regolabili</li> <li>• Elenchi consentiti e negati</li> </ul> | <ul style="list-style-type: none"> <li>• Credenziali del database</li> <li>• Chiavi API</li> <li>• Token OAuth</li> <li>• Chiavi e certificati privati</li> </ul> |
| Encryption (Crittografia)   | Facoltativo con SecureString e AWS KMS                                                                                                                                                                           | AWS crittografia gestita a riposo; chiave aggiuntiva opzionale gestita dal cliente                                                                                                       | AWS KMS crittografia inattiva con una chiave AWS gestita o gestita dal cliente                                                                                    |
| rotazione delle credenziali | Nessuno                                                                                                                                                                                                          | Non applicabile                                                                                                                                                                          | Automatico, con integrazioni native del database                                                                                                                  |
| Costo                       | Livello standard gratuito; livello avanzato e throughput più elevato fatturato                                                                                                                                   | Fatturato in base alla richiesta di configurazione                                                                                                                                       | Fatturato per segreto al mese e per chiamata API                                                                                                                  |
| Implementazione             | Controllo delle versioni senza convalida pre-implementazione o rollback automatico                                                                                                                               | Implementazione graduale, convalida pre-distribuzione e rollback automatico degli allarmi Amazon CloudWatch                                                                              | Controllo delle versioni con etichette di staging                                                                                                                 |

## Parameter Store caratteristiche

Parameter Store supporta le caratteristiche seguenti:

- Aggiornamenti di configurazione centralizzati



Aggiorna la configurazione senza modifiche o ridistribuzioni del codice, migliorando l'agilità operativa e riducendo i rischi. Ad esempio, puoi aggiornare `myapp/prod/inventory-service-endpoint` in modo che punti a un nuovo endpoint dopo la migrazione del servizio di inventario.

#### Note

L'aggiornamento dei parametri ha effetto alla lettura successiva, senza convalida, implementazione graduale o ripristino automatico. Per una configurazione in cui un valore errato potrebbe causare un'interruzione, AWS AppConfig aggiunge un flusso di lavoro di distribuzione gestito. Convalida la modifica (utilizzando JSON Schema o Lambda), la implementa gradualmente e monitora gli allarmi Amazon CloudWatch. Se viene attivato un allarme, annulla AWS AppConfig automaticamente la modifica (ciò richiede le autorizzazioni IAM necessarie). Vedi [Lavorare con le strategie di distribuzione](#).

- High-performance opzione di throughput

Parameter Store fornisce un throughput predefinito adatto a carichi di lavoro su scala ridotta. Per applicazioni di grandi dimensioni o sensibili alla latenza che richiedono tassi di richiesta più elevati, è possibile attivare la modalità ad alta velocità effettiva a un costo aggiuntivo.

Se l'applicazione recupera i parametri frequentemente o su larga scala, valuta in anticipo le impostazioni di throughput per evitare limitazioni. Per informazioni su come abilitare un throughput elevato, vedere [Gestione Parameter Store velocità di trasmissione effettiva](#)

- Gestione gerarchica dei parametri

Utilizza le gerarchie di [parametri](#) per raggruppare i parametri correlati, semplificando l'individuazione, la gestione e il filtraggio tra ambienti e applicazioni. Ad esempio, è possibile creare la convenzione di denominazione `env/computer-type/app/data` e quindi creare parametri specifici dell'applicazione come `dev/webserver-ami`. `linux/approved dev/webserver windows/approved` È possibile recuperare il percorso `dev/webserver` per trovare tutti i parametri del server Web per gli ambienti di sviluppo o `dev/webserver/linux` per trovare solo i parametri delle immagini Linux.

- Funzione Versioni multiple

Parameter Store mantiene le 100 [versioni più recenti](#) di ciascun parametro. Quando si esaminano i problemi operativi, è possibile rivedere e ricostruire i valori precedenti.

- Integrazione con IAM

Utilizza le policy IAM per determinare se un'applicazione è in grado di leggere, scrivere, elencare o eliminare i parametri. Ad esempio, potresti scrivere un ruolo dell'applicazione in grado di leggere i parametri preceduti da `myapp/prod/*` ma non da `myapp/dev/*`. È inoltre possibile concedere a un ruolo l'autorizzazione a decrittografare un parametro crittografato.

- Accessibilità da altri Servizi AWS

È possibile fare riferimento ai valori dei parametri di altri AWS servizi. Ecco alcuni esempi:

- Le funzioni Lambda possono recuperare parametri e segreti utilizzando l'estensione Lambda [Parameters and Secrets](#).
- Amazon Elastic Container Service e AWS Fargate consentono di [inserire variabili ambientali i](#) cui valori sono gestiti centralmente in. Parameter Store

#### Note

Le variabili di ambiente da Parameter Store vengono risolte all'avvio di un'attività. Un'attività in esecuzione richiede una nuova attività o una distribuzione forzata per acquisire un valore modificato. Per una configurazione che dovrebbe essere aggiornata senza sostituire le attività, eseguite l' AWS AppConfig agente come contenitore aggiuntivo per fornire i valori più recenti all'applicazione. Per i segreti, usa AWS Secrets Manager. Vedi [Cos'è AWS AppConfig l'agente?](#)

- AWS CloudFormation i modelli possono fare riferimento ai valori dei [parametri](#).
- Con AWS AppConfig, puoi creare profili di [configurazione che fanno riferimento a un parametro](#) inParameter Store, aumentando la sicurezza della distribuzione (implementazione graduale, convalida e rollback automatico su un CloudWatch allarme Amazon configurato) pur rimanendo la fonte. Parameter Store
- AWS CodeBuild consente di [definire variabili ambientali i](#) cui valori vengono recuperati dinamicamente in fase di compilazione. Parameter Store
- Accesso condiviso all'account

Centralizza i dati di configurazione in un'unica soluzione Account AWS e condividi i parametri con altri account che necessitano di accesso. Per ulteriori informazioni, consulta [Utilizzo di parametri condivisi in Parameter Store](#).

- Applicazione di patch al sistema operativo

Amazon EC2 consente di specificare il sistema operativo per le nuove istanze [facendo riferimento a un parametro anziché codificare un ID \(AMI\)](#). [AMI](#) Questo approccio garantisce che le istanze utilizzino automaticamente le immagini patchate e aggiornate più recenti. AWS e i fornitori di sistemi operativi forniscono parametri [pubblici](#) che tengono traccia delle versioni AMI correnti, in modo da non dover gestire gli aggiornamenti manualmente. Puoi anche definire i tuoi parametri per fare riferimento a un'AMI dorata gestita centralmente, semplificando l'applicazione di configurazioni coerenti e approvate in tutta l'organizzazione.

- Eventi e notifiche

Automatizza i flussi di lavoro Parameter Store iscrivendoti agli eventi di modifica dei parametri. Puoi anche utilizzare gli eventi di [modifica](#) per imporre la scadenza e ricevere notifiche quando un parametro non è stato ruotato entro un periodo di tempo specificato.

## I livelli dei parametri sono in Parameter Store

Parameter Store offre diversi livelli di parametri che controllano i limiti di archiviazione: il numero e la dimensione massimi dei parametri in un AWS account e in un'area geografica. Configura ogni parametro singolarmente per utilizzare il livello standard o il livello avanzato.

È possibile combinare parametri standard e avanzati. Ad esempio, puoi avere fino a 100.000 parametri avanzati e 10.000 parametri standard nello stesso AWS account e nella stessa regione. La tabella seguente descrive le diverse funzionalità supportate per ogni tipo di parametro.

La tabella seguente descrive le differenze tra i livelli dei parametri.

| Caratteristica o caso d'uso                                | Standard                                                                                                                              | Avanzata                                                                                      |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Caso d'uso                                                 | Ideale per la maggior parte dei dati di configurazione e dei carichi di lavoro su piccola scala. Questa è l'impostazione predefinita. | Ideale quando sono necessari limiti più elevati, valori più elevati o politiche di parametri. |
| Parametri massimi<br>(per Account AWS mano<br>Regione AWS) | 10.000                                                                                                                                | 100.000                                                                                       |

| Caratteristica o caso d'uso     | Standard                | Avanzata                                                                                                                               |
|---------------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Dimensione massima del valore   | 4 KB                    | 8 KB                                                                                                                                   |
| Politiche relative ai parametri | Non supportata          | Supportata<br><br>Per ulteriori informazioni, consulta <a href="#">Assegnazione delle politiche dei parametri in Parameter Store</a> . |
| Condivisibilità tra Account AWS | Non supportata          | Supportata<br><br>Per ulteriori informazioni, consulta <a href="#">Utilizzo di parametri condivisi in Parameter Store</a> .            |
| Capacità di upgrade e downgrade | Aggiornabile            | Non declassabile                                                                                                                       |
| Costo                           | Nessun costo aggiuntivo | Soggetto a costi<br><br>Per ulteriori informazioni, consulta <a href="#">Prezzi di AWS Systems Manager per Parameter Store</a> .       |

Utilizza parametri standard per la maggior parte dei dati di configurazione. Utilizza i parametri avanzati solo quando hai bisogno di funzionalità che i parametri standard non supportano.

Per un confronto dettagliato tra parametri standard e avanzati, consulta [Scelta dei livelli dei parametri](#).

## Nozioni di base su Parameter Store

In questo tutorial, imparerai come creare, recuperare, aggiornare ed eliminare Parameter Store i parametri utilizzando la AWS CLI. Gli esempi utilizzano un'applicazione fittizia denominata «devambiente»myapp, «account111122223333» e «Regione». us-east-1

## Prerequisiti

Prima di iniziare, assicurati di disporre di:

- Un AWS account.
- Un posto dove eseguire i comandi AWS CLI. Puoi utilizzare AWS CloudShell un client locale con la AWS CLI installata e configurata o un'istanza Amazon EC2 con la CLI AWS installata.
- Autorizzazioni IAM per creare, recuperare, aggiornare ed eliminare i parametri. Parameter Store Per questo tutorial, il principale che esegue i comandi necessita di autorizzazioni IAM come `ssm:PutParameter`, `ssm:GetParameter`, `ssm:GetParameters`, `ssm:GetParametersByPath`, `ssm>DeleteParameter` e `ssm>DeleteParameters`. Per ulteriori informazioni, consulta [Gestire l'accesso a Parameter Store parametri che utilizzano le politiche IAM](#).
- AWS Autorizzazioni KMS se crei o `SecureString` recuperi parametri crittografati con una chiave gestita dal cliente. Se si utilizza la chiave AWS gestita predefinita per Parameter Store, non sono necessarie autorizzazioni AWS KMS separate.

## Fase 1: Creare un parametro

Esegui il `put-parameter` comando per creare un `String` parametro denominato `/myapp/dev/log-level` con il valore `INFO`. Poiché in questo esempio non si specifica un livello, Parameter Store crea questo parametro nel livello standard predefinito.

```
aws ssm put-parameter \
 --region us-east-1 \
 --name "/myapp/dev/log-level" \
 --type "String" \
 --value "INFO"
```

## Fase 2: Recupera il valore del parametro

Esegui il [comando](#) `get-parameter` per recuperare il valore di un singolo parametro. L'esempio seguente recupera il valore del parametro. `/myapp/dev/log-level`

```
aws ssm get-parameter \
 --region us-east-1 \
```

```
--name "/myapp/dev/log-level"
```

Il seguente output di esempio stampa il valore del parametro e i relativi metadati.

```
{
 "Parameter": {
 "Name": "/myapp/dev/log-level",
 "Type": "String",
 "Value": "INFO",
 "Version": 1,
 "LastModifiedDate": "2026-06-25T17:20:26.517000+00:00",
 "ARN": "arn:aws:ssm:us-east-1:111122223333:parameter/myapp/dev/log-level",
 "DataType": "text"
 }
}
```

### Fase 3: Creazione di un parametro StringList

Esegui il comando seguente per creare un StringList parametro denominato `/myapp/dev/subnet-ids` con tre ID di sottorete separati da virgole.

```
aws ssm put-parameter \
 --region us-east-1 \
 --name "/myapp/dev/subnet-ids" \
 --type "StringList" \
 --value "subnet-123abc,subnet-456def,subnet-789ghi"
```

### Fase 4: Recupera più parametri

Esegui il [comando](#) `get-parameters` per specificare fino a 10 parametri in un elenco. L'esempio seguente specifica i `/myapp/dev/subnet-ids` parametri `/myapp/dev/log-level` e per nome.

```
aws ssm get-parameters \
 --region us-east-1 \
 --names "/myapp/dev/log-level" "/myapp/dev/subnet-ids"
```

## Fase 5: Creare un parametro crittografato

Utilizzalo `SecureString` per i valori di configurazione che richiedono la crittografia, ad esempio gli endpoint di servizio e gli identificatori degli account. Per informazioni segrete, come credenziali di database, chiavi API o token, consigliamo di utilizzare questa soluzione che fornisce controlli di sicurezza appositamente progettati AWS Secrets Manager, tra cui la rotazione automatica e la replica tra regioni.

Eseguite il comando seguente per creare un `SecureString` parametro denominato `/myapp/dev/vendor/merchant-id` con il valore crittografato. `merchant-739482`

```
aws ssm put-parameter \
 --region us-east-1 \
 --name "/myapp/dev/vendor/merchant-id" \
 --type "SecureString" \
 --value "merchant-739482"
```

### Note

Se gestisci credenziali come nomi utente, password o altri segreti, ti consigliamo di utilizzarle. [AWS Secrets Manager](#) Secrets Manager è stato creato appositamente per la gestione di segreti come credenziali di database, chiavi API e segreti supportati forniti da software di terze parti. Per ulteriori informazioni, vedi Che cos'è? [AWS Secrets Manager](#) nella Guida AWS Secrets Manager per l'utente.

Esegui il comando seguente per vedere cosa succede quando recuperi un `SecureString` valore senza decrittografarlo.

```
aws ssm get-parameter \
 --region us-east-1 \
 --name "/myapp/dev/vendor/merchant-id"
```

L'output mostra quel valore crittografato, non il testo in chiaro.

```
{
 "Parameter": {
 "Name": "/myapp/dev/vendor/merchant-id",
 "Type": "SecureString",
 "Value": "AQICAHh1cV16RSGzfLARDIKV0croMvax6aMUDP1thWREL5ToawG6q+Xj8K...==",
 "Version": 1,
 "LastModifiedDate": "2026-06-25T17:27:56.401000+00:00",
 "ARN": "arn:aws:ssm:us-east-1:111122223333:parameter/myapp/dev/vendor/merchant-id",
 "DataType": "text"
 }
}
```

Eseguite il comando seguente per recuperare il valore in testo normale del parametro. `/myapp/dev/vendor/merchant-id` L'`--with-decryption` opzione indica di Parameter Store restituire il valore decrittografato.

```
aws ssm get-parameter \
 --region us-east-1 \
 --name "/myapp/dev/vendor/merchant-id" \
 --with-decryption
```

L'output seguente mostra il valore in testo normale.

```
{
 "Parameter": {
 "Name": "/myapp/dev/vendor/merchant-id",
 "Type": "SecureString",
 "Value": "merchant-739482",
 "Version": 1,
 "LastModifiedDate": "2026-06-25T17:27:56.401000+00:00",
 "ARN": "arn:aws:ssm:us-east-1:111122223333:parameter/myapp/dev/vendor/merchant-id",
 "DataType": "text"
 }
}
```



## Fase 6: Aggiornamento di un parametro

Esegui il comando seguente per aggiornare il valore del `/myapp/dev/log-level` parametro da `INFO` a `DEBUG`. L' `--overwrite` opzione consente al comando di sostituire il valore esistente.

```
aws ssm put-parameter \
 --region us-east-1 \
 --name "/myapp/dev/log-level" \
 --type "String" \
 --value "DEBUG" \
 --overwrite
```

Parameter Store crea una nuova versione del parametro ogni volta che lo si aggiorna, come mostrato nell'output.

```
{
 "Version": 2,
 "Tier": "Standard"
}
```

Eseguite il [comando](#) `get-parameter-history` per visualizzare la cronologia del parametro. `/myapp/dev/log-level`

```
aws ssm get-parameter-history \
 --region us-east-1 \
 --name "/myapp/dev/log-level"
```

La risposta include le versioni precedenti del parametro, inclusi il numero di versione, il valore, il tipo e la data dell'ultima modifica.

```
{
 "Parameters": [
 {
 "Name": "/myapp/dev/log-level",
 "Type": "String",
 "Value": "INFO",
 "Version": 1,
 "LastModifiedDate": "2026-06-25T15:30:00.000000-04:00",
 "DataType": "text"
 },
 {
```

```

 "Name": "/myapp/dev/log-level",
 "Type": "String",
 "Value": "DEBUG",
 "Version": 2,
 "LastModifiedDate": "2026-06-25T15:35:00.000000-04:00",
 "DataType": "text"
 }
]
}

```

## Fase 7: Recupera i parametri in base al percorso

Esegui il [comando](#) `get-parameters-by-path` per recuperare i parametri sotto il percorso `/myapp/dev/`. L'opzione `--recursive` include parametri nei livelli inferiori della gerarchia.

```

aws ssm get-parameters-by-path \
 --region us-east-1 \
 --path "/myapp/dev/" \
 --recursive

```

L'output mostra entrambi i parametri che hai creato. Il `SecureString` parametro è crittografato.

```

{
 "Parameters": [
 {
 "Name": "/myapp/dev/log-level",
 "Type": "String",
 "Value": "DEBUG",
 "Version": 2,
 "LastModifiedDate": "2026-06-25T17:35:39.184000+00:00",
 "ARN": "arn:aws:ssm:us-east-1:111122223333:parameter/myapp/dev/log-level",
 "DataType": "text"
 },
 {
 "Name": "/myapp/dev/vendor/merchant-id",
 "Type": "SecureString",
 "Value": "AQICAHh1cV16RSGzfLARDIKV0croMvax6aMUDP1thWREL5ToawG6q+Xj8K...==",
 "Version": 1,
 "LastModifiedDate": "2026-06-25T17:27:56.401000+00:00",
 "ARN": "arn:aws:ssm:us-east-1:111122223333:parameter/myapp/dev/vendor/merchant-id",
 "DataType": "text"
 }
]
}

```

```
]
}
```

Esegui il comando seguente per recuperare i parametri contenuti nel `/myapp/dev/` percorso e restituire i valori decrittografati per tutti i `SecureString` parametri che il principale è autorizzato a decrittografare.

```
aws ssm get-parameters-by-path \
 --region us-east-1 \
 --path "/myapp/dev/" \
 --recursive \
 --with-decryption
```

## Fase 8: Eliminare un parametro

Esegui il comando seguente per eliminare il `/myapp/dev/log-level` parametro.

```
aws ssm delete-parameter \
 --region us-east-1 \
 --name "/myapp/dev/log-level"
```

## Eliminazione

Eseguite il comando seguente per eliminare i restanti parametri di esempio.

```
aws ssm delete-parameters \
 --region us-east-1 \
 --names "/myapp/dev/subnet-ids" "/myapp/dev/vendor/merchant-id"
```

## Fasi successive

Dopo aver creato i primi parametri, considerate i seguenti passaggi successivi:

- Definisci una convenzione di denominazione per applicazioni, ambienti e team. Per ulteriori informazioni, consulta <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-paramstore-hierarchies.html#ps-hierarchy-examples>.

- Usa le policy IAM per controllare chi può leggere o aggiornare ogni percorso dei parametri.
- Utilizzale `SecureString` per i valori di configurazione che richiedono la crittografia, come gli endpoint di servizio e gli identificatori degli account. Per informazioni segrete, come credenziali di database, chiavi API o token, consigliamo di utilizzare questa soluzione che fornisce controlli di sicurezza appositamente progettati AWS Secrets Manager, tra cui la rotazione automatica e la replica tra regioni.
- Da utilizzare AWS AppConfig per contrassegnare le funzionalità e configurare dinamicamente le applicazioni.

#### Note

Per i contrassegni di funzionalità e la configurazione che cambiano in fase di esecuzione, AWS AppConfig si estende Parameter Store con diverse funzionalità di sicurezza dell'implementazione. Queste includono la convalida prima della distribuzione (JSON Schema o Lambda), il rollout graduale, il rollback automatico su un allarme Amazon CloudWatch configurato e la memorizzazione nella cache locale tramite l'agente. AWS AppConfig Per saperne di più, vedi Che cos'è? [AWS AppConfig](#)

## Configurazione Parameter Store

Prima di impostare i parametri in Parameter Store, configura le policy AWS Identity and Access Management (IAM) che forniscono ai titolari del tuo account il permesso di eseguire le azioni specificate.

In questa sezione, imparerai come configurare manualmente queste policy utilizzando la console IAM e come assegnarle a utenti e gruppi di utenti. È inoltre possibile creare e assegnare policy per controllare quali operazioni di parametro vengono eseguite su un nodo gestito.

Questa sezione spiega anche come creare EventBridge regole Amazon che consentano di ricevere notifiche sulle modifiche ai parametri di Systems Manager. Puoi utilizzare EventBridge le regole per richiamare altre azioni in AWS base alle modifiche apportate. Parameter Store

### Indice

- [Gestire l'accesso a Parameter Store parametri che utilizzano le politiche IAM](#)
- [Scelta dei livelli di parametri in Parameter Store](#)

- [Gestione Parameter Store velocità di trasmissione effettiva](#)
- [Impostazione delle notifiche o delle azioni di attivazione basate su Parameter Store eventi](#)

Gestire l'accesso a Parameter Store parametri che utilizzano le politiche IAM

Il responsabile IAM che accede ai AWS Systems Manager parametri deve disporre dell'autorizzazione per eseguire le azioni SSM richieste. Il principale può essere un utente IAM, un ruolo IAM, un profilo di istanza Amazon EC2, un ruolo di esecuzione Lambda, un ruolo di attività Amazon ECS, un ruolo di servizio o un CodeBuild altro ruolo di servizio. AWS

La tabella seguente descrive le autorizzazioni IAM richieste per diverse azioni. Parameter Store

| Azione                                                | Privilegi IAM richiesti              | Informazioni di riferimento         |
|-------------------------------------------------------|--------------------------------------|-------------------------------------|
| Creare o aggiornare un parametro                      | <code>ssm:PutParameter</code>        | <a href="#">PutParameter</a>        |
| Recupera un parametro                                 | <code>ssm:GetParameter</code>        | <a href="#">GetParameter</a>        |
| Recupera più parametri denominati                     | <code>ssm:GetParameters</code>       | <a href="#">GetParameters</a>       |
| Recupera i parametri in un percorso                   | <code>ssm:GetParametersByPath</code> | <a href="#">GetParametersByPath</a> |
| Visualizza i metadati dei parametri                   | <code>ssm:DescribeParameters</code>  | <a href="#">DescribeParameters</a>  |
| Visualizza la cronologia delle versioni dei parametri | <code>ssm:GetParameterHistory</code> | <a href="#">GetParameterHistory</a> |
| Eliminare un parametro                                | <code>ssm&gt;DeleteParameter</code>  | <a href="#">DeleteParameter</a>     |
| Eliminare più parametri                               | <code>ssm&gt;DeleteParameters</code> | <a href="#">DeleteParameters</a>    |

Quando si utilizzano politiche IAM per concedere l'accesso ai parametri di Systems Manager, si consiglia di creare e utilizzare politiche IAM restrittive. Ad esempio, la seguente politica consente a un responsabile di chiamare le operazioni `GetParameters` API `DescribeParameters` e per un

set limitato di risorse. Il principale può ottenere informazioni e utilizzare tutti i parametri che iniziano con `prod-*`.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:DescribeParameters"
],
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "ssm:GetParameters"
],
 "Resource": "arn:aws:ssm:us-east-1:111122223333:parameter/prod-*"
 }
]
}
```

### Note

La politica precedente consente `ssm:GetParameters` ma non le altre azioni di recupero. Parameter Store autorizza ogni operazione di recupero in base alla propria azione IAM, quindi consentire o negare un'azione non influisce sulle altre. Prima di affidarti a una policy per limitare i parametri che un responsabile può leggere, vedere e [In che modo Parameter Store autorizza il recupero dei parametri](#) [Limitazione dell'accesso a parametri e percorsi specifici](#)

### Important

Parameter Store autorizza l'operazione `GetParametersByPath` in base al percorso specificato nella richiesta, non in base a ciascun parametro restituito dall'operazione. Un

principale a cui è consentito richiamare `GetParametersByPath` il percorso `/a` riceve tutti i parametri inclusi in quel percorso, inclusi `/a/b`. Ciò è vero anche se la stessa politica nega esplicitamente l'accesso `/a/b` ad altre azioni.

Per impedire la restituzione di un parametro `GetParametersByPath`, negare l'azione `ssm:GetParametersByPath` su ogni percorso predecessore che potrebbe includere il parametro nei risultati. Ad esempio, per `/a/b` evitare che venga restituito, nega sia `ssm:GetParametersByPath` per `che. /a /`

Agli amministratori fidati è possibile concedere l'accesso a tutte le operazioni API relative ai parametri di Systems Manager mediante una policy simile a quella riportata nell'esempio seguente. Questa policy concede all'utente l'accesso completo a tutti i parametri di produzione che iniziano con `dbserver-prod-*`.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:PutParameter",
 "ssm>DeleteParameter",
 "ssm:GetParameterHistory",
 "ssm:GetParametersByPath",
 "ssm:GetParameters",
 "ssm:GetParameter",
 "ssm>DeleteParameters"
],
 "Resource": "arn:aws:ssm:us-east-1:111122223333:parameter/dbserver-
prod-*"
 },
 {
 "Effect": "Allow",
 "Action": "ssm:DescribeParameters",
 "Resource": "*"
 }
]
}
```

## Negare le autorizzazioni

Ogni API è univoca e dispone di operazioni e autorizzazioni distinte che può consentire o negare singolarmente. Un rifiuto esplicito in una policy sostituisce il permesso.

### Important

Poiché ogni operazione è autorizzata in base alla propria azione IAM, il rifiuto di una singola azione non impedisce a un principale di recuperare lo stesso parametro tramite un'altra operazione. Ad esempio, la negazione `ssm:GetParameter` da sola non ha alcun effetto su `ssm:GetParameters`, o. `ssm:GetParameterHistory` `ssm:GetParametersByPath`. Nega sempre ogni azione che può restituire il valore. Per una descrizione completa di questo comportamento, consulta [In che modo Parameter Store autorizza il recupero dei parametri](#).

### Note

La chiave default AWS Key Management Service (AWS KMS) è `Decrypt` autorizzata per tutti i principali IAM all' Account AWS interno di. Se desideri livelli di accesso diversi ai `SecureString` parametri del tuo account, non ti consigliamo di utilizzare la chiave predefinita. La limitazione dell'`kms:Decrypt` uso di una chiave gestita dal cliente impedisce la decrittografia di un `SecureString` valore tramite qualsiasi operazione di recupero. Per ulteriori informazioni, consulta [Limitazione della decrittografia dei valori dei parametri SecureString](#).

Tutti e quattro i nomi delle azioni di recupero iniziano con `GetParameter`, quindi la singola voce include,, e. `ssm:GetParameter*` `ssm:GetParameter` `ssm:GetParameters` `ssm:GetParameterHistory` `ssm:GetParametersByPath`. L'esempio seguente utilizza questo modello per negare tutte e quattro le azioni per tutti i parametri che iniziano con. `prod-*`

## JSON

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



```

 "Action": [
 "ssm:GetParameter*"
],
 "Resource": "arn:aws:ssm:us-east-1:111122223333:parameter/prod-*"
 }
]
}

```

### Note

Nell'esempio precedente, il deny on `ssm:GetParametersByPath` si applica solo alle chiamate che richiedono una corrispondenza del percorso. `prod-*` Non impedisce la restituzione di un `prod-*` parametro da una chiamata che richiede un percorso predecessore. Per colmare questa lacuna, `ssm:GetParametersByPath` nega anche i percorsi antenati. Per ulteriori informazioni, consulta [Limitazione dell'accesso a parametri e percorsi specifici](#).

Nell'esempio seguente viene illustrato come negare alcuni comandi consentendo all'utente di eseguire altri comandi su tutti i parametri che iniziano con `prod-*`.

### JSON

```

{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Deny",
 "Action": [
 "ssm:PutParameter",
 "ssm:DeleteParameter",
 "ssm:DeleteParameters",
 "ssm:DescribeParameters"
],
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "ssm:GetParametersByPath",

```

```

 "ssm:GetParameters",
 "ssm:GetParameter",
 "ssm:GetParameterHistory"
],
 "Resource": "arn:aws:ssm:us-east-1:111122223333:parameter/prod-*"
}
]
}

```

### Note

La cronologia dei parametri include tutte le versioni dei parametri, inclusa quella attuale. Pertanto, se a un utente viene negata l'autorizzazione per `GetParameter`, `GetParameters`, e `GetParametersByPath` ma è consentito il permesso per `GetParameterHistory`, possono vedere il parametro corrente, inclusi i parametri `SecureString`, tramite `GetParameterHistory`.

Lo stesso comportamento si applica all'eliminazione. `ssm:DeleteParameters` è autorizzato indipendentemente da `ssm:DeleteParameter`, quindi la sola negazione `ssm:DeleteParameter` non impedisce al principale di eliminare il parametro con l'operazione. `DeleteParameters` Negate entrambe le azioni o utilizzate lo schema. `ssm:DeleteParameter*`

### Crittografia e decrittografia dei parametri utilizzando AWS KMS keys

Parameter Store `SecureString` i parametri utilizzano AWS KMS chiavi per la crittografia. AWS KMS crittografa il valore utilizzando una chiave gestita dal cliente Chiave gestita da AWS o una chiave gestita dal cliente. Per ulteriori informazioni su AWS KMS e AWS KMS key, consulta la Guida [per gli AWS Key Management Service sviluppatori](#).

Tutti gli utenti all'interno dell'account cliente hanno accesso alla chiave AWS gestita predefinita. Puoi individuare l'Amazon Resource Name (ARN) della chiave predefinita nella AWS KMS console nella [pagina delle chiavi](#) AWS gestite. La chiave predefinita è identificata `aws/ssm` nella colonna `Alias`. È possibile utilizzare la chiave predefinita per crittografare `SecureString` i parametri impedendo agli utenti di utilizzare i `SecureString` parametri. In questo caso, le policy IAM devono negare esplicitamente l'accesso alla chiave predefinita, come dimostrato nel seguente esempio di policy.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Deny",
 "Action": [
 "kms:Decrypt",
 "kms:GenerateDataKey"
],
 "Resource": [
 "arn:aws:kms:us-east-1:111122223333:key/abcd1234-ab12-cd34-ef56-abcdeEXAMPLE"
]
 }
]
}
```

Quando si utilizza una chiave gestita dal cliente, la policy IAM che concede l'accesso principale a un parametro o a un percorso di parametro deve fornire `kms:Encrypt` autorizzazioni esplicite per la chiave. Ad esempio, la seguente politica consente a un responsabile di creare, aggiornare e visualizzare SecureString i parametri che iniziano con `prod-` specificato. Regione AWS Account

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:PutParameter",
 "ssm:GetParameter",
 "ssm:GetParameters"
],
 "Resource": [
 "arn:aws:ssm:us-east-1:111122223333:parameter/prod-*"
]
 }
]
}
```

```
 },
 {
 "Effect": "Allow",
 "Action": [
 "kms:Decrypt",
 "kms:Encrypt",
 "kms:GenerateDataKey"
],
 "Resource": [
 "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-12345EXAMPLE"
]
 }
]
}
```

#### Note

L'autorizzazione `kms:GenerateDataKey` è necessaria per creare parametri avanzati crittografati utilizzando la chiave gestita dal cliente specificata.

Se hai bisogno di un controllo di accesso dettagliato sui `SecureString` parametri del tuo account, utilizza una chiave gestita dal cliente per proteggere e limitare l'accesso a questi parametri. Ti consigliamo inoltre di utilizzarla AWS CloudTrail per monitorare le attività relative ai parametri `SecureString`.

Per ulteriori informazioni, consulta i seguenti argomenti:

- [Logica di valutazione delle policy](#) nella Guida per l'utente IAM
- [Utilizzo delle policy chiave AWS KMS](#) nella Guida per gli sviluppatori di AWS Key Management Service
- [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#) nella Guida AWS CloudTrail per l'utente

Consentire ai nodi gestiti di accedere a parametri specifici

Per controllare quali Parameter Store parametri può recuperare un nodo gestito, puoi allegare una policy IAM al ruolo dell'istanza. Se si sceglie il tipo di `SecureString` parametro al momento della

creazione del parametro, Systems Manager lo utilizza AWS KMS per crittografare il valore del parametro. È possibile visualizzarlo Chiave gestita da AWS eseguendo il seguente comando da AWS CLI

```
aws kms describe-key --key-id alias/aws/ssm
```

L'esempio seguente consente ai nodi di ottenere un valore di parametro solo per i parametri che iniziano con prod-. Se il parametro è un parametro SecureString, il nodo decrittografa la stringa utilizzando AWS KMS.

#### Note

Le policy dell'istanza, come nell'esempio seguente, sono assegnate al ruolo dell'istanza in IAM. Per ulteriori informazioni sulla configurazione dell'accesso alle funzionalità di Systems Manager, tra le quali come assegnare policy a utenti e istanze, consulta [Gestire le istanze EC2 con Systems Manager](#).

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:GetParameters"
],
 "Resource": [
 "arn:aws:ssm:us-east-1:111122223333:parameter/prod-*"
]
 },
 {
 "Effect": "Allow",
 "Action": [
 "kms:Decrypt"
],
 "Resource": [
 "arn:aws:kms:us-east-1:111122223333:key/4914ec06-e888-4ea5-a371-5b88eEXAMPLE"
]
 }
]
}
```

```

]
 }
]
}

```

## Scelta dei livelli di parametri in Parameter Store

Per controllare gli attributi di memorizzazione dei parametri, Parameter Store include parametri standard e parametri avanzati. Ogni parametro viene configurato singolarmente per un account e una regione. Il livello dei parametri determina la dimensione massima del valore di un parametro, il numero di parametri in un livello specifico che è possibile creare, se è possibile utilizzare le politiche relative ai parametri e se vengono applicati costi.

I livelli dei parametri sono diversi dalla velocità effettiva dei parametri. I livelli controllano gli attributi di memorizzazione dei parametri, mentre il throughput controlla la frequenza delle richieste.

### Livelli di parametri standard e avanzati

La tabella seguente descrive le differenze tra i livelli.

La tabella seguente descrive le differenze tra i livelli dei parametri.

| Caratteristica o caso d'uso                             | Standard                                                                                                                              | Avanzata                                                                                      |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Caso d'uso                                              | Ideale per la maggior parte dei dati di configurazione e dei carichi di lavoro su piccola scala. Questa è l'impostazione predefinita. | Ideale quando sono necessari limiti più elevati, valori più elevati o politiche di parametri. |
| Parametri massimi<br>(per Account AWS mano Regione AWS) | 10.000                                                                                                                                | 100.000                                                                                       |
| Dimensione massima del valore                           | 4 KB                                                                                                                                  | 8 KB                                                                                          |
| Politiche relative ai parametri                         | Non supportata                                                                                                                        | Supportata                                                                                    |

| Caratteristica o caso d'uso     | Standard                | Avanzata                                                                                                                         |
|---------------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------|
|                                 |                         | Per ulteriori informazioni, consulta <a href="#">Assegnazione delle politiche dei parametri in Parameter Store</a> .             |
| Condivisibilità tra Account AWS | Non supportata          | Supportata<br><br>Per ulteriori informazioni, consulta <a href="#">Utilizzo di parametri condivisi in Parameter Store</a> .      |
| Capacità di upgrade e downgrade | Aggiornabile            | Non declassabile                                                                                                                 |
| Costo                           | Nessun costo aggiuntivo | Soggetto a costi<br><br>Per ulteriori informazioni, consulta <a href="#">Prezzi di AWS Systems Manager per Parameter Store</a> . |

Per un elenco completo di quote e limiti Parameter Store, consulta gli [endpoint e le quote di AWS Systems Manager](#) nel Riferimento ad AWS generale.

Livello predefinito e impostazioni dei livelli dei singoli parametri

Parameter Store supporta le seguenti impostazioni correlate:

- Livello di parametro predefinito per la tua regione Account AWS e la tua regione

Questa impostazione controlla il livello Parameter Store utilizzato quando crei un nuovo parametro e non specifica esplicitamente un livello. È possibile impostare il valore predefinito su Standard, Advanced, o Intelligent-Tiering.

- Livello per un singolo parametro

È possibile specificare il livello quando si crea o si aggiorna un singolo parametro. È possibile modificare un parametro standard in un parametro avanzato, ma non è possibile modificare un parametro avanzato in un parametro standard.

Il livello del parametro predefinito è separato dal livello di un singolo parametro. La modifica del livello dei parametri predefinito ha effetto solo sui nuovi parametri creati senza specificare un livello. I parametri esistenti non sono interessati.

### Visualizzazione delle impostazioni del livello dei parametri

Puoi visualizzare l'impostazione del livello predefinito per la tua regione Account AWS e l'impostazione del livello per ogni singolo parametro.

### Visualizza il livello di parametro predefinito

Per visualizzare il livello di parametri predefinito per la tua regione Account AWS e per la tua regione, usa l'azione. L'esempio seguente recupera il livello di parametro predefinito.

```
aws ssm get-service-setting \
 --region us-east-1 \
 --setting-id arn:aws:ssm:us-east-1:111122223333:servicesetting/ssm/parameter-store/
default-parameter-tier
```

Il seguente esempio mostra un output campione.

```
{
 "ServiceSetting": {
 "SettingId": "/ssm/parameter-store/default-parameter-tier",
 "SettingValue": "Standard",
 "Status": "Default"
 }
}
```

### Visualizza il livello per un parametro specifico

Per visualizzare il livello per un parametro specifico, usa l'azione. L'esempio seguente restituisce il livello del parametro/myapp/dev/log-level.

```
aws ssm describe-parameters \
```



```
--region us-east-1 \
--parameter-filters "Key=Name,Option=Equals,Values=/myapp/dev/log-level" \
--query "Parameters[0].Tier" \
--output text
```

Il comando restituisce il livello del parametro, ad esempio Standard o Advanced.

### Argomenti

- [Specificare un livello di parametro predefinito per il Account AWS and Regione AWS](#)
- [Modifica di un parametro standard in un parametro avanzato](#)
- [Limitazioni alla modifica dei livelli per i singoli parametri](#)

### Specificare un livello di parametro predefinito per il Account AWS and Regione AWS

Se si crea o si aggiorna un parametro ma non si specifica un livello di parametro nel comando, l'impostazione del livello predefinito determina il livello. Per impostazione predefinita, Parameter Store imposta l'impostazione predefinita sul livello dei parametri standard.

### Opzioni predefinite del livello dei parametri

I parametri standard sono disponibili gratuitamente, ma sono soggetti a restrizioni relative a dimensioni e funzionalità, come descritto in [Livelli di parametri standard e avanzati](#). Se il tuo caso d'uso richiede funzionalità o limiti che i parametri standard non supportano, valuta la possibilità di impostare il livello avanzato come predefinito. Il livello avanzato offre limiti più elevati e funzionalità aggiuntive, a un costo. Per ulteriori informazioni, consulta [Prezzi di AWS Systems Manager per Parameter Store](#).

Puoi modificare le impostazioni del livello Parameter Store predefinito in qualsiasi momento utilizzando l'[UpdateServiceSetting](#) API. Imposta il valore predefinito del livello del parametro su StandardAdvanced,, o Intelligent-Tiering.

Per massimizzare l'efficienza e ridurre i costi, considera l'impostazione Intelligent-Tiering come valore predefinito. Questa impostazione determina se utilizzare il livello standard o avanzato in base al contenuto della richiesta. Ad esempio, se si crea un parametro che soddisfa i criteri di un parametro standard, il tiering intelligente crea il parametro nel livello standard. Se si crea un parametro in cui uno o più criteri non soddisfano i requisiti del livello standard, il tiering intelligente crea il parametro nel livello avanzato.

Il tiering intelligente offre i seguenti vantaggi:

## Controllo dei costi

Il tiering intelligente consente di controllare i costi relativi ai parametri creando sempre parametri standard, a meno che la richiesta non richieda il livello avanzato.

### Aggiornamento automatico al livello avanzato

Quando apporti una modifica al codice che richiede l'aggiornamento di un parametro standard a un parametro avanzato, il tiering intelligente gestisce la conversione per te. Non è necessario modificare il codice per gestire l'aggiornamento. Di seguito sono riportati alcuni esempi di casi d'uso:

- AWS CloudFormation I tuoi modelli forniscono numerosi parametri quando vengono eseguiti. Quando questo processo ti fa raggiungere la quota di 10.000 parametri nel livello dei parametri standard, ti aggiorna Intelligent-Tiering automaticamente al livello dei parametri avanzati e i tuoi processi non vengono interrotti. CloudFormation
- Puoi archiviare un valore di certificato in un parametro, ruotare il valore del certificato regolarmente e il contenuto è inferiore alla quota di 4 KB del livello dei parametri standard. Se il valore di un certificato sostitutivo supera i 4 KB, aggiorna Intelligent-Tiering automaticamente il parametro al livello dei parametri avanzati.
- È opportuno associare numerosi parametri standard esistenti a una policy dei parametri, che richiede il livello dei parametri avanzati. Invece di includere nelle chiamate `PutParameter` l'opzione `AdvancedOptions` di aggiornamento dei parametri, aggiorna Intelligent-Tiering automaticamente i parametri al livello avanzato.

### Configurazione delle autorizzazioni per specificare un Parameter Store livello predefinito

Verifica di disporre dell'autorizzazione in AWS Identity and Access Management (IAM) per modificare il livello di parametro predefinito Parameter Store effettuando una delle seguenti operazioni:

- Accertati di collegare la policy `AdministratorAccess` all'entità IAM (come l'utente, il gruppo o il ruolo).
- Assicuratevi di disporre delle autorizzazioni per modificare l'impostazione del livello predefinito utilizzando le operazioni API seguenti:
  - [GetServiceSetting](#)
  - [UpdateServiceSetting](#)
  - [ResetServiceSetting](#)

Concedi le seguenti autorizzazioni all'entità IAM per consentire a un utente di visualizzare e modificare l'impostazione del piano predefinita per i parametri in una specifica Regione AWS in un Account AWS.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:GetServiceSetting"
],
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "ssm:UpdateServiceSetting"
],
 "Resource": "arn:aws:ssm:us-east-1:111122223333:servicesetting/ssm/parameter-store/default-parameter-tier"
 }
]
}
```

Gli amministratori possono specificare l'autorizzazione di sola lettura assegnando le seguenti autorizzazioni.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:GetServiceSetting"
],

```

```
 "Resource": "*"
 },
 {
 "Effect": "Deny",
 "Action": [
 "ssm:ResetServiceSetting",
 "ssm:UpdateServiceSetting"
],
 "Resource": "*"
 }
]
 }
}
```

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.

Impostazione del Parameter Store livello predefinito utilizzando la console, AWS CLI, o PowerShell

Per impostazione predefinita, Parameter Store imposta l'impostazione predefinita sul livello dei parametri standard. È possibile impostare il livello dei parametri predefinito per la propria Account AWS regione utilizzando la console di Systems Manager, AWS CLI, o PowerShell. Ad esempio, è possibile modificare il livello predefinito in avanzato e quindi di nuovo in standard.

## Console

La procedura seguente mostra come utilizzare la console di Systems Manager per impostare il livello di parametri predefinito per l'attuale Account AWS e Regione AWS.

Per impostare il Parameter Store livello predefinito

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Parameter Store.
3. Seleziona la scheda Impostazioni.
4. Scegli Gestisci impostazioni.
5. Nella sezione Parameter default tier, scegliete un'opzione. Per informazioni su queste opzioni, consulta [Specificare un livello di parametro predefinito per il Account AWS and Regione AWS](#).
6. Se richiesto, seleziona l'opzione per approvare le modifiche e autorizzare gli addebiti. Scegliere Save settings (Salva impostazioni).

Per modificare l'impostazione del livello predefinito in un secondo momento, ripeti i passaggi precedenti e specifica un'opzione diversa per il livello predefinito.

## CLI

La procedura seguente mostra come AWS CLI utilizzare il livello di parametro predefinito per l'attuale Account AWS e Regione AWS.

Per impostare il Parameter Store livello predefinito utilizzando AWS CLI

1. Apri AWS CLI ed esegui il seguente comando per impostare l'impostazione del livello di parametro predefinito per uno specifico Regione AWS in un Account AWS.

```
aws ssm update-service-setting \
 --region region \
 --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/parameter-
store/default-parameter-tier \
 --setting-value tier-option
```

*region* rappresenta l'identificatore di una regione Regione AWS supportata da AWS Systems Manager, ad esempio us-east-2 per la regione Stati Uniti orientali (Ohio). Per un

elenco dei *region* valori supportati, vedere la colonna Regione negli endpoint [del servizio Systems Manager](#) in. Riferimenti generali di Amazon Web Services

*tier-opzioni* valori includono StandardAdvanced, e. Intelligent-Tiering Per informazioni su queste opzioni, consulta [Specificare un livello di parametro predefinito per il Account AWS and Regione AWS](#).

Se il comando va a buon fine, non viene generato output.

2. Esegui il comando seguente per visualizzare le impostazioni predefinite correnti del servizio a livello di parametro Parameter Store nell'attuale Account AWS e Regione AWS.

```
aws ssm get-service-setting \
 --region region \
 --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/parameter-
store/default-parameter-tier
```

Il comando restituisce un risultato simile al seguente.

```
{
 "ServiceSetting": {
 "SettingId": "/ssm/parameter-store/default-parameter-tier",
 "SettingValue": "Advanced",
 "LastModifiedDate": 1556551683.923,
 "LastModifiedUser": "arn:aws:sts::123456789012:assumed-role/
Administrator/Jasper",
 "ARN": "arn:aws:ssm:us-east-2:123456789012:servicesetting/ssm/parameter-
store/default-parameter-tier",
 "Status": "Customized"
 }
}
```

Per modificare nuovamente l'impostazione del livello predefinito, ripeti questa procedura e specifica un'*SettingValue* opzione diversa.

## PowerShell

La procedura seguente mostra come utilizzare gli Strumenti per Windows PowerShell per impostare il livello di parametro predefinito per uno specifico Regione AWS account Amazon Web Services.

## Per impostare Parameter Store livello predefinito utilizzando PowerShell

1. Imposta il livello Parameter Store predefinito nel livello corrente Account AWS e Regione AWS utilizzando AWS Strumenti per PowerShell (Strumenti per PowerShell).

```
Update-SSMServiceSetting -SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/parameter-store/default-parameter-tier" -SettingValue "tier-option" -Region region
```

*region* rappresenta l'identificatore di una regione Regione AWS supportata da AWS Systems Manager, ad esempio us-east-2 per la regione Stati Uniti orientali (Ohio). Per un elenco dei *region* valori supportati, vedere la colonna Regione negli endpoint [del servizio](#) Systems Manager in. Riferimenti generali di Amazon Web Services

*tier-option* valori includono StandardAdvanced, e. Intelligent-Tiering Per informazioni su queste opzioni, consulta [Specificare un livello di parametro predefinito per il Account AWS and Regione AWS](#).

Se il comando va a buon fine, non viene generato output.

2. Esegui il comando seguente per visualizzare le impostazioni predefinite correnti del servizio a livello di parametro Parameter Store nell'attuale Account AWS e Regione AWS.

```
Get-SSMServiceSetting -SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/parameter-store/default-parameter-tier" -Region region
```

*region* rappresenta l'identificatore di una regione Regione AWS supportata da AWS Systems Manager, ad esempio us-east-2 per la regione Stati Uniti orientali (Ohio). Per un elenco dei *region* valori supportati, vedere la colonna Regione negli endpoint [del servizio](#) Systems Manager in. Riferimenti generali di Amazon Web Services

Il comando restituisce un risultato simile al seguente.

```
ARN : arn:aws:ssm:us-east-2:123456789012:servicesetting/ssm/parameter-store/default-parameter-tier
LastModifiedDate : 4/29/2019 3:35:44 PM
LastModifiedUser : arn:aws:sts::123456789012:assumed-role/Administrator/Jasper
SettingId : /ssm/parameter-store/default-parameter-tier
SettingValue : Advanced
Status : Customized
```

Per modificare nuovamente l'impostazione del livello predefinito, ripetere questa procedura e specificare un `SettingValue` opzione diversa.

## Modifica di un parametro standard in un parametro avanzato

Utilizza la procedura seguente per convertire un parametro standard esistente in un parametro avanzato. Per informazioni su come creare un nuovo parametro avanzato, consulta [Creazione in corso Parameter Store parametri in Systems Manager](#).

### Console

Per convertire un parametro standard in un parametro avanzato

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Parameter Store.
3. Scegliere un parametro, quindi Modifica.
4. In Descrizione, immetti le informazioni su questo parametro.
5. Scegli Avanzato.
6. In Valore, immetti il valore di questo parametro. I parametri avanzati hanno un limite massimo di 8 KB.
7. Scegli Save changes (Salva modifiche).

### AWS CLI

È possibile sovrascrivere l'impostazione predefinita specificando il livello del parametro utilizzando l'[PutParameter](#) operazione. Ad esempio, potresti voler condividere il valore AMI predefinito tra AWS gli account. L' AWS CLI esempio seguente imposta esplicitamente il parametro tier su Advanced per il `default-ami` parametro in Linux & macOS.

```
aws ssm put-parameter \
 --region us-east-1 \
 --name "default-ami" \
 --type "String" \
 --value "t3.micro" \
 --tier "Advanced"
```



## Limitazioni alla modifica dei livelli per i singoli parametri

È possibile modificare un parametro standard in un parametro avanzato in qualsiasi momento. Non è possibile modificare un parametro avanzato in un parametro standard per i seguenti motivi:

- La modifica del parametro sul livello standard troncherebbe il valore del parametro da 8 KB a 4 KB, con conseguente perdita di dati.
- La modifica del parametro sul livello standard rimuoverebbe tutte le politiche associate al parametro.
- I parametri avanzati e standard utilizzano una diversa forma di crittografia.

Se non hai più bisogno o desideri eliminare i costi di un parametro avanzato, cancellalo e ricrealo come nuovo parametro standard.

Il livello di parametro predefinito è un'impostazione separata. È possibile modificare il livello di parametro predefinito per una regione Account AWS and da Standard a Advanced, quindi modificarlo nuovamente in Standard. L'impostazione del livello predefinito ha effetto solo sui nuovi parametri creati senza specificare un livello. I parametri esistenti non sono interessati.

Ad esempio, è possibile creare parametri mentre è Standard impostato il livello predefinito e quindi impostare il livello dei parametri predefinito su Advanced. I nuovi parametri creati senza specificare un livello utilizzano il Advanced livello. Successivamente è possibile ripristinare il livello predefinito Standard senza modificare il livello dei parametri esistenti.

I parametri avanzati sono a pagamento. Per ulteriori informazioni, consulta [Prezzi di AWS Systems Manager per Parameter Store](#).

## Gestione Parameter Store velocità di trasmissione effettiva

Parameter Store throughput definisce il numero di transazioni API al secondo (TPS) che Systems Manager è in grado di elaborare. L'impostazione del throughput si applica all'API nel Parameter Store suo insieme anziché a una singola API. Per impostazione predefinita, Parameter Store è configurata con una quota di throughput standard che è spesso adatta per carichi di lavoro di volume da basso a moderato. Per carichi di lavoro con volumi più elevati, puoi abilitare un throughput più elevato, il che aumenta il numero massimo di transazioni supportate al secondo per il tuo account e la tua regione. Puoi abilitare e disabilitare un throughput più elevato in base alle esigenze.

## Quote di produttività in Parameter Store

La tabella seguente elenca i limiti di transazione per diverse categorie di API utilizzando un throughput predefinito e superiore. Le azioni API includono l'utilizzo AWS della console, AWS CLI i comandi e le letture delle applicazioni. Per ulteriori informazioni sulle quote e sui limiti di velocità, consulta [AWS Systems Manager Endpoints and quotas](#).

| Operazioni dell'API                                                                                                                                                                         | Velocità di trasmissione effettiva predefinita              | Velocità di trasmissione effettiva più alta                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">GetParameter</a> , <a href="#">GetParameters</a> e <a href="#">GetParametersByPath</a>                                                                                          | 40 TPS<br>condiviso tra tutte e tre le azioni API combinate | <a href="#">GetParameter</a> : 10,000 TPS;<br><a href="#">GetParameters</a> : 1,000 TPS;<br><a href="#">GetParametersByPath</a> : 100 TPS |
| <a href="#">DeleteParameter</a> e <a href="#">DeleteParameters</a>                                                                                                                          | 3 TPS                                                       | 5 TPS                                                                                                                                     |
| <a href="#">DescribeParameters</a> , <a href="#">GetParameterHistory</a> , <a href="#">LabelParameterVersion</a> , <a href="#">UnlabelParameterVersion</a> , e <a href="#">PutParameter</a> | 3 TPS                                                       | 10 TPS                                                                                                                                    |

In questo contesto, una transazione è un'azione API per un account in una singola regione. Ad esempio, il comando seguente crea una singola transazione.

```
aws ssm get-parameter --name "/myapp/prod/log-level"
```

Le azioni API possono essere distribuite tra le applicazioni. Ad esempio, ciascuno dei seguenti scenari raggiunge il limite di throughput predefinito di 40 TPS:

- 1 applicazione effettua 40 `GetParameter` chiamate al secondo.
- 10 applicazioni effettuano 4 `GetParameter` chiamate al secondo.
- 40 applicazioni `GetParameter` effettuano 1 chiamata al secondo.

Un limite di velocità effettiva si applica a tutte le API all'interno di una categoria. Ad esempio, la seguente combinazione di chiamate simultanee di parametri per un'applicazione soddisfa il limite predefinito di 40 TPS per le API di recupero dei parametri:

- `GetParameter` effettua 25 chiamate al secondo.
- `GetParameter` effettua 10 chiamate al secondo.
- `GetParameterByPath` effettua 5 chiamate al secondo.

Le `DescribeParameters` chiamate hanno un limite di throughput separato. Un'applicazione può effettuare le chiamate precedenti effettuando anche 3 `DescribeParameters` chiamate al secondo senza superare il limite complessivo per la velocità effettiva standard.

Se le richieste di produzione superano un limite di produttività durante il funzionamento standard o nei periodi pianificati di traffico elevato, utilizzate le seguenti tecniche di ottimizzazione.

#### Argomenti

- [Ottimizzazione della produttività in Parameter Store](#)
- [Modifica dell'impostazione della velocità effettiva in Parameter Store](#)

#### Ottimizzazione della produttività in Parameter Store

Quando Parameter Store riceve più richieste di parametri in un breve intervallo, l'applicazione può subire delle limitazioni. Ad esempio, CloudWatch i log o i log dell'applicazione mostrano `RateExceeded` gli errori generati dall'SDK quando chiama `GetParameter`, `ThrottlingException` `GetParameters` o `GetParametersByPath`. In altri casi, la logica applicativa riprova con successo le chiamate API, ma la latenza dell'applicazione aumenta. Il risultato può essere interruzioni delle applicazioni, esperienza utente non ottimale, implementazioni non riuscite, soluzioni alternative complesse e perdita di tempo per gli sviluppatori.

Diversi fattori possono far sì che l'applicazione raggiunga i limiti di quota, tra cui: Parameter Store

- L'applicazione si espande rapidamente a causa di un picco di traffico. Ad esempio, l'applicazione viene normalmente eseguita su 5 istanze Amazon EC2. Quando il traffico aumenta improvvisamente, Amazon EC2 Auto Scaling lancia altre 50 istanze. Se ogni istanza legge i parametri all'avvio, le richieste combinate possono superare il limite di richieste predefinito.

- Il tuo servizio container avvia molte attività contemporaneamente. Ad esempio, un servizio Amazon ECS potrebbe avviare molte attività sostitutive durante un aggiornamento e ciascuna attività potrebbe leggere le impostazioni dal Parameter Store momento dell'avvio.
- Le tue funzioni Lambda ricevono molte richieste contemporaneamente. Ad esempio, Lambda potrebbe avviare molti ambienti funzionali per gestire l'aumento del traffico. Ogni ambiente funzionale potrebbe leggere i parametri all'avvio.
- Il processo di compilazione o rilascio legge molti parametri in un breve intervallo di tempo. Ad esempio, un processo di compilazione potrebbe leggere le impostazioni per diverse applicazioni o ambienti.
- L'applicazione legge molti parametri in base al percorso. Ad esempio, l'applicazione legge ripetutamente tutti i parametri in esso contenuti `/myapp/prod/` anziché leggere solo i parametri specifici necessari. Queste richieste ripetute possono superare il limite di richieste predefinito.

Puoi risolvere il problema della Parameter Store limitazione nei seguenti modi complementari:

- Ridurre la produttività

L'applicazione potrebbe recuperare più dati del necessario o recuperarli in modo inefficiente.

- Consentire un throughput più elevato

È possibile aumentare la resilienza delle applicazioni aumentando la quota di throughput per una regione e un account specificati. Puoi abilitare e disabilitare l'impostazione di throughput più elevato in qualsiasi momento per i periodi di traffico elevato. Per i carichi di lavoro di produzione che generano regolarmente errori di limitazione, valuta la possibilità di abilitare l'impostazione in modo permanente.

## Ridurre la produttività in Parameter Store

Indipendentemente dal fatto che utilizzi una velocità effettiva standard o superiore, controlla la frequenza e il tipo di chiamate verso Parameter Store. In alcuni casi, puoi ridurre il numero di richieste senza modificare i parametri. Poiché il costo è determinato in base all'utilizzo anziché a un modello di abbonamento o di livello, il risultato è un minor numero di interazioni API fatturate.

- Memorizza nella cache i valori dei parametri nell'applicazione anziché leggere gli stessi valori per ogni richiesta.

Ad esempio, se l'applicazione legge `/myapp/prod/log-level` molte volte al minuto, può leggere il valore una volta e riutilizzarlo per un breve periodo di tempo. Questa tecnica riduce le chiamate ripetute a `Parameter Store`. Scegli un periodo di riutilizzo più breve per i valori che cambiano spesso e un periodo di riutilizzo più lungo per i valori che cambiano raramente.

- Usalo [GetParameters](#) quando conosci i nomi di più parametri.

Ad esempio, invece di effettuare [GetParameter](#) chiamate separate per i parametri `/myapp/prod/database/host` `/myapp/prod/log-level` `/myapp/prod/vendor/merchant-id`, è possibile recuperare un elenco di questi parametri in un'unica `GetParameters` richiesta.

- Evita di leggere più parametri di quelli necessari all'applicazione.

Se la tua applicazione richiede solo pochi parametri noti, usa `GetParameter` o `GetParameters` invece di leggere ripetutamente un intero percorso, ad esempio `/myapp/prod/`. Da utilizzare [GetParametersByPath](#) quando l'applicazione richiede un gruppo di parametri all'interno di un percorso. Quando si utilizza un throughput più elevato, la `GetParameter` quota è 100 volte la quota per `GetParametersByPath`.

- Il parametro `Spread out` viene letto quando molte risorse vengono avviate contemporaneamente.

Ad esempio, se molte istanze di Amazon EC2 o attività di Amazon ECS vengono avviate durante un aggiornamento, evita che tutte le risorse leggano i parametri esattamente nello stesso momento. Le quote sono al secondo. Ove possibile, leggete i parametri una volta e memorizzatene i valori nella cache dell'applicazione, oppure aggiungete un piccolo ritardo in modo che le richieste non avvengano tutte nello stesso secondo.

- Per le funzioni Lambda, considera l'utilizzo dell'estensione Lambda [AWS Parameters and Secrets](#).

L'estensione può memorizzare i valori dei parametri localmente per il riutilizzo da parte della funzione. Questa tecnica può ridurre il numero di chiamate `Parameter Store` e può anche ridurre il tempo necessario per recuperare i valori dei parametri. Per un esempio dettagliato di questa tecnica, vedi [Uso dell'estensione Lambda AWS Parameter and Secrets per memorizzare nella cache parametri e segreti](#).

## Aumento del throughput in

Per carichi di lavoro con volumi più elevati, puoi abilitare un throughput più elevato. Questa impostazione aumenta il numero massimo di transazioni supportate al secondo per l'account e la regione, a un costo. Prendi in considerazione un throughput più elevato nei seguenti scenari:

- La tua applicazione ha bisogno temporaneo di un throughput più elevato.

Ad esempio, un negozio online potrebbe leggere i parametri più spesso durante i saldi del fine settimana. È possibile attivare un throughput più elevato prima dell'inizio della vendita e quindi tornare al throughput standard dopo la fine della vendita. Puoi abilitare o disabilitare un throughput più elevato in qualsiasi momento dalla pagina **Parameter Store Impostazioni** o utilizzando il **AWS CLI**.

- L'applicazione di produzione recupera regolarmente i parametri contemporaneamente e si imbatte in problemi di limitazione.

Il recupero simultaneo può avvenire quando più istanze, contenitori, funzioni o processi di compilazione leggono i parametri contemporaneamente. **Parameter Store** Considerare i seguenti esempi:

- La scalabilità dell'applicazione è rapida. Ad esempio, l'applicazione viene normalmente eseguita su 5 istanze Amazon EC2. Quando il traffico aumenta improvvisamente, Amazon EC2 Auto Scaling lancia altre 50 istanze. Se ogni istanza legge i parametri all'avvio, le richieste combinate possono superare il limite di richieste predefinito.
- Il tuo servizio container avvia molte attività contemporaneamente. Ad esempio, un servizio Amazon ECS potrebbe avviare molte attività sostitutive durante un aggiornamento e ciascuna attività potrebbe leggere le impostazioni dal **Parameter Store** momento dell'avvio.
- Le tue funzioni Lambda ricevono molte richieste contemporaneamente. Ad esempio, Lambda potrebbe avviare molti ambienti funzionali per gestire l'aumento del traffico. Ogni ambiente funzionale potrebbe leggere i parametri all'avvio.
- Il processo di compilazione o rilascio legge molti parametri in un breve intervallo di tempo. Ad esempio, un processo di compilazione potrebbe leggere le impostazioni per diverse applicazioni o ambienti.

### Considerazioni sui costi per una maggiore produttività

Per l'opzione a maggiore produttività, si applicano costi aggiuntivi. Per i prezzi e gli esempi attuali delle **Parameter Store API**, vedi [AWS Systems Manager Pricing](#).

I costi si basano sulle interazioni **Parameter Store API**. Un'interazione API è definita come un'interazione tra una richiesta API e un singolo parametro. Ad esempio, se una singola `GetParameter` richiesta restituisce 10 parametri, questa richiesta conta come 10 interazioni **Parameter Store API** ai fini della fatturazione.

Considera uno scenario in cui desideri passare a un throughput più elevato per un breve periodo di aumento del traffico. Il tuo negozio online organizza una vendita nel fine settimana ed effettua interazioni 1,000,000 Parameter Store API durante la vendita. Se il costo per una maggiore produttività in questo esempio è \$0.05 per interazioni 10,000 API, il costo aggiuntivo totale è approssimativo. \$5 Puoi tornare alla velocità effettiva standard al termine della vendita e smettere di incorrere in costi.

### Combinazione di livelli di produttività e parametri

Il throughput funziona indipendentemente dai livelli dei parametri. Mentre i livelli di parametro controllano i limiti di archiviazione e la disponibilità delle funzionalità, le impostazioni di throughput controllano il volume delle richieste. Per soddisfare i requisiti di prestazioni e scalabilità, puoi utilizzare contemporaneamente livelli e throughput.

Ad esempio, per supportare applicazioni semplici e a basso carico, puoi utilizzare parametri standard con throughput predefinito. Per supportare modelli di accesso su larga scala e ad alta frequenza, è possibile combinare parametri avanzati con un throughput più elevato. In generale, è necessario aumentare la velocità effettiva quando l'applicazione supera i limiti TPS predefiniti (ad esempio, durante sequenze di letture o scritture simultanee), indipendentemente dal livello di parametri utilizzato.

Per ulteriori informazioni sulla velocità effettiva massima e su altre Parameter Store quote, consulta Endpoints and quotas. [AWS Systems Manager](#)

### Modifica dell'impostazione della velocità effettiva in Parameter Store

Le seguenti procedure descrivono come utilizzare Systems Manager per modificare il numero di transazioni al secondo che Parameter Store possono essere elaborate per l'attuale Account AWS e Regione AWS. È possibile modificare l'impostazione in qualsiasi momento.

#### Console

##### Cambiare Parameter Store throughput utilizzando la console

#### Tip

Se non hai ancora creato un parametro, puoi usare AWS Command Line Interface (AWS CLI) o AWS Tools for Windows PowerShell per modificare la velocità effettiva. Per informazioni, consulta [Modifica dell'impostazione della velocità effettiva in Parameter Store](#).

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Parameter Store.
3. Seleziona la scheda Impostazioni.
4. Scegli Gestisci le impostazioni.
5. Nella sezione Parameter throughput, scegliete un'opzione.
6. Se richiesto, seleziona l'opzione per approvare le modifiche e autorizzare gli addebiti. Scegliere Save settings (Salva impostazioni).

## CLI

### Modificare Parameter Store throughput utilizzando AWS CLI

1. Apri AWS CLI ed esegui il `aws ssm update-service-setting` comando per aumentare o diminuire le transazioni al secondo che Parameter Store possono essere elaborate nell'attuale Account AWS e Regione AWS. L'esempio seguente aumenta il throughput a un livello elevato.

```
aws ssm update-service-setting \
--setting-id arn:aws:ssm:region:account-id:servicessetting/ssm/parameter-store/
high-throughput-enabled \
--setting-value true
```

Se il comando va a buon fine, non viene generato output. Per disattivare la velocità effettiva elevata, imposta su `--setting-value. false`

2. Esegui il comando seguente per visualizzare le impostazioni correnti del servizio di throughput Parameter Store nell'attuale Account AWS e. Regione AWS

```
aws ssm get-service-setting \
--setting-id arn:aws:ssm:region:account-id:servicessetting/ssm/parameter-store/
high-throughput-enabled
```

Questo sistema restituisce informazioni simili alle seguenti.

```
{
 "ServiceSetting": {
 "SettingId": "/ssm/parameter-store/high-throughput-enabled",
```



```

 "SettingValue": "true",
 "LastModifiedDate": 1556551683.923,
 "LastModifiedUser": "arn:aws:sts::123456789012:assumed-role/
Administrator/Jasper",
 "ARN": "arn:aws:ssm:us-east-2:123456789012:servicesetting/ssm/parameter-
store/high-throughput-enabled",
 "Status": "Customized"
 }
}

```

## PowerShell

### Modificare Parameter Store throughput utilizzando PowerShell

1. Aumentate o Parameter Store diminuite la produttività nella corrente Account AWS e Regione AWS utilizzando AWS Strumenti per PowerShell (Strumenti per PowerShell). L'esempio seguente imposta il throughput su un livello elevato.

```

Update-SSMServiceSetting -SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/parameter-store/high-throughput-enabled" -SettingValue
"true" -Region region

```

Se il comando va a buon fine, non viene generato output.

2. Eseguite il comando seguente per visualizzare le impostazioni correnti del servizio di throughput per Parameter Store l'attuale Account AWS e Regione AWS

```

Get-SSMServiceSetting -SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/parameter-store/high-throughput-enabled" -Region region

```

Questo sistema restituisce informazioni simili alle seguenti.

```

ARN : arn:aws:ssm:us-east-2:123456789012:servicesetting/ssm/
parameter-store/high-throughput-enabled
LastModifiedDate : 4/29/2019 3:35:44 PM
LastModifiedUser : arn:aws:sts::123456789012:assumed-role/Administrator/Jasper
SettingId : /ssm/parameter-store/high-throughput-enabled
SettingValue : true
Status : Customized

```

## Impostazione delle notifiche o delle azioni di attivazione basate su Parameter Store eventi

Puoi utilizzare Amazon EventBridge e Amazon Simple Notification Service (Amazon SNS) per notificarti le modifiche ai AWS Systems Manager parametri. Gli eventi vengono emessi secondo il principio del massimo sforzo. Ad esempio, puoi creare regole che effettuano le seguenti operazioni:

- Ti avvisa quando viene creata, aggiornata o eliminata una versione di un parametro o di un'etichetta di parametro.
- Notifica le modifiche o lo stato relativi alle politiche relative ai parametri, ad esempio quando un parametro scade, sta per scadere o non è cambiato per un determinato periodo di tempo.

### Note

Le policy dei parametri sono disponibili per i parametri che utilizzano il livello di parametri avanzati. Soggetto a costi. Per ulteriori informazioni, consultare [Assegnazione delle politiche dei parametri in Parameter Store](#) e [Scelta dei livelli di parametri in Parameter Store](#).

- Avvia altre azioni su un obiettivo per eventi con parametri specifici. Ad esempio, è possibile eseguire una AWS Lambda funzione per ricreare automaticamente un parametro quando scade o viene eliminato. Puoi impostare una notifica per richiamare una funzione Lambda quando un parametro che memorizza un ID AMI approvato viene aggiornato. La funzione Lambda può aggiornare un modello di avvio o avviare un flusso di lavoro di distribuzione che utilizza il nuovo ID AMI.

EventBridge supporta anche l'esecuzione di Run Command comandi ed esecuzioni di automazione e azioni in molti altri. Servizi AWSRun Commande Automation sono entrambi strumenti in AWS Systems Manager. Per ulteriori informazioni, consulta la [Amazon EventBridge User Guide](#).

### Prima di iniziare

Crea tutte le risorse delle quali hai bisogno per specificare l'operazione di destinazione per la regola che crei. Ad esempio, se la regola che crei è per l'invio di una notifica, prima crea un argomento Amazon SNS. Per ulteriori informazioni, consulta [Nozioni di base su Amazon SNS](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Configurazione delle EventBridge regole per i parametri e delle politiche relative ai parametri

Questo argomento illustra quanto segue:

- Come creare una EventBridge regola che richiami un obiettivo in base agli eventi che accadono a uno o più parametri nel tuo Account AWS
- Come creare EventBridge regole che richiamano obiettivi in base agli eventi che si verificano a una o più politiche di parametri nel tuo Account AWS Quando si crea un parametro avanzato, è necessario specificare quando un parametro scade, quando ricevere la notifica prima che un parametro scada e il tempo di attesa prima di inviare la notifica che un parametro non ha subito modifiche. Le notifiche per questi eventi vengono configurate utilizzando la procedura seguente. Per ulteriori informazioni, consultare [Assegnazione delle politiche dei parametri in Parameter Store](#) e [Sceglia dei livelli di parametri in Parameter Store](#).

Per configurare una EventBridge regola per un parametro o una policy parametrica di Systems Manager

1. Apri la EventBridge console Amazon all'indirizzo <https://console.aws.amazon.com/events/>.
2. Scegli EventBridge Regola con modello di evento e poi Crea regola.
3. Scegli Advanced builder se non è già selezionato.
4. Inserisci un nome e una descrizione per la regola. Quindi scegli Successivo.

Una regola non può avere lo stesso nome di un'altra regola nella stessa Regione e sullo stesso router di eventi.

5. Per Router di eventi, seleziona il router di eventi che desideri associare a questa regola. Se desideri che questa regola venga avviata in base agli eventi corrispondenti che provengono dai tuoi Account AWS, seleziona predefinito. Quando un Servizio AWS utente del tuo account emette un evento, viene sempre indirizzato al bus eventi predefinito del tuo account.
6. Per Rule type (Tipo di regola), lascia l'impostazione predefinita Rule with an event pattern (Regola con un modello di evento).
7. Scegli Next (Successivo).
8. Per Origine evento, lascia selezionati AWS gli eventi predefiniti o gli eventi dei EventBridge partner. È possibile saltare la sezione Sample event (Evento di esempio).
9. Per Event pattern (Modello di eventi), procedi come segue:
  - Scegli modello personalizzato (editor JSON).
  - Per Modello di eventi, incolla uno dei seguenti contenuti nella casella, a seconda che tu stia creando una regola per un parametro o una policy di parametro:

## Parameter

```
{
 "source": [
 "aws.ssm"
],
 "detail-type": [
 "Parameter Store Change"
],
 "detail": {
 "name": [
 "parameter-1-name",
 "/parameter-2-name/level-2",
 "/parameter-3-name/level-2/level-3"
],
 "operation": [
 "Create",
 "Update",
 "Delete",
 "LabelParameterVersion"
]
 }
}
```

## Parameter policy

```
{
 "source": [
 "aws.ssm"
],
 "detail-type": [
 "Parameter Store Policy Action"
],
 "detail": {
 "parameter-name": [
 "parameter-1-name",
 "/parameter-2-name/level-2",
 "/parameter-3-name/level-2/level-3"
],
 "policy-type": [
 "Expiration",
 "ExpirationNotification",
 "NoChangeNotification"
]
 }
}
```

```
]
 }
}
```

- Modifica i contenuti dei parametri e delle operazioni su cui desideri agire come mostrato negli esempi seguenti.

### Parameter

Con questo esempio, viene eseguita un'operazione quando uno dei parametri denominati `/Oncall` e `/Project/Teamlead` viene aggiornato:

```
{
 "source": [
 "aws.ssm"
],
 "detail-type": [
 "Parameter Store Change"
],
 "detail": {
 "name": [
 "/Oncall",
 "/Project/Teamlead"
],
 "operation": [
 "Update"
]
 }
}
```

### Parameter policy

Con questo esempio, viene eseguita un'operazione ogni volta che il parametro denominato `/OncallDuties` scade e viene eliminato:

```
{
 "source": [
 "aws.ssm"
],
 "detail-type": [
 "Parameter Store Policy Action"
],
 "detail": {
```

```
 "parameter-name": [
 "/OncallDuties"
],
 "policy-type": [
 "Expiration"
]
 }
}
```

10. Scegli Next (Successivo).
11. Per Destinazione 1, scegli un tipo di destinazione e una risorsa supportata. Ad esempio, se scegli il AWS servizio e poi l'argomento SNS, seleziona Argomento. Se lo desideri CodePipeline, inserisci un ARN della pipeline per Pipeline ARN. Fornisci i valori di configurazione aggiuntivi, se necessario.

 Tip

Scegli Aggiungi un'altra destinazione se hai bisogno di destinazioni aggiuntive per la regola.

12. Scegli Next (Successivo).
13. (Facoltativo) Inserire uno o più tag per la regola. Per ulteriori informazioni, consulta i EventBridge tag [Amazon](#) nella Amazon User Guide. EventBridge
14. Scegli Next (Successivo).
15. Scegli Crea regola.

#### Ulteriori informazioni

- [Uso di etichette di parametri per semplificare l'aggiornamento della configurazione tra ambienti diversi](#)
- [Tutorial: EventBridge da utilizzare per inoltrare eventi AWS Systems ManagerRun Command](#) nella Amazon EventBridge User Guide
- [Tutorial: imposta AWS Systems Manager l'automazione come EventBridge obiettivo](#) nella Amazon EventBridge User Guide

## Lavorare con Parameter Store

Parameter Store consente di creare, organizzare e gestire i dati di configurazione e i segreti utilizzati dalle applicazioni in fase di esecuzione.

In questa sezione, imparerete a lavorare con i parametri durante tutto il loro ciclo di vita, creandoli e organizzandoli, applicando policy, gestendo versioni ed etichette e controllando gli accessi. È possibile eseguire queste attività utilizzando, il Console di gestione AWS, o. AWS Command Line Interface AWS Tools for Windows PowerShell

Parameter Store centralizza i dati di configurazione come variabili di ambiente, URL degli endpoint di servizio, identificatori di risorse, ID AMI approvati e parametri di ottimizzazione delle applicazioni, in modo da poter aggiornare i valori senza modificare il codice dell'applicazione. I parametri vengono archiviati come coppie chiave-valore, possono essere organizzati gerarchicamente e supportano il controllo delle versioni e la crittografia opzionale con. AWS Key Management Service

### Argomenti

- [Creazione in corso Parameter Store parametri in Systems Manager](#)
- [Alla ricerca di Parameter Store parametri in Systems Manager](#)
- [Assegnazione delle politiche dei parametri in Parameter Store](#)
- [Utilizzo delle gerarchie di parametri in Parameter Store](#)
- [Impedire l'accesso a Parameter Store operazioni API](#)
- [Utilizzo delle etichette dei parametri in Parameter Store](#)
- [Utilizzo delle versioni dei parametri in Parameter Store](#)
- [Utilizzo di parametri condivisi in Parameter Store](#)
- [Utilizzo dei parametri in Parameter Store utilizzo di Run Command comandi](#)
- [Utilizzo del supporto nativo dei parametri in Parameter Store per Amazon Machine Image ID](#)
- [Eliminazione dei parametri da Parameter Store](#)

### Creazione in corso Parameter Store parametri in Systems Manager

Un parametro è qualsiasi dato memorizzato in Parameter Store, ad esempio un blocco di testo, un elenco di nomi, un AMI ID, una chiave di licenza e così via. È possibile fare riferimento a questi dati in modo centralizzato e sicuro negli script, nei comandi e nei documenti di SSM.

Parameter Store fornisce supporto per i seguenti tipi di parametri:

- String
- StringList
- SecureString

Per ulteriori informazioni sui tipi precedenti, vedere [Riferimento Parameter Store](#).

Nelle sezioni seguenti, imparerete a creare Parameter Store parametri utilizzando Console di gestione AWS, AWS Command Line Interface (AWS CLI) o AWS Tools for Windows PowerShell (Strumenti per Windows PowerShell).

### Argomenti

- [Creare un Parameter Store parametro utilizzando la console](#)
- [Creare un Parameter Store parametro utilizzando il AWS CLI](#)
- [Creare un Parameter Store parametro utilizzando Tools for Windows PowerShell](#)

### Creare un Parameter Store parametro utilizzando la console

È possibile utilizzare la AWS Systems Manager console per creare ed eseguire String e tipi di SecureString parametri. StringList Dopo aver eliminato un parametro, attendere almeno 30 secondi per creare un parametro con lo stesso nome.

#### Note

I parametri sono disponibili solo nel Regione AWS luogo in cui sono stati creati.

La procedura seguente ti guiderà attraverso il processo di creazione di un parametro, nella console Parameter Store. Puoi creare i tipi di parametri String, StringList e SecureString dalla console.

### Per creare un parametro

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Parameter Store.
3. Scegli Create parameter (Crea parametro).



4. Nella casella Name (Nome) immettere una gerarchia e un nome. Ad esempio, specifica **/Test/helloWorld**.

Per ulteriori informazioni sulle gerarchie di parametri, consulta [Utilizzo delle gerarchie di parametri in Parameter Store](#).

5. Nella casella Description (Descrizione), immettere una descrizione che identifichi il parametro come parametro di test.
6. In Parameter tier (Livello parametri) scegliere Standard o Advanced (Avanzato). Per ulteriori informazioni sui parametri avanzati, consultare [Scelta dei livelli di parametri in Parameter Store](#).
7. Per Tipo, scegli String, StringList, o SecureString.
  - Se si sceglie String, viene visualizzato il campo Tipo di dati. Se stai creando un parametro per contenere l'ID risorsa per un'Amazon Machine Image (AMI), seleziona `aws:ec2:image`. In caso contrario, mantieni selezionata l'impostazione predefinita `text`.
  - Se si sceglie SecureString, viene visualizzato il campo KMS Key ID. Se non fornisci un AWS Key Management Service AWS KMS key ID, un AWS KMS key Amazon Resource Name (ARN), un nome alias o un ARN alias, il sistema utilizza `alias/aws/ssm`, che è quello di Systems Manager. Chiave gestita da AWS. In alternativa, è possibile utilizzare una chiave gestita dal cliente. Per ulteriori informazioni sulle chiavi gestite dal cliente e sulle Chiavi gestite da AWS, consulta [Concetti di AWS Key Management Service](#) nella Guida per gli sviluppatori di AWS Key Management Service. Per ulteriori informazioni sulla AWS KMS crittografia Parameter Store e sulla crittografia, consulta How Uses. [AWS Systems Manager Parameter Store AWS KMS](#)

 Important

Parameter Store supporta solo [Chiavi KMS simmetriche](#). Non è possibile utilizzare una [chiave KMS asimmetrica](#) per crittografare i parametri. Per informazioni su come determinare se una chiave KMS è simmetrica o asimmetrica, consulta [Identificazione di chiavi KMS simmetriche e asimmetriche](#) nella Guida per gli sviluppatori di AWS Key Management Service

- Quando si crea un parametro SecureString nella console utilizzando il parametro `key-id` con un nome alias della CMK gestita dal cliente o con un ARN dell'alias, è necessario specificare il prefisso `alias/` prima dell'alias. Di seguito è riportato un ARN di esempio.

```
arn:aws:kms:us-east-2:123456789012:alias/abcd1234-ab12-cd34-ef56-abcdeEXAMPLE
```

Di seguito è riportato un nome alias di esempio.

```
alias/MyAliasName
```

8. Nella casella Value (Valore) immettere un valore. Ad esempio, digita **This is my first parameter** o **ami-0dbf5ea29aEXAMPLE**.

 Note

I parametri non possono essere referenziati o nidificati nei valori di altri parametri. Non è possibile includere `{{}}` o `{{ssm:parameter-name}}` in un valore di parametro. Se si sceglie questa opzione SecureString, il valore del parametro viene mascherato per impostazione predefinita («\*\*\*\*\*») quando lo si visualizza successivamente nella scheda Panoramica dei parametri, come illustrato nella seguente illustrazione. Scegliere Show (Mostra) per visualizzare il valore del parametro.



9. (Facoltativo) Nell'area Tags (Tag), applicare una o più coppie chiave tag-valore al parametro.

I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Ad esempio, puoi aggiungere tag a un parametro System Manager per identificare il tipo di risorsa a cui viene applicato, l'ambiente o il tipo di dati di configurazione a cui il parametro fa riferimento. In questo caso, è possibile specificare le coppie chiave-valore seguenti:

- Key=Resource, Value=S3bucket
- Key=OS, Value=Windows
- Key=ParameterType, Value=LicenseKey

10. Scegli **Create parameter** (Crea parametro).
11. Nell'elenco dei parametri scegliere il nome del parametro creato. Verifica i dettagli nella scheda **Panoramica**. Se è stato creato un parametro **SecureString**, scegli **Mostra** per visualizzare il valore non crittografato.

#### Note

Non è possibile convertire un parametro avanzato in un parametro standard. Se non hai più bisogno o desideri eliminare i costi di un parametro avanzato, cancellalo e ricrealo come nuovo parametro standard.

#### Note

Non è possibile modificare il tipo di un parametro esistente (ad esempio, da **String** a **SecureString**) utilizzando la console. Per modificare il tipo di parametro, è necessario utilizzare AWS CLI o **s** con l'opzione **--overwrite**. Per ulteriori informazioni, consulta [Creare un Parameter Store parametro utilizzando il AWS CLI](#).

### Creare un Parameter Store parametro utilizzando il AWS CLI

È possibile utilizzare AWS Command Line Interface (AWS CLI) per creare **String** e **StringList** tipi di **SecureString** parametri. Dopo aver eliminato un parametro, attendere almeno 30 secondi per creare un parametro con lo stesso nome.

I parametri non possono essere referenziati o nidificati nei valori di altri parametri. Non è possibile includere `{{}}` o `{{ssm:parameter-name}}` in un valore di parametro.

#### Note

I parametri sono disponibili solo nel Regione AWS luogo in cui sono stati creati.

### Argomenti

- [Creazione di un parametro String utilizzando AWS CLI](#)
- [Creazione di un StringList parametro utilizzando AWS CLI](#)

- [Creazione di un SecureString parametro utilizzando AWS CLI](#)
- [Creazione di un parametro multilinea utilizzando AWS CLI](#)

## Creazione di un **parametro** String utilizzando AWS CLI

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Per creare un parametro di tipo String, eseguire questo comando. Sostituisci ogni *example resource placeholder* con le tue informazioni.

### Linux & macOS

```
aws ssm put-parameter \
 --name "parameter-name" \
 --value "parameter-value" \
 --type String \
 --tags "Key=tag-key,Value=tag-value"
```

### Windows

```
aws ssm put-parameter ^
 --name "parameter-name" ^
 --value "parameter-value" ^
 --type String ^
 --tags "Key=tag-key,Value=tag-value"
```

oppure

Eseguire il comando seguente per creare un parametro che contiene un ID Amazon Machine Image (AMI) come valore del parametro.

### Linux & macOS

```
aws ssm put-parameter \
 --name "parameter-name" \
 --value "an-AMI-id" \
 --type String \
 --tags "Key=tag-key,Value=tag-value"
```

```
--data-type "aws:ec2:image" \
--tags "Key=tag-key,Value=tag-value"
```

## Windows

```
aws ssm put-parameter ^
 --name "parameter-name" ^
 --value "an-AMI-id" ^
 --type String ^
 --data-type "aws:ec2:image" ^
 --tags "Key=tag-key,Value=tag-value"
```

L'opzione `--name` supporta le gerarchie. Per informazioni sulle gerarchie, consultare [Utilizzo delle gerarchie di parametri in Parameter Store](#).

L'opzione `--data-type` deve essere specificata solo se si sta creando un parametro che contiene un ID AMI. Convalida che il valore del parametro inserito sia un ID AMI di Amazon Elastic Compute Cloud (Amazon EC2) correttamente formattato. Per tutti gli altri parametri, il tipo di dati di default è `text` ed è facoltativo per specificare un valore. Per ulteriori informazioni, consulta [Utilizzo del supporto nativo dei parametri in Parameter Store per Amazon Machine Image ID](#).

### Important

In caso di esito positivo, il comando restituisce il numero di versione del parametro. Eccezione: se è stato specificato `aws:ec2:image` come tipo di dati, un nuovo numero di versione nella risposta non significa che il valore del parametro sia stato ancora convalidato. Per ulteriori informazioni, consulta [Utilizzo del supporto nativo dei parametri in Parameter Store per Amazon Machine Image ID](#).

Il seguente esempio aggiunge due tag di tipo coppia chiave-valore a un parametro.

## Linux & macOS

```
aws ssm put-parameter \
 --name parameter-name \
 --value "parameter-value" \
 --type "String" \
 --tags "Key=tag-key,Value=tag-value"
```

```
--tags '[{"Key":"Region","Value":"East"}, {"Key":"Environment",
"Value":"Production"}]'
```

## Windows

```
aws ssm put-parameter ^
 --name parameter-name ^
 --value "parameter-value" ^
 --type "String" ^
 --tags [{"Key\\":\\"Region1\\",\\"Value\\":\\"East1\\"}, {"Key\\":\\"Environment1\\",
\\"Value\\":\\"Production1\\"}]
```

L'esempio seguente utilizza una gerarchia di parametri nel nome per creare un testo normale di parametro String. Restituisce il numero di versione del parametro. Per ulteriori informazioni sulle gerarchie di parametri, consulta [Utilizzo delle gerarchie di parametri in Parameter Store](#).

## Linux & macOS

### Parametro non in una gerarchia

```
aws ssm put-parameter \
 --name "golden-ami" \
 --type "String" \
 --value "ami-12345abcdeEXAMPLE"
```

### Parametro in una gerarchia

```
aws ssm put-parameter \
 --name "/amis/linux/golden-ami" \
 --type "String" \
 --value "ami-12345abcdeEXAMPLE"
```

## Windows

### Parametro non in una gerarchia

```
aws ssm put-parameter ^
 --name "golden-ami" ^
 --type "String" ^
```

```
--value "ami-12345abcdeEXAMPLE"
```

### Parametro in una gerarchia

```
aws ssm put-parameter ^
 --name "/amis/windows/golden-ami" ^
 --type "String" ^
 --value "ami-12345abcdeEXAMPLE"
```

3. Eseguire il comando seguente per visualizzare il valore più recente del parametro e verificare i dettagli del nuovo parametro.

```
aws ssm get-parameters --names "/Test/IAD/helloWorld"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
 "InvalidParameters": [],
 "Parameters": [
 {
 "Name": "/Test/IAD/helloWorld",
 "Type": "String",
 "Value": "My updated parameter value",
 "Version": 2,
 "LastModifiedDate": "2020-02-25T15:55:33.677000-08:00",
 "ARN": "arn:aws:ssm:us-east-2:123456789012:parameter/Test/IAD/
helloWorld"
 }
]
}
```

Eseguire questo comando per modificare il valore del parametro. Restituisce il numero di versione del parametro.

```
aws ssm put-parameter --name "/Test/IAD/helloWorld" --value "My updated 1st parameter"
 --type String --overwrite
```

Eseguire questo comando per visualizzare la cronologia del valore del parametro.

```
aws ssm get-parameter-history --name "/Test/IAD/helloWorld"
```

Eseguire questo comando per utilizzare questo parametro in un comando.

```
aws ssm send-command --document-name "AWS-RunShellScript" --parameters '{"commands":
["echo {{ssm:/Test/IAD/helloWorld}}"]}' --targets "Key=instanceids,Values=instance-ids"
```

Eseguire il comando seguente se si desidera recuperare solo il parametro Value (Valore).

```
aws ssm get-parameter --name testDataTypeParameter --query "Parameter.Value"
```

Eseguire il comando seguente se si desidera recuperare solo il parametro Value (Valore) tramite `get-parameters`.

```
aws ssm get-parameters --names "testDataTypeParameter" --query "Parameters[*].Value"
```

Eseguire questo comando per visualizzare i metadati del parametro.

```
aws ssm describe-parameters --filters "Key=Name,Values=/Test/IAD/helloWorld"
```

#### Note

Name (Nome) deve avere l'iniziale maiuscola.

Il sistema restituisce informazioni simili alle seguenti.

```
{
 "Parameters": [
 {
 "Name": "helloworld",
 "Type": "String",
 "LastModifiedUser": "arn:aws:iam::123456789012:user/JohnDoe",
 "LastModifiedDate": 1494529763.156,
 "Version": 1,
 "Tier": "Standard",
 "Policies": []
 }
]
}
```



```
]
}
```

## Creazione di un StringList parametro utilizzando AWS CLI

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Per creare un parametro, eseguire questo comando. Sostituisci ogni *example resource placeholder* con le tue informazioni.

### Linux & macOS

```
aws ssm put-parameter \
 --name "parameter-name" \
 --value "a-comma-separated-list-of-values" \
 --type StringList \
 --tags "Key=tag-key,Value=tag-value"
```

### Windows

```
aws ssm put-parameter ^
 --name "parameter-name" ^
 --value "a-comma-separated-list-of-values" ^
 --type StringList ^
 --tags "Key=tag-key,Value=tag-value"
```

#### Note

In caso di esito positivo, il comando restituisce il numero di versione del parametro.

Questo esempio aggiunge due tag di tipo coppia chiave-valore a un parametro. (A seconda del tipo di sistema operativo nel computer locale, utilizzare uno dei comandi seguenti. La versione da eseguire su una macchina Windows locale include i caratteri di escape ("\"), è necessario eseguire il comando dal proprio strumento a riga di comando.)

Ecco un esempio StringList che utilizza una gerarchia di parametri.

## Linux & macOS

```
aws ssm put-parameter \
 --name /IAD/ERP/Oracle/addUsers \
 --value "Milana,Mariana,Mark,Miguel" \
 --type StringList
```

## Windows

```
aws ssm put-parameter ^
 --name /IAD/ERP/Oracle/addUsers ^
 --value "Milana,Mariana,Mark,Miguel" ^
 --type StringList
```

### Note

Gli elementi in `StringList` devono essere separati da una virgola (,). Non è possibile utilizzare altri caratteri speciali o di punteggiatura per eseguire l'escape degli elementi inclusi nell'elenco. Se un valore di parametro richiede una virgola, utilizzare il tipo di dati `String`.

3. Eseguire il comando `get-parameters` per verificare i dettagli del parametro. Ad esempio:

```
aws ssm get-parameters --name "/IAD/ERP/Oracle/addUsers"
```

## Creazione di un `SecureString` parametro utilizzando AWS CLI

Utilizza la procedura seguente per creare un parametro `SecureString`. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Solo il valore di un parametro `SecureString` viene crittografato. I nomi dei parametri, le descrizioni e altre proprietà non sono crittografati.

### Important

Parameter Store supporta solo [Chiavi KMS simmetriche](#). Non è possibile utilizzare una [chiave KMS asimmetrica](#) per crittografare i parametri. Per informazioni su come determinare se una

chiave KMS è simmetrica o asimmetrica, consulta [Identificazione di chiavi KMS simmetriche e asimmetriche](#) nella Guida per gli sviluppatori di AWS Key Management Service

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Eseguire uno dei seguenti comandi per creare un parametro che utilizza il tipo di dati SecureString.

## Linux & macOS

Create un **SecureString** parametro utilizzando il valore predefinito Chiave gestita da AWS

```
aws ssm put-parameter \
 --name "parameter-name" \
 --value "parameter-value" \
 --type "SecureString"
```

Creazione di un parametro **SecureString** che utilizza una chiave gestita del cliente

```
aws ssm put-parameter \
 --name "parameter-name" \
 --value "a-parameter-value, for example merchant-739482" \
 --type "SecureString" \
 --tags "Key=tag-key,Value=tag-value"
```

Create un **SecureString** parametro che utilizza una AWS KMS chiave personalizzata

```
aws ssm put-parameter \
 --name "parameter-name" \
 --value "a-parameter-value, for example merchant-739482" \
 --type "SecureString" \
 --key-id "your-account-ID/the-custom-AWS KMS-key" \
 --tags "Key=tag-key,Value=tag-value"
```

## Windows

Create un **SecureString** parametro utilizzando il valore predefinito Chiave gestita da AWS

```
aws ssm put-parameter ^
 --name "parameter-name" ^
 --value "parameter-value" ^
 --type "SecureString"
```

Creazione di un parametro **SecureString** che utilizza una chiave gestita del cliente

```
aws ssm put-parameter ^
 --name "parameter-name" ^
 --value "a-parameter-value, for example merchant-739482" ^
 --type "SecureString" ^
 --tags "Key=tag-key,Value=tag-value"
```

Create un **SecureString** parametro che utilizza una AWS KMS chiave personalizzata

```
aws ssm put-parameter ^
 --name "parameter-name" ^
 --value "a-parameter-value, for example merchant-739482" ^
 --type "SecureString" ^
 --key-id " " ^
 --tags "Key=tag-key,Value=tag-valueaccount-ID/the-custom-AWS KMS-key"
```

Se crei un parametro SecureString utilizzando la chiave Chiave gestita da AWS nel tuo account e nella tua Regione, non devi fornire un valore per il parametro `--key-id`.

#### Note

Per utilizzare il parametro AWS KMS key assegnato alla tua Account AWS mano Regione AWS, rimuovi il `key-id` parametro dal comando. Per ulteriori informazioni su AWS KMS keys, consulta [Concetti di AWS Key Management Service](#) nella Guida per gli sviluppatori AWS Key Management Service .

Per utilizzare una chiave gestita dal cliente anziché quella Chiave gestita da AWS assegnata al tuo account, specifica la chiave utilizzando il `--key-id` parametro. Il parametro supporta i formati di KMS seguenti.

- Esempio chiave Amazon Resource Name (ARN):

```
arn:aws:kms:us-east-2:123456789012:key/key-id
```

- Esempio di ARN alias:

```
arn:aws:kms:us-east-2:123456789012:alias/alias-name
```

- Esempio di ID chiave:

```
12345678-1234-1234-1234-123456789012
```

- Esempio di nome alias:

```
alias/MyAliasName
```

Puoi creare una chiave gestita dal cliente utilizzando Console di gestione AWS o l' AWS KMS API. I seguenti AWS CLI comandi creano una chiave gestita dal cliente nella versione corrente Regione AWS della tua Account AWS.

```
aws kms create-key
```

Utilizza un comando nel formato seguente per creare un parametro SecureString utilizzando la chiave appena creata.

L'esempio seguente utilizza un parametro denominato `/myapp/prod/vendor/merchant-id` con un ID commerciante come valore crittografato e un AWS KMS key.

## Linux & macOS

```
aws ssm put-parameter \
 --name /myapp/prod/vendor/merchant-id \
 --value "merchant-739482" \
 --type SecureString \
 --key-id arn:aws:kms:us-
east-2:123456789012:key/1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d5e
```

## Windows

```
aws ssm put-parameter ^
 --name /myapp/prod/vendor/merchant-id ^
 --value "merchant-739482" ^
 --type SecureString ^
```

```
--key-id arn:aws:kms:us-east-2:123456789012:key/1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d5e
```

3. Utilizzare il comando seguente per verificare i dettagli del parametro.

Se non si specifica il parametro `with-decryption` o se è necessario specificare il parametro `no-with-decryption`, il comando restituisce un GUID criptato.

#### Linux & macOS

```
aws ssm get-parameters \
 --name "the-parameter-name-you-specified" \
 --with-decryption
```

#### Windows

```
aws ssm get-parameters ^
 --name "the-parameter-name-you-specified" ^
 --with-decryption
```

4. Eseguire questo comando per visualizzare i metadati del parametro.

#### Linux & macOS

```
aws ssm describe-parameters \
 --filters "Key=Name,Values=the-name-that-you-specified"
```

#### Windows

```
aws ssm describe-parameters ^
 --filters "Key=Name,Values=the-name-that-you-specified"
```

5. Eseguire il comando seguente per modificare il valore del parametro se non si utilizza una AWS KMS key gestita dal cliente.

#### Linux & macOS

```
aws ssm put-parameter \
 --name "the-name-that-you-specified" \
 --value "a-new-parameter-value" \
 --type "SecureString" \
 --with-decryption
```

```
--overwrite
```

## Windows

```
aws ssm put-parameter ^
 --name "the-name-that-you-specified" ^
 --value "a-new-parameter-value" ^
 --type "SecureString" ^
 --overwrite
```

oppure

Eseguire uno dei seguenti comandi per modificare il valore del parametro se si utilizza una AWS KMS key gestita dal cliente.

## Linux & macOS

```
aws ssm put-parameter \
 --name "the-name-that-you-specified" \
 --value "a-new-parameter-value" \
 --type "SecureString" \
 --key-id "the-KMSkey-ID" \
 --overwrite
```

```
aws ssm put-parameter \
 --name "the-name-that-you-specified" \
 --value "a-new-parameter-value" \
 --type "SecureString" \
 --key-id "account-alias/the-KMSkey-ID" \
 --overwrite
```

## Windows

```
aws ssm put-parameter ^
 --name "the-name-that-you-specified" ^
 --value "a-new-parameter-value" ^
 --type "SecureString" ^
 --key-id "the-KMSkey-ID" ^
 --overwrite
```

```
aws ssm put-parameter ^
 --name "the-name-that-you-specified" ^
 --value "a-new-parameter-value" ^
 --type "SecureString" ^
 --key-id "account-alias/the-KMSkey-ID" ^
 --overwrite
```

6. Eseguire questo comando per visualizzare il valore più recente del parametro.

#### Linux & macOS

```
aws ssm get-parameters \
 --name "the-name-that-you-specified" \
 --with-decryption
```

#### Windows

```
aws ssm get-parameters ^
 --name "the-name-that-you-specified" ^
 --with-decryption
```

7. Eseguire questo comando per visualizzare la cronologia del valore del parametro.

#### Linux & macOS

```
aws ssm get-parameter-history \
 --name "the-name-that-you-specified"
```

#### Windows

```
aws ssm get-parameter-history ^
 --name "the-name-that-you-specified"
```

#### Note

Puoi creare manualmente un parametro con un valore criptato. In questo caso, poiché il valore è già crittografato, non è necessario scegliere il tipo di SecureString parametro. Se lo scegliSecureString, il parametro è doppiamente crittografato.



Per impostazione predefinita, tutti i valori SecureString vengono visualizzati come testo crittografato. Per decrittografare un SecureString valore, un utente deve disporre dell'autorizzazione per chiamare l'operazione AWS KMS [https://docs.aws.amazon.com/kms/latest/APIReference/API\\_Decrypt.html](https://docs.aws.amazon.com/kms/latest/APIReference/API_Decrypt.html) Decrypt API. Per informazioni sulla configurazione di AWS KMS controllo di accesso, vedere [Autenticazione e controllo degli accessi per AWS KMS](#) nella Guida per gli sviluppatori AWS Key Management Service .

#### Important

Se modificate l'alias della chiave KMS per la chiave KMS utilizzata per crittografare un parametro, dovete aggiornare anche l'alias della chiave a cui il parametro fa riferimento. AWS KMS Questo vale solo per l'alias della chiave del Servizio di gestione delle chiavi; l'ID chiave a cui viene associato un alias rimane lo stesso, a meno che non si elimini l'intera chiave.

## Creazione di un parametro multilinea utilizzando AWS CLI

È possibile utilizzare il AWS CLI per creare un parametro con interruzioni di riga. Utilizzare le interruzioni di riga per suddividere il testo in valori di parametro più lunghi per una migliore leggibilità o, ad esempio, aggiornare il contenuto di parametri multiparagrafo per una pagina Web. È possibile includere il contenuto in un file JSON e utilizzare `--cli-input-json`, utilizzando caratteri di interruzione di riga come `\n`, come mostrato nell'esempio seguente.

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Per creare un parametro a linea multipla, eseguire il seguente comando.

### Linux & macOS

```
aws ssm put-parameter \
 --name "MultiLineParameter3" \
 -type String \
 -value "{ \"Value\": \"LineOne\nLineTwo\nLine3\nLine4\"}"
```

### Windows

```
aws ssm put-parameter ^
```

```
-name "MultiLineParameter3" ^
-type String ^
-value "{ \"Value\": \"LineOne\\nLineTwo\\nLine3\\nLine4\\\"}"
```

## Linux & macOS

```
aws ssm put-parameter \
 --name "MultiLineParameter" \
 --type String \
 --cli-input-json file://MultiLineParameter.json
```

## Windows

```
aws ssm put-parameter ^
 --name "MultiLineParameter" ^
 --type String ^
 --cli-input-json file://MultiLineParameter.json
```

Nell'esempio seguente viene mostrato il contenuto del file `MultiLineParameter.json`.

```
{
 "Value": "<para>Paragraph One</para>\\n<para>Paragraph Two</para>
\\n<para>Paragraph Three</para>"
}
```

Il valore del parametro salvato viene memorizzato come segue.

```
<para>Paragraph One</para>
<para>Paragraph Two</para>
<para>Paragraph Three</para>
```

## Creare un Parameter Store parametro utilizzando Tools for Windows PowerShell

È possibile utilizzare AWS Tools for Windows PowerShell per creare `String` e `StringList` tipi di `SecureString` parametri. Dopo aver eliminato un parametro, attendere almeno 30 secondi per creare un parametro con lo stesso nome.

I parametri non possono essere referenziati o nidificati nei valori di altri parametri. Non è possibile includere `{{}}` o `{{ssm:parameter-name}}` in un valore di parametro.

#### Note

I parametri sono disponibili solo nel Regione AWS luogo in cui sono stati creati.

## Argomenti

- [Creazione di un parametro String \(Strumenti per Windows PowerShell\)](#)
- [Creazione di un StringList parametro \(Strumenti per Windows PowerShell\)](#)
- [Creazione di un SecureString parametro \(Strumenti per Windows PowerShell\)](#)

## Creazione di un parametro String (Strumenti per Windows PowerShell)

1. Installa e configura AWS Strumenti per PowerShell (Strumenti per Windows PowerShell), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione di AWS Strumenti per PowerShell](#).

2. Eseguire il comando seguente per creare un parametro che contiene un valore di testo normale. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
Write-SSMParameter `
 -Name "parameter-name" `
 -Value "parameter-value" `
 -Type "String"
```

oppure

Eseguire il comando seguente per creare un parametro che contiene un ID Amazon Machine Image (AMI) come valore del parametro.

#### Note

Per creare un parametro con un tag, create il `service.model.tag` prima mano come variabile. Ecco un esempio.

```
$tag = New-Object Amazon.SimpleSystemsManagement.Model.Tag
```

```
$tag.Key = "tag-key"
$tag.Value = "tag-value"
```

```
Write-SSMParameter `
 -Name "parameter-name" `
 -Value "an-AMI-id" `
 -Type "String" `
 -DataType "aws:ec2:image" `
 -Tags $tag
```

L'opzione `-DataType` deve essere specificata solo se si sta creando un parametro che contiene un ID AMI. Per tutti gli altri parametri, il tipo di dati predefinito è `text`. Per ulteriori informazioni, consulta [Utilizzo del supporto nativo dei parametri in Parameter Store per Amazon Machine Image ID](#).

Ecco un esempio che utilizza una gerarchia di parametri.

```
Write-SSMParameter `
 -Name "/IAD/Web/SQL/IPaddress" `
 -Value "99.99.99.999" `
 -Type "String" `
 -Tags $tag
```

3. Utilizzare il comando seguente per verificare i dettagli del parametro.

```
(Get-SSMParameterValue -Name "the-parameter-name-you-specified").Parameters
```

## Creazione di un StringList parametro (Strumenti per Windows PowerShell)

1. Installa e configura AWS Strumenti per PowerShell (Strumenti per Windows PowerShell), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione di AWS Strumenti per PowerShell](#).

2. Esegui il comando seguente per creare un StringList parametro. Sostituisci ogni *example resource placeholder* con le tue informazioni.

 Note

Per creare un parametro con un tag, create il `service.model.tag` prima mano come variabile. Ecco un esempio.

```
$tag = New-Object Amazon.SimpleSystemsManagement.Model.Tag
$tag.Key = "tag-key"
$tag.Value = "tag-value"
```

```
Write-SSMParameter `
 -Name "parameter-name" `
 -Value "a-comma-separated-list-of-values" `
 -Type "StringList" `
 -Tags $tag
```

In caso di esito positivo, il comando restituisce il numero di versione del parametro.

Ecco un esempio.

```
Write-SSMParameter `
 -Name "stringlist-parameter" `
 -Value "Milana,Mariana,Mark,Miguel" `
 -Type "StringList" `
 -Tags $tag
```

 Note

Gli elementi in `StringList` devono essere separati da una virgola (,). Non è possibile utilizzare altri caratteri speciali o di punteggiatura per eseguire l'escape degli elementi inclusi nell'elenco. Se un valore di parametro richiede una virgola, utilizzare il tipo di dati `String`.

3. Utilizzare il comando seguente per verificare i dettagli del parametro.

```
(Get-SSMParameterValue -Name "the-parameter-name-you-specified").Parameters
```

## Creazione di un SecureString parametro (Strumenti per Windows PowerShell)

Prima di creare un parametro SecureString, consulta i requisiti relativi a questo tipo di parametro. Per ulteriori informazioni, consulta [Creazione di un SecureString parametro utilizzando AWS CLI](#).

Solo il valore di un parametro SecureString viene crittografato. I nomi dei parametri, le descrizioni e altre proprietà non sono crittografati.

### Important

Parameter Store supporta solo [Chiavi KMS simmetriche](#). Non è possibile utilizzare una [chiave KMS asimmetrica](#) per crittografare i parametri. Per informazioni su come determinare se una chiave KMS è simmetrica o asimmetrica, consulta [Identificazione di chiavi KMS simmetriche e asimmetriche](#) nella Guida per gli sviluppatori di AWS Key Management Service

1. Installa e configura AWS Strumenti per PowerShell (Strumenti per Windows PowerShell), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione di AWS Strumenti per PowerShell](#).

2. Per creare un parametro, eseguire questo comando. Sostituisci ogni *example resource placeholder* con le tue informazioni.

### Note

Per creare un parametro con un tag, crea prima il service.model.tag come variabile. Ecco un esempio.

```
$tag = New-Object Amazon.SimpleSystemsManagement.Model.Tag
$tag.Key = "tag-key"
$tag.Value = "tag-value"
```

```
Write-SSMParameter `
 -Name "parameter-name" `
 -Value "parameter-value" `
 -Type "SecureString" `
 -KeyId "an AWS KMS key ID, an AWS KMS key ARN, an alias name, or an alias ARN"
```

```
-Tags $tag
```

In caso di esito positivo, il comando restituisce il numero di versione del parametro.

#### Note

Per utilizzare quella Chiave gestita da AWS assegnata al tuo account, rimuovi il `-KeyId` parametro dal comando.

L'esempio seguente crea un `SecureString` parametro denominato `/myapp/dev/vendor/merchant-id` con un ID commerciante come valore crittografato e un Chiave gestita da AWS.

```
Write-SSMParameter `
 -Name "/myapp/dev/vendor/merchant-id" `
 -Value "merchant-739482" `
 -Type "SecureString" `
 -Tags $tag
```

3. Utilizzare il comando seguente per verificare i dettagli del parametro.

```
(Get-SSMParameterValue -Name "the-parameter-name-you-specified" -WithDecryption
 $true).Parameters
```

Per impostazione predefinita, tutti i valori `SecureString` vengono visualizzati come testo crittografato. Per decrittografare un `SecureString` valore, un utente deve disporre dell'autorizzazione per chiamare l'operazione AWS KMS [https://docs.aws.amazon.com/kms/latest/APIReference/API\\_Decrypt.html](https://docs.aws.amazon.com/kms/latest/APIReference/API_Decrypt.html) Decrypt API. Per informazioni sulla configurazione di AWS KMS controllo di accesso, vedere [Autenticazione e controllo degli accessi per AWS KMS](#) nella Guida per gli sviluppatori AWS Key Management Service .

#### Important

Se si modifica l'alias della chiave del Servizio di gestione delle chiavi utilizzata per crittografare un parametro, è necessario aggiornare anche l'alias chiave utilizzato dal parametro per fare riferimento AWS KMS. Questo vale solo per l'alias della chiave del

Servizio di gestione delle chiavi; l'ID chiave a cui viene associato un alias rimane lo stesso, a meno che non si elimini l'intera chiave.

## Alla ricerca di Parameter Store parametri in Systems Manager

Quando si dispone di un numero elevato di parametri nel proprio account, può essere difficile trovare informazioni su uno o alcuni parametri alla volta. In questo caso, è possibile utilizzare gli strumenti di filtro per cercare quelli su cui sono necessarie informazioni, in base ai criteri di ricerca specificati. Puoi usare la AWS Systems Manager console, la AWS Command Line Interface (AWS CLI) AWS Strumenti per PowerShell, la o l'[DescribeParameters](#) API per cercare i parametri.

### Argomenti

- [Ricerca di un parametro utilizzando la console](#)
- [Ricerca di un parametro utilizzando AWS CLI](#)

### Ricerca di un parametro utilizzando la console

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Parameter Store.
3. Fare clic nella casella di ricerca e scegliere come si desidera eseguire la ricerca. Ad esempio Type o Name.
4. Fornire informazioni per il tipo di ricerca selezionato. Ad esempio:
  - Se la ricerca viene effettuata per Type, scegliere tra String, StringList o SecureString.
  - Se la ricerca viene effettuata per Name, scegliere contains, equals o begins-with, quindi immettere tutto o parte del nome di un parametro.



#### Note

Nella console, il tipo di ricerca predefinito per Name è contains.

5. Premere Invio.

L'elenco dei parametri viene aggiornato con i risultati della ricerca.



 Note

La ricerca potrebbe contenere più risultati di quelli visualizzati nella prima pagina dei risultati. Utilizzate la freccia destra (>) sull'argomento dell'elenco dei parametri (se disponibile) per visualizzare il prossimo set di risultati.

## Ricerca di un parametro utilizzando AWS CLI

Utilizzare il comando `describe-parameters` per visualizzare informazioni su uno o più parametri nell' AWS CLI.

Gli esempi seguenti illustrano varie opzioni che è possibile utilizzare per visualizzare informazioni sui parametri del proprio Account AWS. Per ulteriori informazioni su queste opzioni, consulta [describe-parameters](#) nella Guida per l'utente di AWS Command Line Interface .

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Sostituire i valori di esempio nei comandi seguenti con valori che riflettono i parametri creati nell'account.

### Linux & macOS

```
aws ssm describe-parameters \
 --parameter-filters "Key=Name,Values=MyParameterName"
```

### Windows

```
aws ssm describe-parameters ^
 --parameter-filters "Key=Name,Values=MyParameterName"
```

 Note

Per `describe-parameters`, il tipo di ricerca predefinito per `Name` è `Equals`. Nei filtri dei parametri, specificare `"Key=Name,Values=MyParameterName"` è come specificare `"Key=Name,Option=Equals,Values=MyParameterName"`.

```
aws ssm describe-parameters \
 --parameter-filters "Key=Name,Option=Contains,Values=Product"
```

```
aws ssm describe-parameters \
 --parameter-filters "Key=Type,Values=String"
```

```
aws ssm describe-parameters \
 --parameter-filters "Key=Path,Values=/Production/West"
```

```
aws ssm describe-parameters \
 --parameter-filters "Key=Tier,Values=Standard"
```

```
aws ssm describe-parameters \
 --parameter-filters "Key=tag:tag-key,Values=tag-value"
```

```
aws ssm describe-parameters \
 --parameter-filters "Key=KeyId,Values=key-id"
```

 Note

Nell'ultimo esempio, *key-id* rappresenta l'ID di una chiave AWS Key Management Service (AWS KMS) utilizzata per crittografare un `SecureString` parametro creato nel tuo account. In alternativa, puoi inserire `alias/aws/ssm` per utilizzare la AWS KMS chiave predefinita per il tuo account. Per ulteriori informazioni, consulta [Creazione di un `SecureString` parametro utilizzando AWS CLI](#).

Se il comando viene eseguito correttamente, verrà visualizzato un output simile al seguente:

```
{
 "Parameters": [
 {
 "Name": "/Production/West/Manager",
 "Type": "String",
 "LastModifiedDate": 1573438580.703,
 "LastModifiedUser": "arn:aws:iam::111122223333:user/Mateo.Jackson",
 "Version": 1,
 "Tier": "Standard",
 "Policies": []
 },
 {
 "Name": "/Production/West/TeamLead",
 "Type": "String",
 "LastModifiedDate": 1572363610.175,
 "LastModifiedUser": "arn:aws:iam::111122223333:user/Mateo.Jackson",
 "Version": 1,
 "Tier": "Standard",
 "Policies": []
 },
 {
 "Name": "/Production/West/HR",
 "Type": "String",
 "LastModifiedDate": 1572363680.503,
 "LastModifiedUser": "arn:aws:iam::111122223333:user/Mateo.Jackson",
 "Version": 1,
 "Tier": "Standard",
 "Policies": []
 }
]
}
```

## Assegnazione delle politiche dei parametri in Parameter Store

Le policy dei parametri aiutano a gestire un set di parametri crescente, consentendo di assegnare criteri specifici a un parametro, ad esempio una data di scadenza o il time-to-live. Le policy relative ai parametri sono particolarmente utili per forzare l'aggiornamento o l'eliminazione dei dati di configurazione archiviati in Parameter Store, uno strumento in AWS Systems Manager.

Parameter Store offre i seguenti tipi di policy: `Expiration`, `ExpirationNotification`, e `NoChangeNotification`.

Se gestisci credenziali che richiedono la rotazione automatica, l'accesso tra più account o una registrazione di controllo dettagliata, ti consigliamo di utilizzarle. [AWS Secrets Manager](#) Secrets Manager è stato creato appositamente per la gestione di informazioni segrete quali credenziali di database, chiavi API e informazioni segrete supportate da software di terze parti. Per ulteriori informazioni, vedi Che cos'è? [AWS Secrets Manager](#) nella Guida AWS Secrets Manager per l'utente.

Parameter Store applica le policy dei parametri utilizzando scansioni asincrone periodiche. Dopo aver creato una policy, non è necessario eseguire altre operazioni per applicarla. Parameter Store esegue indipendentemente l'operazione definita dalla policy in base ai criteri specificati.

 Note

Le policy dei parametri sono disponibili per i parametri che utilizzano il livello di parametri avanzati. Per ulteriori informazioni, consulta [Scelta dei livelli di parametri in Parameter Store](#).

Una policy dei parametri è un array JSON, come illustrato nella seguente tabella. È possibile assegnare una policy quando si crea un nuovo parametro avanzato oppure applicarla aggiornando un parametro. Parameter Store supporta i seguenti tipi di policy dei parametri.

| Policy   | Informazioni                                                                                                                                                                                                                                                                                                                                                               | Esempi                                                                                                                             |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Scadenza | Questa policy elimina il parametro. È possibile specificare una determinata data e ora utilizzando il formato <code>ISO_INSTANT</code> o <code>ISO_OFFSET_DATE_TIME</code> . Per modificare l'ora in cui eliminare il parametro, devi aggiornare la policy. L'aggiornamento di un parametro non influisce sulla data o l'ora di scadenza della policy associata. Quando si | <pre>{   "Type": "Expiration",   "Version": "1.0",   "Attributes": {     "Timestamp":       "2018-12-02T21:34:33.000Z"   } }</pre> |

| Policy                 | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                         | Esempi                                                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | <p>raggiunge la data e l'ora di scadenza, Parameter Store elimina il parametro.</p> <div data-bbox="591 382 1032 1083"> <p> <b>Note</b></p> <p>In questo esempio viene utilizzato il formato ISO_INSTANT. È possibile anche specificare una data e un'ora utilizzando il formato ISO_OFFSET_DATE_TIME. Ecco un esempio: 2019-11-01T22:13:48.87+10:30:00.</p> </div> |                                                                                                                                                                     |
| ExpirationNotification | <p>Questa politica avvia un evento in Amazon EventBridge (EventBridge) che ti avvisa della scadenza. Utilizzando questa policy, è possibile ricevere le notifiche ore o giorni prima della scadenza.</p>                                                                                                                                                                                                                                             | <pre data-bbox="1084 1142 1507 1507">{   "Type": "ExpirationNotification",   "Version": "1.0",   "Attributes": {     "Before": "15",     "Unit": "Days"   } }</pre> |

| Policy               | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Esempi                                                                                                                           |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| NoChangeNotification | <p>Questa policy avvia un evento EventBridge se un parametro non è stato modificato per un determinato periodo di tempo. Questo tipo di policy è utile quando, ad esempio, un ID AMI approvato deve essere rivisto o aggiornato entro un determinato periodo di tempo.</p> <p>La policy stabilisce quando inviare una notifica leggendo l'attributo LastModifiedTime del parametro. Se si modifica un parametro, il sistema reimposta il periodo di tempo per la notifica in base al nuovo valore di LastModifiedTime .</p> | <pre>{   "Type": "NoChangeNotification",   "Version": "1.0",   "Attributes": {     "After": "20",     "Unit": "Days"   } }</pre> |

È possibile assegnare più regole a un parametro. Ad esempio, è possibile assegnare ExpirationNotification policy Expiration e in modo che il sistema avvii un EventBridge evento per notificare l'imminente eliminazione di un parametro. È possibile assegnare un massimo di 10 (dieci) policy a un parametro.

L'esempio seguente mostra la sintassi della richiesta per una richiesta [PutParameter](#) API che assegna quattro politiche a un nuovo parametro denominato. SecureString /myapp/prod/vendor/merchant-id

```
{
 "Name": "/myapp/prod/vendor/merchant-id",
 "Description": "Parameter with policies",
 "Value": "merchant-739482",
 "Type": "SecureString",
 "Overwrite": "True",
 "Policies": [
```

```

 {
 "Type": "Expiration",
 "Version": "1.0",
 "Attributes": {
 "Timestamp": "2018-12-02T21:34:33.000Z"
 }
 },
 {
 "Type": "ExpirationNotification",
 "Version": "1.0",
 "Attributes": {
 "Before": "30",
 "Unit": "Days"
 }
 },
 {
 "Type": "ExpirationNotification",
 "Version": "1.0",
 "Attributes": {
 "Before": "15",
 "Unit": "Days"
 }
 },
 {
 "Type": "NoChangeNotification",
 "Version": "1.0",
 "Attributes": {
 "After": "20",
 "Unit": "Days"
 }
 }
]
}

```

## Aggiunta di policy a un parametro esistente

Questa sezione include informazioni su come aggiungere policy a un parametro esistente utilizzando la AWS Systems Manager console, AWS Command Line Interface (AWS CLI) e. AWS Tools for Windows PowerShell Per informazioni su come creare un nuovo parametro che includa le policy, consulta [Creazione in corso Parameter Store parametri in Systems Manager](#).

## Argomenti

- [Aggiungere policy a un parametro esistente utilizzando la console](#)

- [Aggiungere politiche a un parametro esistente utilizzando il AWS CLI](#)
- [Aggiungere criteri a un parametro esistente \(Strumenti per Windows PowerShell\)](#)

Aggiungere policy a un parametro esistente utilizzando la console

Utilizza la procedura seguente per aggiungere policy a un parametro esistente utilizzando la console Systems Manager.

Per aggiungere policy a un parametro esistente

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Parameter Store.
3. Scegli l'opzione accanto al parametro da aggiornare per includere le policy, quindi seleziona Modifica.
4. Scegli Avanzato.
5. (Facoltativo) Nella sezione Policy dei parametri, scegli Abilitato. È possibile specificare una data di scadenza e una o più policy di notifica per il parametro.
6. Scegli Salva modifiche.

#### Important

- Parameter Store conserva le policy in un parametro finché non vengono sovrascritte da nuove policy o non vengono rimosse.
- Per rimuovere tutte le policy da un parametro esistente, modificare il parametro e applicare una policy vuota utilizzando parentesi quadre e parentesi graffe, come illustrato di seguito: `[{}]`
- Se si aggiunge una nuova policy a un parametro che ha già delle policy, Systems Manager sovrascrive le policy associate al parametro. Le policy esistenti vengono eliminate. Per aggiungere una nuova policy a un parametro che già ne contiene alcune, copiare e incollare la policy originale, digitare quella nuova, quindi salvare le modifiche.



## Aggiungere politiche a un parametro esistente utilizzando il AWS CLI

Utilizza la procedura seguente per aggiungere policy a un parametro esistente utilizzando AWS CLI.

Per aggiungere policy a un parametro esistente

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Esegui questo comando per aggiungere le policy a un parametro esistente. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Linux & macOS

```
aws ssm put-parameter
 --name "parameter name" \
 --value 'parameter value' \
 --type parameter type \
 --overwrite \
 --policies "[{policies-enclosed-in-brackets-and-curly-braces}]"
```

Windows

```
aws ssm put-parameter
 --name "parameter name" ^
 --value 'parameter value' ^
 --type parameter type ^
 --overwrite ^
 --policies "[{policies-enclosed-in-brackets-and-curly-braces}]"
```

L'esempio seguente include una politica di scadenza che elimina il parametro dopo 15 giorni. L'esempio include anche una politica di notifica che genera un EventBridge evento cinque (5) giorni prima dell'eliminazione del parametro. Infine, include una policy NoChangeNotification se il parametro non viene modificato dopo 60 giorni. L'esempio utilizza un parametro denominato `/myapp/prod/vendor/merchant-id` con un ID commerciante come valore crittografato e un AWS Key Management Service AWS KMS key. Per

ulteriori informazioni AWS KMS keys, consulta [AWS Key Management Service Concepts](#) nella AWS Key Management Service Developer Guide.

## Linux & macOS

```
aws ssm put-parameter \
 --name "/myapp/prod/vendor/merchant-id" \
 --value "merchant-739482" \
 --type "SecureString" \
 --overwrite \
 --policies "[{\"Type\":\"Expiration\",\"Version\":\"1.0\",\"Attributes\":{\"Timestamp\":\"2020-05-13T00:00:00.000Z\"}}, {\"Type\":\"ExpirationNotification\",\"Version\":\"1.0\",\"Attributes\":{\"Before\":\"5\",\"Unit\":\"Days\"}}, {\"Type\":\"NoChangeNotification\",\"Version\":\"1.0\",\"Attributes\":{\"After\":\"60\",\"Unit\":\"Days\"}}]"
```

## Windows

```
aws ssm put-parameter ^
 --name "/myapp/prod/vendor/merchant-id" ^
 --value "merchant-739482" ^
 --type "SecureString" ^
 --overwrite ^
 --policies "[{\"Type\":\"Expiration\",\"Version\":\"1.0\",\"Attributes\":{\"Timestamp\":\"2020-05-13T00:00:00.000Z\"}}, {\"Type\":\"ExpirationNotification\",\"Version\":\"1.0\",\"Attributes\":{\"Before\":\"5\",\"Unit\":\"Days\"}}, {\"Type\":\"NoChangeNotification\",\"Version\":\"1.0\",\"Attributes\":{\"After\":\"60\",\"Unit\":\"Days\"}}]"
```

3. Utilizzare il comando seguente per verificare i dettagli del parametro. Sostituisci *parameter name* con informazioni personali.

## Linux & macOS

```
aws ssm describe-parameters \
 --parameter-filters "Key=Name,Values=parameter name"
```

## Windows

```
aws ssm describe-parameters ^
 --parameter-filters "Key=Name,Values=parameter name"
```

 Important

- Parameter Store conserva le policy per un parametro finché non vengono sovrascritte da nuove policy o non vengono rimosse.
- Per rimuovere tutte le policy da un parametro esistente, modificare il parametro e applicare una policy vuota utilizzando parentesi quadre e parentesi graffe. Sostituisci ogni *example resource placeholder* con le tue informazioni. Ad esempio:

Linux & macOS

```
aws ssm put-parameter \
 --name parameter name \
 --type parameter type \
 --value 'parameter value' \
 --policies "[{}]"
```

Windows

```
aws ssm put-parameter ^
 --name parameter name ^
 --type parameter type ^
 --value 'parameter value' ^
 --policies "[{}]"
```

- Se si aggiunge una nuova policy a un parametro che ha già delle policy, Systems Manager sovrascrive le policy associate al parametro. Le policy esistenti vengono eliminate. Per aggiungere una nuova policy a un parametro che già ne contiene alcune, copiare e incollare la policy originale, digitare quella nuova, quindi salvare le modifiche.

## Aggiungere criteri a un parametro esistente (Strumenti per Windows PowerShell)

Utilizzare la procedura seguente per aggiungere criteri a un parametro esistente utilizzando Strumenti per Windows PowerShell. Sostituisci ogni *example resource placeholder* con le tue informazioni.

Per aggiungere policy a un parametro esistente

1. Apri Strumenti per Windows PowerShell ed esegui il comando seguente per specificare le tue credenziali. È necessario disporre delle autorizzazioni di amministratore in Amazon Elastic

Compute Cloud (Amazon EC2) oppure disporre dell'autorizzazione appropriata in AWS Identity and Access Management (IAM).

```
Set-AWSCredentials `
 -AccessKey access-key-name `
 -SecretKey secret-key-name
```

2. Esegui il comando seguente per impostare la regione per la tua sessione. PowerShell L'esempio utilizza la Regione Stati Uniti orientali (Ohio) (us-east-2).

```
Set-DefaultAWSRegion `
 -Region us-east-2
```

3. Esegui questo comando per aggiungere le policy a un parametro esistente. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
Write-SSMParameter `
 -Name "parameter name" `
 -Value "parameter value" `
 -Type "parameter type" `
 -Policies "[{policies-enclosed-in-brackets-and-curly-braces}]" `
 -Overwrite
```

L'esempio seguente include una politica di scadenza che elimina il parametro alla mezzanotte (GMT) del 13 maggio 2020. L'esempio include anche una politica di notifica che genera un EventBridge evento cinque (5) giorni prima dell'eliminazione del parametro. Infine, include una policy NoChangeNotification se il parametro non viene modificato dopo 60 giorni. L'esempio utilizza un parametro denominato `/myapp/prod/vendor/merchant-id` con un ID commerciante come valore crittografato e un Chiave gestita da AWS.

```
Write-SSMParameter `
 -Name "/myapp/prod/vendor/merchant-id" `
 -Value "merchant-739482" `
 -Type "SecureString" `
 -Policies "[{"Type": "Expiration", "Version": "1.0", "Attributes": {"Timestamp": "2018-05-13T00:00:00.000Z"}}, {"Type": "ExpirationNotification", "Version": "1.0", "Attributes": {"Before": "5", "Unit": "Days"}}, {"Type": "NoChangeNotification", "Version": "1.0", "Attributes": {"After": "60", "Unit": "Days"}}]" `
 -Overwrite
```

4. Utilizzare il comando seguente per verificare i dettagli del parametro. Sostituiscilo *parameter name* con le tue informazioni.

```
(Get-SSMParameterValue -Name "parameter name").Parameters
```

#### Important

- Parameter Store conserva le policy in un parametro finché non vengono sovrascritte da nuove policy o non vengono rimosse.
- Per rimuovere tutte le policy da un parametro esistente, modificare il parametro e applicare una policy vuota utilizzando parentesi quadre e parentesi graffe. Ad esempio:

```
Write-SSMParameter `
 -Name "parameter name" `
 -Value "parameter value" `
 -Type "parameter type" `
 -Policies "[{}]"
```

- Se si aggiunge una nuova policy a un parametro che ha già delle policy, Systems Manager sovrascrive le policy associate al parametro. Le policy esistenti vengono eliminate. Per aggiungere una nuova policy a un parametro che già ne contiene alcune, copiare e incollare la policy originale, digitare quella nuova, quindi salvare le modifiche.

## Utilizzo delle gerarchie di parametri in Parameter Store

La gestione di un numero elevatissimo di parametri come un elenco semplice è un'attività dispendiosa in termini di tempo ed è soggetta a errori. Può anche risultare difficile identificare il parametro corretto per un'attività specifica. Ciò significa che è possibile usare inavvertitamente il parametro errato oppure creare più parametri che utilizzano gli stessi dati di configurazione.

È possibile pertanto utilizzare le gerarchie di parametri per semplificare l'organizzazione e la gestione dei parametri di . Una gerarchia è un nome di parametro che include un percorso definito mediante l'utilizzo di barre (/).

### Argomenti

- [Comprensione della gerarchia dei parametri tramite esempi](#)

- [Esecuzioni di query sui parametri in una gerarchia](#)
- [Gestione dei parametri mediante gerarchie utilizzando AWS CLI](#)

Comprensione della gerarchia dei parametri tramite esempi

L'esempio seguente utilizza tre livelli di gerarchia nel nome per identificare gli elementi seguenti:

/Environment/Type of computer/Application/Data

/Dev/WebServer/Linux/approved-ami

È possibile creare una gerarchia con un massimo di 15 livelli. Ti consigliamo di creare gerarchie in base a una struttura gerarchica esistente nell'ambiente in uso, come illustrato negli esempi seguenti:

- Il tuo [ambiente di integrazione continua e distribuzione](#) continua (CI/CD flussi di lavoro)

/Dev/WebServer/Linux/approved-ami

/Staging/WebServer/Linux/approved-ami

/Prod/WebServer/Linux/approved-ami

- Applicazioni che utilizzano container

/MyApp/.NET/Images/*approved-ami*

- Organizzazione aziendale

/Finance/Accountants/UserList

/Finance/Analysts/UserList

/HR/Employees/EU/UserList

Le gerarchie di parametri standardizzano la modalità di creazione dei parametri e semplificano la gestione dei parametri nel corso del tempo. Una gerarchia di parametri può anche semplificare l'identificazione del parametro più idoneo per un'attività di configurazione. Ciò ti consente di evitare la creazione di più parametri con gli stessi dati di configurazione.

Puoi creare una gerarchia che ti consenta di condividere i parametri tra diversi ambienti, come mostrato nei seguenti esempi che utilizzano ID AMI approvati negli ambienti di sviluppo e staging.

/DevTest/MyApp/images/*approved-ami*

È quindi possibile creare un ID AML approvato univoco per il proprio ambiente di produzione, come mostrato nell'esempio seguente:

/prod/MyApp/images/*approved-ami*

Non è necessario specificare una gerarchia di parametri. È possibile creare i parametri al primo livello. Questo tipo di parametri è definito parametri root. Per garantire la compatibilità con le versioni precedenti, tutti i parametri creati in Parameter Store prima del rilascio della funzionalità delle gerarchie sono parametri root. I sistemi gestiscono entrambi i seguenti parametri come parametri root.

/parameter-name

parameter-name

Esecuzioni di query sui parametri in una gerarchia

Un altro vantaggio dell'utilizzo delle gerarchie è la possibilità di interrogare tutti i parametri compresi in un determinato livello di una gerarchia utilizzando l'[GetParametersByPath](#) operazione API. Ad esempio, se si esegue il seguente comando da AWS Command Line Interface (AWS CLI), il sistema restituisce tutti i parametri al di sotto del livello: `Oncall`

```
aws ssm get-parameters-by-path --path /Dev/Web/Oncall
```

Output di esempio:

```
{
 "Parameters": [
 {
 "Name": "/Dev/Web/Oncall/Week1",
 "Type": "String",
 "Value": "John Doe",
 "Version": 1,
 "LastModifiedDate": "2024-11-22T07:18:53.510000-08:00",
 "ARN": "arn:aws:ssm:us-east-2:123456789012:parameter/Dev/Web/Oncall/Week1",
 "DataType": "text"
 },
 {
```

```
 "Name": "/Dev/Web/Oncall/Week2",
 "Type": "String",
 "Value": "Mary Major",
 "Version": 1,
 "LastModifiedDate": "2024-11-22T07:21:25.325000-08:00",
 "ARN": "arn:aws:ssm:us-east-2:123456789012:parameter/Dev/Web/Oncall/Week2",
 "DataType": "text"
 }
]
```

Per visualizzare i parametri `SecureString` decrittati in una gerarchia, devi specificare il percorso e il parametro `--with-decryption`, come illustrato nel seguente esempio.

```
aws ssm get-parameters-by-path --path /Prod/ERP/SAP --with-decryption
```

## Gestione dei parametri mediante gerarchie utilizzando AWS CLI

Questa procedura illustra come utilizzare i parametri e le gerarchie di parametri con AWS CLI.

Per gestire i parametri mediante le gerarchie

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Eseguire questo comando per creare un parametro che utilizza il parametro `allowedPattern` e il tipo di parametro `String`. Il modello consentito in questo esempio indica che il valore del parametro deve avere una lunghezza compresa tra 1 e 4 cifre.

### Linux & macOS

```
aws ssm put-parameter \
 --name "/MyService/Test/MaxConnections" \
 --value 100 --allowed-pattern "\d{1,4}" \
 --type String
```

### Windows

```
aws ssm put-parameter ^
 --name "/MyService/Test/MaxConnections" ^
```



```
--value 100 --allowed-pattern "\d{1,4}" ^
--type String
```

Il comando restituisce il numero di versione del parametro.

3. Eseguire questo comando per tentare di sovrascrivere il parametro appena creato con un nuovo valore.

## Linux & macOS

```
aws ssm put-parameter \
 --name "/MyService/Test/MaxConnections" \
 --value 10,000 \
 --type String \
 --overwrite
```

## Windows

```
aws ssm put-parameter ^
 --name "/MyService/Test/MaxConnections" ^
 --value 10,000 ^
 --type String ^
 --overwrite
```

Il sistema restituisce il seguente errore perché il nuovo valore non è conforme ai requisiti del modello consentito specificato nella fase precedente.

```
An error occurred (ParameterPatternMismatchException) when calling the PutParameter
operation: Parameter value, cannot be validated against allowedPattern: \d{1,4}
```

4. Esegui il seguente comando per creare un parametro SecureString che utilizza un Chiave gestita da AWS. Il modello consentito in questo esempio conferma che il valore del parametro è un ID AMI.

## Linux & macOS

```
aws ssm put-parameter \
 --name "/MyService/Test/approved-ami" \
 --value "ami-0abcdef1234567890" \
 --allowed-pattern "ami-[a-f0-9]{17}" \
 --type SecureString
```

```
--type SecureString
```

## Windows

```
aws ssm put-parameter ^
 --name "/MyService/Test/approved-ami" ^
 --value "ami-0abcdef1234567890" ^
 --allowed-pattern "ami-[a-f0-9]{17}" ^
 --type SecureString
```

5. Eseguire questi comandi per creare altri parametri che utilizzano la struttura gerarchica definita nella fase precedente.

## Linux & macOS

```
aws ssm put-parameter \
 --name "/MyService/Test/DBname" \
 --value "SQLDevDb" \
 --type String
```

```
aws ssm put-parameter \
 --name "/MyService/Test/user" \
 --value "SA" \
 --type String
```

```
aws ssm put-parameter \
 --name "/MyService/Test/userType" \
 --value "SQLuser" \
 --type String
```

## Windows

```
aws ssm put-parameter ^
 --name "/MyService/Test/DBname" ^
 --value "SQLDevDb" ^
 --type String
```

```
aws ssm put-parameter ^
 --name "/MyService/Test/user" ^
 --value "SA" ^
```

```
--type String
```

```
aws ssm put-parameter ^
 --name "/MyService/Test/userType" ^
 --value "SQLuser" ^
 --type String
```

6. Eseguire questo comando per recuperare il valore dei due parametri.

#### Linux & macOS

```
aws ssm get-parameters \
 --names "/MyService/Test/user" "/MyService/Test/userType"
```

#### Windows

```
aws ssm get-parameters ^
 --names "/MyService/Test/user" "/MyService/Test/userType"
```

7. Eseguire questo comando per eseguire query su tutti i parametri sotto un singolo livello.

#### Linux & macOS

```
aws ssm get-parameters-by-path \
 --path "/MyService/Test"
```

#### Windows

```
aws ssm get-parameters-by-path ^
 --path "/MyService/Test"
```

8. Eseguire questo comando per eliminare due parametri.

#### Linux & macOS

```
aws ssm delete-parameters \
 --names "/IADRegion/Dev/user" "/IADRegion/Dev/userType"
```

#### Windows

```
aws ssm delete-parameters ^
```

```
--names "/IADRegion/Dev/user" "/IADRegion/Dev/userType"
```

## Impedire l'accesso a Parameter Store operazioni API

Utilizzando [condizioni specifiche del servizio](#) supportate dalle policy di Systems Manager for AWS Identity and Access Management (IAM), puoi consentire o negare esplicitamente l'accesso alle operazioni e ai contenuti delle Parameter Store API. Utilizzando queste condizioni, è possibile consentire solo a determinate entità IAM (utenti e ruoli) dell'organizzazione di richiamare determinate operazioni API o impedire a determinate entità IAM di eseguirle. Ciò include le azioni eseguite tramite la Parameter Store console, AWS Command Line Interface (AWS CLI) e gli SDK.

Prima di scrivere una policy che neghi l'accesso a determinati parametri, esaminala. [In che modo Parameter Store autorizza il recupero dei parametri](#) Parameter Store autorizza ogni operazione di recupero in modo indipendente, quindi una politica che nega una sola azione potrebbe non produrre il risultato desiderato.

### Argomenti

- [In che modo Parameter Store autorizza il recupero dei parametri](#)
- [Limitazione dell'accesso a parametri e percorsi specifici](#)
- [Limitazione della decrittografia dei valori dei parametri SecureString](#)
- [Chiavi di condizione specifiche per Parameter Store](#)
- [Impedire le modifiche ai parametri esistenti utilizzando SSM:overwrite](#)
- [Impedire la creazione o l'aggiornamento di parametri che utilizzano una policy di parametri utilizzando SSM:Policies](#)

## In che modo Parameter Store autorizza il recupero dei parametri

Quattro Parameter Store operazioni possono restituire un valore di parametro e ognuna è autorizzata in base alla propria azione IAM. Tre di esse eseguono l'autorizzazione in base ai parametri indicati nella richiesta. `GetParametersByPath` è l'eccezione: autorizza in base al percorso della richiesta anziché in base ai parametri restituiti.

| Operation                    | Azione IAM autorizzata        | Risorsa autorizzata contro |
|------------------------------|-------------------------------|----------------------------|
| <a href="#">GetParameter</a> | <code>ssm:GetParameter</code> | Il parametro richiesto     |

| Operation                           | Azione IAM autorizzata  | Risorsa autorizzata contro                                          |
|-------------------------------------|-------------------------|---------------------------------------------------------------------|
| <a href="#">GetParameters</a>       | ssm:GetParameters       | Ogni parametro richiesto                                            |
| <a href="#">GetParameterHistory</a> | ssm:GetParameterHistory | Il parametro richiesto                                              |
| <a href="#">GetParametersByPath</a> | ssm:GetParametersByPath | Il percorso specificato nella richiesta, non i parametri restituiti |

Due conseguenze di questo modello sono importanti quando si progettano politiche restrittive.

Ogni azione è autorizzata indipendentemente

Parameter Store autorizza ogni operazione di recupero rispetto alla propria azione IAM.

ssm:GetParameter La negazione non ha effetto sulle chiamate assm:GetParameters,, o. ssm:GetParametersByPath ssm:GetParameterHistory Per limitare l'accesso a un valore di parametro, negate tutte le azioni che possono restituirlo.

Poiché tutti e quattro i nomi delle azioni iniziano conGetParameter, il modello di caratteri jolly li ssm:GetParameter\* racchiude in un'unica dichiarazione. Per alcuni esempi, consulta [Negare le autorizzazioni](#).

**GetParametersByPath** è autorizzato in base al percorso richiesto

Ciò significa che le negazioni a livello di risorsa su un singolo parametro non limitano il risultato di una query di percorso. Se utilizzi gerarchie di parametri per separare ambienti o livelli di applicazione, applica i controlli ai percorsi stessi.

#### Important

Parameter Store autorizza l'GetParametersByPath operazione in base al percorso specificato nella richiesta, non in base a ciascun parametro restituito dall'operazione. Un principale a cui è consentito richiamare GetParametersByPath il percorso /a riceve tutti i parametri inclusi in quel percorso, inclusi/a/b. Ciò è vero anche se la stessa politica nega esplicitamente l'accesso /a/b ad altre azioni.

Per impedire la restituzione di un parametroGetParametersByPath, negate l'ssm:GetParametersByPath azione su ogni percorso predecessore che potrebbe

includere il parametro nei risultati. Ad esempio, per `/a/b` evitare che venga restituito, nega sia `ssm:GetParametersByPath` per che. `/a /`

Lo stesso schema si applica all'eliminazione. [DeleteParameters](#) è autorizzato contro `ssm:DeleteParameters`, non contro `ssm:DeleteParameter`. Per impedire a un responsabile di eliminare un parametro, nega entrambe le azioni.

#### Note

Parameter Store le operazioni sono registrate in AWS CloudTrail. Se desideri verificare quali operazioni sono state utilizzate per recuperare un parametro nel tuo account, consulta [Verifica e registrazione dell'attività Parameter Store](#).

### Limitazione dell'accesso a parametri e percorsi specifici

Utilizza il seguente approccio per limitare l'accesso a un parametro o a un set di parametri. Questo approccio riflette il comportamento di autorizzazione descritto in [In che modo Parameter Store autorizza il recupero dei parametri](#).

Per limitare l'accesso a parametri o percorsi specifici

1. Preferisci concedere un accesso ristretto piuttosto che negare un accesso ampio. Ove possibile, `Allow` riduci le istruzioni al set più piccolo di parametri di cui un principale ha bisogno, anziché concedere un ampio accesso e quindi sottrarre da esso. Un'Allow istruzione che non concede mai l'accesso a un parametro non dipende dalla corretta enumerazione di ogni azione.
2. Separate i parametri sensibili in un percorso separato. La limitazione dell'accesso è più semplice quando i parametri sensibili non condividono un percorso con parametri che i principali sono autorizzati a leggere. Ad esempio, memorizza i valori limitati in `/myapp/restricted/` anziché accanto alla configurazione generale in `/myapp/config/`. Per ulteriori informazioni sull'organizzazione dei parametri, vedere [Utilizzo delle gerarchie di parametri in Parameter Store](#).
3. Quando neghi l'accesso, nega ogni azione che può restituire il valore. Includi `ssm:GetParameters`, `ssm:GetParameterHistory`, `ssm:GetParametersByPath`, e o usa `ssm:GetParameter*` per abbinare tutti e quattro.
4. Perché **`GetParametersByPath`**, nega ogni percorso degli antenati. Un rifiuto sull'ARN del parametro non impedisce che il parametro venga restituito da una chiamata su un

- percorso sopra di esso. Proteggere/myapp/restricted/db-password, negare ssm:GetParametersByPath per/myapp/restricted, e/myapp. /
5. Per **SecureString** i parametri, limita **kms:Decrypt** la chiave KMS. Il recupero di un SecureString valore decrittografato richiede l'kms:Decrypt autorizzazione sulla chiave che lo ha crittografato, indipendentemente dall'operazione utilizzata. Parameter Store La negazione impedisce kms:Decrypt quindi la decrittografia attraverso ogni percorso di recupero. Consulta [Limitazione della decrittografia dei valori dei parametri SecureString](#).
  6. Verifica il risultato. Verifica ogni operazione di recupero come principale limitato. Includi un test GetParametersByPath rispetto a ciascun percorso precedente per confermare che la policy si comporti come previsto. Puoi anche utilizzare il simulatore di [policy IAM](#) per valutare una policy rispetto ad azioni e risorse specifiche.

Per ulteriori informazioni su come IAM combina Allow e Deny dichiara, consulta la logica di valutazione delle [policy](#) nella IAM User Guide.

### Limitazione della decrittografia dei valori dei parametri **SecureString**

SecureStringIl valore di un parametro viene crittografato con una chiave. AWS KMS Qualsiasi principale che recupera il valore decrittografato deve disporre dell'kms:Decrypt autorizzazione per quella chiave, a prescindere Parameter Store dall'operazione chiamata. Ciò rende le autorizzazioni delle AWS KMS chiavi un controllo efficace SecureString dei parametri, poiché una singola dichiarazione di AWS KMS politica si applica a tutti i percorsi di recupero contemporaneamente.

Per utilizzare questo controllo in modo efficace, crittografa i parametri sensibili con una chiave gestita dal cliente anziché con. Chiave gestita da AWS

#### Important

Il Chiave gestita da AWS for Parameter Store (aws/ssm) concede Decrypt l'autorizzazione a tutti i presidi IAM in. Account AWS Se hai bisogno di diversi livelli di accesso ai SecureString parametri all'interno di un account, non crittografarli con la chiave predefinita.

Per esempi di policy chiave, tra cui come negare l'accesso Chiave gestita da AWS e come concedere l'accesso a una chiave gestita dal cliente, consulta. [Crittografia e decrittografia dei parametri utilizzando AWS KMS keys](#)

 Note

La restrizione `kms:Decrypt` impedisce a un principale di leggere un valore crittografato. Non nasconde il nome, la descrizione o altri metadati del parametro, che non sono crittografati, e non impedisce che il parametro venga elencato. Usa le Parameter Store azioni negate come descritto in [Limitazione dell'accesso a parametri e percorsi specifici](#) per controllarle.

## Chiavi di condizione specifiche per Parameter Store

Systems Manager supporta due chiavi di condizione specifiche per Parameter Store. Entrambe si applicano al `PutParameter` funzionamento e controllano il modo in cui i parametri possono essere creati e aggiornati.

### `ssm:Overwrite`

Controlla se un responsabile può aggiornare un parametro esistente. Consulta [Impedire le modifiche ai parametri esistenti utilizzando SSM:overwrite](#).

### `ssm:Policies`

Controlla se un principale può creare o aggiornare un parametro che include una politica di parametri. Consulta [Impedire la creazione o l'aggiornamento di parametri che utilizzano una policy di parametri utilizzando SSM:Policies](#).

Per limitare i parametri che un responsabile può leggere, utilizza i controlli a livello di risorsa e a livello di azione come descritto in anziché nelle chiavi di condizione. [Limitazione dell'accesso a parametri e percorsi specifici](#)

## Impedire le modifiche ai parametri esistenti utilizzando `SSM:overwrite`

Utilizza la condizione `ssm:Overwrite` per controllare se le entità IAM siano in grado di aggiornare i parametri esistenti.

Nella seguente politica di esempio, l'"Allow"istruzione concede l'autorizzazione a creare parametri eseguendo l'operazione `PutParameter` API nel Account AWS 123456789012 nella regione degli Stati Uniti orientali (Ohio) (`us-east-2`).

Tuttavia, l'istruzione "Deny" impedisce alle Entità di modificare i valori dei parametri esistenti, poiché l'opzione `Overwrite` è esplicitamente negata per l'operazione `PutParameter`. In altre parole,



le Entità a cui è stata assegnata questa policy creano parametri, ma non apportano modifiche ai parametri esistenti.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:PutParameter"
],
 "Resource": "arn:aws:ssm:us-east-1:111122223333:parameter/*"
 },
 {
 "Effect": "Deny",
 "Action": [
 "ssm:PutParameter"
],
 "Condition": {
 "StringEquals": {
 "ssm:Overwrite": [
 "true"
]
 }
 },
 "Resource": "arn:aws:ssm:us-east-1:111122223333:parameter/*"
 }
]
}
```

Impedire la creazione o l'aggiornamento di parametri che utilizzano una policy di parametri utilizzando SSM:Policies

Utilizza la condizione `ssm:Policies` per controllare se le Entità creano parametri che includono una politica di parametro e aggiornano i parametri esistenti che effettivamente la includono.

Nel seguente esempio di policy, l'"Allow"istruzione concede l'autorizzazione generale alla creazione di parametri, ma impedisce alle Entità di creare o aggiornare parametri che includono una policy di parametri nella regione Account AWS 123456789012 nella regione Stati Uniti orientali (Ohio)

(us-east-2). "Deny" Ad ogni modo, le Entità continuano a creare o aggiornare parametri a cui non è assegnata una politica di parametro.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:PutParameter"
],
 "Resource": "arn:aws:ssm:us-east-1:111122223333:parameter/*"
 },
 {
 "Effect": "Deny",
 "Action": [
 "ssm:PutParameter"
],
 "Condition": {
 "StringEquals": {
 "ssm:Policies": [
 "true"
]
 }
 },
 "Resource": "arn:aws:ssm:us-east-1:111122223333:parameter/*"
 }
]
}
```

## Utilizzo delle etichette dei parametri in Parameter Store

Un'etichetta di parametro è un alias definito dall'utente che consente di semplificare la gestione delle diverse versioni di un parametro. Quando modificate un parametro, salva AWS Systems Manager automaticamente una nuova versione e incrementa il numero di versione di uno. Un'etichetta può aiutarti a ricordare lo scopo di una versione del parametro in presenza di più versioni.

Ad esempio, supponiamo che tu abbia un parametro chiamato /MyApp/Images/ApprovedAMI. Il valore del parametro è un ID AMI approvato per un ambiente di test. Al termine del test

dell'immagine, si desidera che il parametro utilizzi l'ID AMI approvato per un ambiente di produzione. Modifica il valore di `/MyApp/Images/ApprovedAMI`. Systems Manager crea automaticamente la versione due con il nuovo ID AMI. Per aiutarti a ricordare lo scopo di ciascuna versione, è possibile associare un'etichetta a ciascun parametro. Alla versione 1 è possibile associare l'etichetta Test, mentre alla versione 2 è possibile associare l'etichetta Produzione.

È possibile spostare le etichette da una versione di un parametro a un'altra. Ad esempio, se si crea la versione 3 del `/MyApp/Images/ApprovedAMI` parametro con un nuovo ID AMI approvato, è possibile spostare l'etichetta di produzione dalla versione 2 del parametro alla versione 3 del parametro.

Le etichette di parametro sono una valida alternativa ai tag. L'organizzazione potrebbe avere adottato linee guida rigorose per i tag che devono essere applicati alle varie risorse AWS. Al contrario, un'etichetta è una semplice stringa di testo associata a una versione specifica di un parametro.

Analogamente ai tag, è possibile eseguire query sui parametri utilizzando le etichette. Puoi visualizzare un elenco di versioni di parametri specifici che utilizzano tutte la stessa etichetta se interroghi il set di parametri utilizzando l'operazione [GetParametersByPath](#) API, come descritto più avanti in questa sezione.

#### Note

Se esegui un comando che specifica una versione di un parametro che non esiste, il comando ha esito negativo. Non torna al valore più recente o predefinito del parametro.

## Requisiti e restrizioni relativi alle etichette

Le etichette di parametro sono caratterizzate dalle limitazioni e dai requisiti seguenti:

- La versione di un parametro può avere un massimo di 10 etichette.
- Non è possibile associare la stessa etichetta a versioni differenti dello stesso parametro. Ad esempio, se la versione 1 del parametro è associata all'etichetta Produzione, non potrai associare l'etichetta Produzione alla versione 2.
- È possibile spostare un'etichetta da una versione di un parametro a un'altra.
- Non è possibile creare un'etichetta durante la creazione di un parametro. Devi associare un'etichetta a una versione specifica di un parametro.

- Se non vuoi più utilizzare un'etichetta di parametro, devi spostarla in un'altra versione di un parametro o cancellarla.
- Un'etichetta può avere una lunghezza massima di 100 caratteri.
- Le etichette possono contenere lettere (con distinzione tra lettere maiuscole e minuscole), numeri, punti (.), trattini (-) o caratteri di sottolineatura (\_).
- Le etichette non possono iniziare con un numero, "aws" o "ssm" (senza distinzione tra lettere maiuscole e minuscole). Se non è conforme a questi requisiti, un'etichetta non verrà associata alla versione di parametro e verrà visualizzata dal sistema nell'elenco `InvalidLabels`.

## Argomenti

- [Lavorare con etichette di parametro utilizzando la console](#)
- [Lavorare con le etichette dei parametri utilizzando il AWS CLI](#)

## Lavorare con etichette di parametro utilizzando la console

Questa sezione descrive come eseguire le attività seguenti utilizzando la console di Systems Manager.

- [Creazione di un'etichetta di parametro utilizzando la console](#)
- [Visualizzare le etichette associate a un parametro utilizzando la console](#)
- [Spostare un'etichetta di parametro utilizzando la console](#)
- [Eliminare delle etichette di parametro attraverso la console](#)

## Creazione di un'etichetta di parametro utilizzando la console

La procedura riportata di seguito illustra come associare un'etichetta a una versione specifica di un parametro esistente utilizzando la console di Systems Manager. Non è possibile associare un'etichetta durante la creazione di un parametro.

## Associazione di un'etichetta alla versione di un parametro

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Parameter Store.
3. Scegliere il nome di un parametro per aprire la corrispondente pagina dei dettagli.

4. Scegli la scheda Cronologia.
5. Scegliere la versione di parametro alla quale si desidera associare un'etichetta.
6. Scegliere Gestione delle etichette.
7. Scegliere Aggiungi nuova etichetta.
8. Nella casella di testo, inserire il nome dell'etichetta. Per aggiungere altre etichette, scegli Aggiungi nuova etichetta. È possibile associare un massimo di dieci etichette.
9. Al termine, scegli Salva modifiche.

Visualizzare le etichette associate a un parametro utilizzando la console

Una versione di parametro può avere un massimo di 10 etichette. La procedura riportata di seguito illustra come visualizzare tutte le etichette associate a una versione di parametro utilizzando la console di Systems Manager.

Visualizzazione delle etichette collegate alla versione di un parametro

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Parameter Store.
3. Scegliere il nome di un parametro per aprire la corrispondente pagina dei dettagli.
4. Scegli la scheda Cronologia.
5. Individuare la versione di parametro per la quale si desidera visualizzare tutte le etichette associate. Nella colonna Etichette sono visualizzate tutte le etichette associate a una versione di parametro.

Spostare un'etichetta di parametro utilizzando la console

La procedura riportata di seguito illustra come spostare un'etichetta di parametro in una versione diversa dello stesso parametro utilizzando la console di Systems Manager.

Spostamento di un'etichetta in una versione di parametro diversa

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Parameter Store.

3. Scegliere il nome di un parametro per aprire la corrispondente pagina dei dettagli.
4. Scegli la scheda Cronologia.
5. Scegliere la versione di parametro per la quale si desidera spostare l'etichetta.
6. Scegliere Gestione delle etichette.
7. Scegliere Aggiungi nuova etichetta.
8. Nella casella di testo, inserire il nome dell'etichetta.
9. Al termine, scegli Salva modifiche.

### Eliminare delle etichette di parametro attraverso la console

La procedura riportata di seguito descrive come eliminare una o più etichette di parametri utilizzando la console di Systems Manager.

#### Eliminazione di etichette da un parametro

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Parameter Store.
3. Scegliere il nome di un parametro per aprire la corrispondente pagina dei dettagli.
4. Scegli la scheda Cronologia.
5. Scegliere la versione di parametro per la quale si desidera eliminare le etichette.
6. Scegli Gestisci etichette.
7. Scegli Rimuovi accanto a ciascuna etichetta che desideri eliminare.
8. Al termine, scegli Salva modifiche.
9. Conferma che le modifiche siano corrette, inserisci **Confirm** nella casella di testo e scegli Conferma.

### Lavorare con le etichette dei parametri utilizzando il AWS CLI

Questa sezione descrive come eseguire le attività seguenti utilizzando AWS Command Line Interface (AWS CLI).

- [Creazione di una nuova etichetta di parametro utilizzando AWS CLI](#)
- [Visualizzazione delle etichette per un parametro utilizzando il AWS CLI](#)

- [Visualizzazione di un elenco di parametri a cui è stata assegnata un'etichetta utilizzando AWS CLI](#)
- [Spostare l'etichetta di un parametro utilizzando il AWS CLI](#)
- [Eliminazione delle etichette dei parametri utilizzando AWS CLI](#)

## Creazione di una nuova etichetta di parametro utilizzando AWS CLI

La procedura riportata di seguito illustra come associare un'etichetta a una versione specifica di un parametro esistente utilizzando AWS CLI. Non è possibile associare un'etichetta durante la creazione di un parametro.

Per creare un'etichetta di parametro

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Eseguire questo comando per visualizzare un elenco dei parametri ai quali si è autorizzati ad associare un'etichetta.

### Note

I parametri sono disponibili solo nel Regione AWS luogo in cui sono stati creati. Se il parametro al quale si desidera associare un'etichetta non è disponibile, verificare la regione.

```
aws ssm describe-parameters
```

Annotare il nome del parametro al quale si desidera associare un'etichetta.

3. Eseguire questo comando per visualizzare tutte le versioni del parametro.

```
aws ssm get-parameter-history --name "parameter-name"
```

Annotare la versione di parametro alla quale si desidera associare un'etichetta.

4. Eseguire questo comando per recuperare le informazioni su un parametro in base al numero di versione.

```
aws ssm get-parameters --names "parameter-name:version-number"
```

L'esempio seguente mostra il comando.

```
aws ssm get-parameters --names "/Production/ApprovedAMI:3"
```

5. Eseguire uno di questi comandi per associare un'etichetta a una versione di un parametro. Se si associano più etichette, separare i nomi di etichetta con uno spazio.

Associazione di un'etichetta alla versione più recente di un parametro

```
aws ssm label-parameter-version --name parameter-name --labels label-name
```

Associazione di un'etichetta a una versione specifica di un parametro

```
aws ssm label-parameter-version --name parameter-name --parameter-version version-number --labels label-name
```

Gli esempi seguenti mostrano i comandi.

```
aws ssm label-parameter-version --name /config/approved-ami --labels production
east-region finance
```

```
aws ssm label-parameter-version --name /config/approved-ami --parameter-version 3
--labels image-test
```

#### Note

Se l'output mostra l'etichetta creata nell'elenco `InvalidLabels`, significa che l'etichetta non è conforme ai requisiti descritti più indietro in questo argomento. Esaminare i requisiti e riprovare. Se l'elenco `InvalidLabels` è vuoto, significa che l'etichetta è stata correttamente applicata alla versione del parametro.

6. È possibile visualizzare i dettagli del parametro utilizzando il numero di versione o il nome dell'etichetta. Eseguire questo comando e specificare l'etichetta creata nella fase precedente.



```
aws ssm get-parameter --name parameter-name:label-name --with-decryption
```

Il comando restituisce informazioni simili alle seguenti.

```
{
 "Parameter": {
 "Version": version-number,
 "Type": "parameter-type",
 "Name": "parameter-name",
 "Value": "parameter-value",
 "Selector": "::label-name"
 }
}
```

 Note

Il valore di Selector nell'output rappresenta il numero di versione o l'etichetta specificata nel campo di input Name.

## Visualizzazione delle etichette per un parametro utilizzando il AWS CLI

È possibile utilizzare l'operazione [GetParameterHistory](#) API per visualizzare la cronologia completa e tutte le etichette associate a un parametro specificato. In alternativa, puoi utilizzare l'operazione [GetParametersByPath](#) API per visualizzare un elenco di tutti i parametri a cui è assegnata un'etichetta specifica.

Per visualizzare le etichette di un parametro utilizzando l'operazione [GetParameterHistory](#) API

1. Eseguire questo comando per visualizzare un elenco dei parametri per i quali è possibile visualizzare le etichette.

 Note

I parametri sono disponibili solo nella regione in cui sono stati creati. Se il parametro per il quale si desidera spostare un'etichetta non è disponibile, verificare la regione.

```
aws ssm describe-parameters
```

Annotare il nome del parametro di cui si desidera visualizzare le etichette.

2. Eseguire questo comando per visualizzare tutte le versioni del parametro.

```
aws ssm get-parameter-history --name parameter-name --with-decryption
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
 "Parameters": [
 {
 "Name": "/Config/endpoint",
 "LastModifiedDate": 1528932105.382,
 "Labels": [
 "Deprecated"
],
 "Value": "MyTestService-June-Release.example.com",
 "Version": 1,
 "LastModifiedUser": "arn:aws:iam::123456789012:user/test",
 "Type": "String"
 },
 {
 "Name": "/Config/endpoint",
 "LastModifiedDate": 1528932111.222,
 "Labels": [
 "Current"
],
 "Value": "MyTestService-July-Release.example.com",
 "Version": 2,
 "LastModifiedUser": "arn:aws:iam::123456789012:user/test",
 "Type": "String"
 }
]
}
```

Visualizzazione di un elenco di parametri a cui è stata assegnata un'etichetta utilizzando AWS CLI

È possibile utilizzare l'operazione [GetParametersByPath](#) API per visualizzare un elenco di tutti i parametri in un percorso a cui viene assegnata un'etichetta specifica.

Eseguire questo comando per visualizzare l'elenco dei parametri in un percorso a cui è assegnata un'etichetta specifica. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
aws ssm get-parameters-by-path \
 --path parameter-path \
 --parameter-filters Key=Label,Values=label-name,Option=Equals \
 --max-results a-number \
 --with-decryption --recursive
```

Il sistema restituisce informazioni simili alle seguenti. Per questo esempio, l'utente ha eseguito una ricerca nel percorso /Config.

```
{
 "Parameters": [
 {
 "Version": 3,
 "Type": "SecureString",
 "Name": "/Config/DBpwd",
 "Value": "MyS@perGr&pass33"
 },
 {
 "Version": 2,
 "Type": "String",
 "Name": "/Config/DBusername",
 "Value": "TestUserDB"
 },
 {
 "Version": 2,
 "Type": "String",
 "Name": "/Config/endpoint",
 "Value": "MyTestService-July-Release.example.com"
 }
]
}
```

## Spostare l'etichetta di un parametro utilizzando il AWS CLI

La procedura riportata di seguito illustra come spostare un'etichetta di parametro in una versione diversa dello stesso parametro.

Per spostare un'etichetta di parametro

1. Eseguire questo comando per visualizzare tutte le versioni del parametro. Sostituisci *parameter name* con le tue informazioni.

```
aws ssm get-parameter-history \
 --name "parameter name"
```

Prendi nota delle versioni dei parametri da e verso le quali desideri spostare l'etichetta.

2. Eseguire questo comando per assegnare un'etichetta esistente a una versione diversa di un parametro. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
aws ssm label-parameter-version \
 --name parameter name \
 --parameter-version version number \
 --labels name-of-existing-label
```

### Note

Se si desidera spostare un'etichetta esistente nella versione più recente di un parametro, rimuovere `--parameter-version` dal comando.

## Eliminazione delle etichette dei parametri utilizzando AWS CLI

La procedura seguente descrive come eliminare le etichette di parametro tramite AWS CLI.

Eliminazione di un'etichetta di parametro

1. Eseguire questo comando per visualizzare tutte le versioni del parametro. *parameter name* Sostituisci con le tue informazioni.

```
aws ssm get-parameter-history \
 --name "parameter name"
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
 "Parameters": [
 {
 "Name": "foo",
 "DataType": "text",
 "LastModifiedDate": 1607380761.11,
 "Labels": [
 "13",
 "12"
],
 "Value": "test",
 "Version": 1,
 "LastModifiedUser": "arn:aws:iam::123456789012:user/test",
 "Policies": [],
 "Tier": "Standard",
 "Type": "String"
 },
 {
 "Name": "foo",
 "DataType": "text",
 "LastModifiedDate": 1607380763.11,
 "Labels": [
 "11"
],
 "Value": "test",
 "Version": 2,
 "LastModifiedUser": "arn:aws:iam::123456789012:user/test",
 "Policies": [],
 "Tier": "Standard",
 "Type": "String"
 }
]
}
```

Annotare la versione di parametro della quale si desidera eliminare un'etichetta o delle etichette.

2. Eseguire il comando seguente per eliminare le etichette selezionate da tale parametro. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
aws ssm unlabel-parameter-version \
```

```
--name parameter name \
--parameter-version version \
--labels label 1,label 2,label 3
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
 "InvalidLabels": ["invalid"],
 "DeletedLabels" : ["Prod"]
}
```

## Utilizzo delle versioni dei parametri in Parameter Store

Ogni volta che modifichi il valore di un parametroParameter Store, uno strumento in AWS Systems Manager crea una nuova versione del parametro e mantiene le versioni precedenti. Quando inizialmente crei un parametro, Parameter Store assegna la versione 1 a tale parametro. Quando modifichi il valore del parametro, Parameter Store incrementa automaticamente il numero di versione di uno. È possibile visualizzare i dettagli, inclusi i valori, di tutte le versioni nella cronologia di un parametro.

Inoltre, è possibile specificare la versione di un parametro da utilizzare nei comandi API e nei documenti SSM; ad esempio, `ssm:MyParameter:3`. È possibile specificare un nome di parametro e un numero di versione specifico nelle chiamate API e nei documenti SSM. Se non specifichi un numero di versione, il sistema utilizza in automatico la versione più recente. Se specifichi il numero di una versione che non esiste, il sistema restituisce un errore anziché ricorrere alla versione più recente o predefinita del parametro.

È possibile utilizzare le versioni di un parametro per visualizzare il numero di variazioni di tale parametro in un periodo di tempo. Le versioni dei parametri forniscono inoltre un livello di protezione se un valore del parametro viene modificato per errore.

È possibile creare e mantenere un massimo di 100 versioni di un parametro. Dopo aver creato 100 versioni di un parametro, ogni volta che si crea una nuova versione, la versione meno recente del parametro viene rimossa dalla cronologia per fare spazio alla nuova versione.

Un'eccezione è quando sono presenti già 100 versioni dei parametri nella cronologia e un'etichetta di parametro viene assegnata alla versione meno recente di un parametro. In questo caso, tale versione non viene rimossa dalla cronologia e la richiesta di creare una nuova versione dei parametri non riesce. Questa protezione serve a impedire l'eliminazione delle versioni dei parametri con etichette

essenziali per l'organizzazione assegnate loro. Per continuare a creare nuovi parametri, spostare innanzitutto l'etichetta dalla versione meno recente del parametro a una più recente per utilizzarla nelle operazioni. Per informazioni sullo spostamento delle etichette dei parametri, vedere [Spostare un'etichetta di parametro utilizzando la console](#) e [Spostare l'etichetta di un parametro utilizzando il AWS CLI](#).

Nelle procedure seguenti viene illustrato come modificare un parametro e quindi verificare la creazione di una nuova versione. È possibile utilizzare il plugin `get-parameter` e `get-parameters` per visualizzare le versioni dei parametri. Per esempi sull'utilizzo di questi comandi, consultate [GetParameter](#) e [GetParameters](#) nella sezione AWS Systems Manager API Reference

### Argomenti

- [Creare una nuova versione di un parametro utilizzando la console](#)
- [Riferirsi a una versione di parametro](#)

### Creare una nuova versione di un parametro utilizzando la console

È possibile utilizzare la console di Systems Manager per creare una nuova versione di un parametro e visualizzare la cronologia delle versioni di un parametro.

Per creare una nuova versione di un parametro

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Parameter Store.
3. Scegliere il nome di un parametro creato in precedenza. Per ulteriori informazioni sulla creazione di un nuovo parametro, consultare [Creazione in corso Parameter Store parametri in Systems Manager](#).
4. Scegli Modifica.
5. Nella casella Valore, inserire un nuovo valore, quindi scegliere Salva modifiche.
6. Scegliere il nome del parametro appena aggiornato. Nella scheda Overview (Panoramica) verificare se il numero di versione è stato incrementato di 1 e controllare il nuovo valore.
7. Per visualizzare la cronologia di tutte le versioni di un parametro, scegli la scheda Cronologia .

## Riferirsi a una versione di parametro

È possibile fare riferimento a versioni di parametro specifiche nei comandi, nelle chiamate API e nei documenti SSM utilizzando il seguente formato: `ssm: parameter-name:version-number`.

Nel seguente esempio, Amazon Elastic Compute Cloud (Amazon EC2) `run-instances` command utilizza la versione 3 del parametro `golden-ami`.

### Linux & macOS

```
aws ec2 run-instances \
 --image-id resolve:ssm:/golden-ami:3 \
 --count 1 \
 --instance-type t2.micro \
 --key-name my-key-pair \
 --security-groups my-security-group
```

### Windows

```
aws ec2 run-instances ^
 --image-id resolve:ssm:/golden-ami:3 ^
 --count 1 ^
 --instance-type t2.micro ^
 --key-name my-key-pair ^
 --security-groups my-security-group
```

#### Note

L'utilizzo di `resolve` e di un valore di parametro funziona solo con l'opzione `--image-id` e con un parametro che contiene come valore un'Amazon Machine Image (AMI). Per ulteriori informazioni, consulta [Utilizzo del supporto nativo dei parametri in Parameter Store per Amazon Machine Image ID](#).

Di seguito è riportato un esempio di specifica della versione 2 di un parametro denominato `MyRunCommandParameter` in un documento SSM.

### YAML

```

```



```
schemaVersion: '2.2'
description: Run a shell script or specify the commands to run.
parameters:
 commands:
 type: String
 description: "(Required) Specify a shell script or a command to run."
 displayType: textarea
 default: "{{ssm:MyRunCommandParameter:2}}"
mainSteps:
- action: aws:runShellScript
 name: RunScript
 inputs:
 runCommand:
 - "{{commands}}"
```

## JSON

```
{
 "schemaVersion": "2.2",
 "description": "Run a shell script or specify the commands to run.",
 "parameters": {
 "commands": {
 "type": "String",
 "description": "(Required) Specify a shell script or a command to run.",
 "displayType": "textarea",
 "default": "{{ssm:MyRunCommandParameter:2}}"
 }
 },
 "mainSteps": [
 {
 "action": "aws:runShellScript",
 "name": "RunScript",
 "inputs": {
 "runCommand": [
 "{{commands}}"
]
 }
 }
]
}
```

## Utilizzo di parametri condivisi in Parameter Store

La condivisione di parametri avanzati semplifica la gestione dei dati di configurazione in un ambiente con più account. È possibile archiviare e gestire centralmente i parametri e condividerli con altri Account AWS utenti che devono farvi riferimento.

Parameter Store si integra con AWS Resource Access Manager (AWS RAM) per abilitare la condivisione avanzata dei parametri. AWS RAM è un servizio che consente di condividere risorse con altri Account AWS 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, i permessi da concedere e gli utenti con cui poter condividere. I consumatori includono:

- Specifico Account AWS all'interno o all'esterno della sua organizzazione in AWS Organizations
- Un'unità organizzativa all'interno della sua organizzazione in AWS Organizations
- La sua intera organizzazione in AWS Organizations

Per ulteriori informazioni AWS RAM, consultare la Guida [AWS RAM per l'utente](#).

Questo argomento spiega come condividere i propri parametri e come utilizzare i parametri condivisi.

### Indice

- [Prerequisiti per la condivisione dei parametri](#)
- [Condivisione di un parametro](#)
- [Interrompere la condivisione di un parametro](#)
- [Identificare i parametri condivisi](#)
- [Accesso ai parametri condivisi](#)
- [Set di autorizzazioni per la condivisione dei parametri](#)
- [Throughput massimo per i parametri condivisi](#)
- [Prezzi per i parametri condivisi](#)
- [Cross-account accesso per persone chiuse Account AWS](#)

### Prerequisiti per la condivisione dei parametri

È necessario soddisfare i seguenti prerequisiti prima di condividere i parametri dal proprio account:

- Per condividere un parametro, devi possederlo nel tuo Account AWS. Non è possibile condividere un parametro che è stato condiviso con te.
- Per condividere un parametro, è necessario che si trovi in un livello avanzato. Per informazioni sui livelli dei parametri, consulta [Scelta dei livelli di parametri in Parameter Store](#). Per informazioni sulla modifica di un parametro standard esistente in un parametro avanzato, consulta [Modifica di un parametro standard in un parametro avanzato](#).
- Per condividere un SecureString parametro, è necessario crittografarlo con una chiave gestita dal cliente e condividere la chiave separatamente tramite AWS Key Management Service. Chiavi gestite da AWS non può essere condiviso. I parametri crittografati con l'impostazione predefinita Chiave gestita da AWS possono essere aggiornati per utilizzare invece una chiave gestita dal cliente. Per le definizioni delle AWS KMS chiavi, consulta [AWS KMS i concetti](#) nella AWS Key Management Service Developer Guide.
- Per condividere un parametro con la tua organizzazione o un'unità organizzativa in AWS Organizations, devi abilitare la condivisione con AWS Organizations. Per ulteriori informazioni, consulta [Abilita la condivisione con AWS Organizations](#) nella Guida per l'utente di AWS RAM .

## Condivisione di un parametro

Per condividere un parametro, è necessario 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. Una condivisione di risorse specifica le risorse da condividere e i consumatori con cui sono condivise.

Quando condividi un parametro che possiedi con altri Account AWS, puoi scegliere tra due autorizzazioni AWS gestite da concedere ai consumatori. Per ulteriori informazioni, consulta [Set di autorizzazioni per la condivisione dei parametri](#).

Se fai parte di un'organizzazione AWS Organizations e la condivisione all'interno della tua organizzazione è abilitata, puoi concedere ai consumatori dell'organizzazione l'accesso dalla AWS RAM console al parametro condiviso. In caso contrario, i consumatori ricevono l'invito a partecipare alla condivisione di risorse e, dopo averlo accettato, ottengono l'accesso al parametro condiviso.

È possibile condividere un parametro tramite la console AWS RAM , o tramite AWS CLI.

### Note

Sebbene sia possibile condividere un parametro utilizzando l'operazione [PutResourcePolicy](#) API di Systems Manager, consigliamo invece di utilizzare AWS Resource Access Manager

(AWS RAM). Questo perché l'utilizzo PutResourcePolicy richiede il passaggio aggiuntivo di promozione del parametro a una condivisione di risorse standard utilizzando l'operazione AWS RAM [PromoteResourceShareCreatedFromPolicy](#) API. In caso contrario, il parametro non verrà restituito dall'operazione [DescribeParameters](#) API di Systems Manager utilizzando l'--sharedopzione.

Per condividere un parametro di tua proprietà, usa AWS RAM console

Consulta [Creazione di una condivisione di risorse su AWS RAM](#) nella Guida per l'utente di AWS RAM

Effettua le seguenti selezioni quando completi la procedura:

- Nella pagina sulla Fase 1, per le Risorse, vai su **Parameter Store Advanced Parameter**, quindi seleziona la casella di ogni parametro nel livello dei parametri avanzati che desideri condividere.
- Nella pagina sulla Fase 2, per le Autorizzazioni gestite, scegli l'autorizzazione da concedere ai consumatori, come descritto più avanti in [Set di autorizzazioni per la condivisione dei parametri](#).

Scegli altre opzioni in base agli obiettivi di condivisione dei parametri.

Per condividere un parametro di tua proprietà usando AWS CLI

Utilizza il comando [create-resource-share](#) per aggiungere parametri a una nuova condivisione di risorse.

Utilizza il comando [associate-resource-share](#) per aggiungere parametri a una condivisione di risorse esistente.

L'esempio seguente crea una nuova condivisione di risorse per condividere i parametri con i consumatori di un'organizzazione e di un account individuale.

```
aws ram create-resource-share \
 --name "MyParameter" \
 --resource-arns "arn:aws:ssm:us-east-2:123456789012:parameter/MyParameter" \
 --principals "arn:aws:organizations::123456789012:ou/o-63bEXAMPLE/ou-46xi-rEXAMPLE" \
 "987654321098"
```

## Interrompere la condivisione di un parametro

Quando interrompi la condivisione di un parametro condiviso, l'account utente non sarà più in grado di accedere al parametro.

Per interrompere la condivisione di un parametro è necessario rimuoverlo dalla condivisione di risorse. È possibile effettuare tale operazione mediante la console Systems Manager, AWS RAM o tramite AWS CLI.

Per interrompere la condivisione di un parametro di tua proprietà, usa AWS RAM console

Consulta [Aggiornamento di una condivisione di risorse su AWS RAM](#) nella Guida per l'utente di AWS RAM .

Per interrompere la condivisione di un parametro di tua proprietà, usa AWS CLI

Utilizza il comando [disassociate-resource-share](#).

## Identificare i parametri condivisi

Proprietari e consumatori identificano i parametri condivisi tramite AWS CLI.

Per identificare i parametri condivisi utilizzando AWS CLI

Per identificare i parametri condivisi utilizzando il AWS CLI, è possibile scegliere tra il [describe-parameters](#) comando Systems Manager e il AWS RAM [list-resources](#) comando.

Quando si utilizza l'opzione `--shared` con `describe-parameters`, il comando restituisce i parametri condivisi.

Di seguito è riportato un esempio:

```
aws ssm describe-parameters --shared
```

## Accesso ai parametri condivisi

I consumatori possono accedere ai parametri condivisi utilizzando gli strumenti a riga di AWS comando e gli AWS SDK. Per quanto riguarda l'account utente, i parametri condivisi non sono inclusi nella pagina I miei parametri.

Esempio CLI: accesso ai dettagli dei parametri condivisi utilizzando AWS CLI

Per accedere ai dettagli dei parametri condivisi utilizzando il AWS CLI, è possibile utilizzare i [get-parameters](#) comandi [get-parameter](#) o. È necessario specificare il parametro ARN completo, come il `--name`, per recuperare il parametro da un altro account.

Di seguito è riportato un esempio di :

```
aws ssm get-parameter \
 --name arn:aws:ssm:us-east-2:123456789012:parameter/MySharedParameter
```

## Integrazioni supportate e non supportate per parametri condivisi

Attualmente, è possibile utilizzare i parametri condivisi nei seguenti scenari di integrazione:

- AWS CloudFormation [parametri del modello](#)
- [Estensione lambda di parametri e segreti di AWS](#)
- [Modelli di lancio Amazon Elastic Compute Cloud \(EC2\)](#)
- Valori da ImageID utilizzare con il RunInstances comando [EC2](#) per creare istanze da un Amazon Machine Image () AMI
- [Recupero dei valori dei parametri nei runbook](#) per automazione, uno strumento di Systems Manager

Attualmente, gli scenari e i servizi integrati indicati di seguito non supportano l'uso di parametri condivisi:

- [Parametri nei comandi](#) in Run Command, uno strumento di Systems Manager
- AWS CloudFormation [riferimenti dinamici](#)
- I [valori delle variabili di ambiente](#) in AWS CodeBuild
- I [valori delle variabili di ambiente](#) in AWS App Runner
- Il [valore di un segreto](#) su Amazon Elastic Container Service

## Set di autorizzazioni per la condivisione dei parametri

Gli account utente ricevono l'accesso in sola lettura ai parametri condivisi con loro. L'utente non ha la possibilità di aggiornare o eliminare il parametro. L'utente non ha la possibilità di condividere il parametro con un terzo account.

Quando crei una condivisione di risorse AWS Resource Access Manager per condividere i tuoi parametri, puoi scegliere tra due set di autorizzazioni AWS gestiti per concedere questo accesso di sola lettura:

#### AWSRAMDefaultPermissionSSMParameterReadOnly

Operazioni consentite: `DescribeParameters`, `GetParameter`, `GetParameters`

#### AWSRAMPermissionSSMParameterReadOnlyWithHistory

Operazioni consentite: `DescribeParameters`, `GetParameter`, `GetParameters`, `GetParameterHistory`

Quando segui i passaggi descritti in [Creazione di una condivisione di risorse AWS RAM](#) nella Guida per l'AWS RAM utente, scegli `Parameter Store Advanced Parameters` come tipo di risorsa. Seleziona una delle autorizzazioni gestite in base al fatto che desideri che gli utenti visualizzino la cronologia dei parametri.

#### Note

Se stai recuperando parametri condivisi a livello di codice (ad esempio, utilizzando AWS Lambda), potresti dover aggiungere le `ssm:PutResourcePolicy` autorizzazioni `ssm:GetResourcePolicies` and a qualsiasi ruolo IAM che richiama le azioni API. AWS Resource Access Manager

#### Throughput massimo per i parametri condivisi

Systems Manager limita il throughput massimo (transazioni al secondo) per [GetParameter](#) e le operazioni [GetParameters](#). Il throughput viene applicato a livello di account individuale. Pertanto, ogni account che utilizza un parametro condiviso utilizza il throughput massimo consentito senza essere influenzato da altri account. Per ulteriori informazioni sul throughput massimo per i parametri, consulta i seguenti argomenti:

- [Aumento del throughput in Parameter Store](#)
- [Service Quotas di Systems Manager](#) in Riferimenti generali di Amazon Web Services.

## Prezzi per i parametri condivisi

Cross-account la condivisione è disponibile solo nel livello dei parametri avanzati. Per i parametri avanzati, vengono addebitati i costi al prezzo corrente per l'archiviazione e l'utilizzo dell'API per ciascun parametro avanzato. Lo storage del parametro avanzato è a carico del proprio account. A qualsiasi account utente che effettua una chiamata API a un parametro avanzato condiviso viene addebitato l'utilizzo del parametro.

Ad esempio, se l'account A crea un parametro avanzato, `MyAdvancedParameter`, a tale account vengono addebitati 0,05 USD al mese per archiviare il parametro.

L'account A condivide poi `MyAdvancedParameter` con l'account B e l'account C. Durante un mese, i tre account effettuano chiamate verso `MyAdvancedParameter`. La tabella seguente illustra i costi a cui sarebbero soggetti in base al numero di chiamate effettuate da ciascuno di essi.

### Note

I costi nella tabella seguente sono solo per scopi illustrativi. Per verificare i prezzi correnti, consulta la sezione [Prezzi AWS Systems Manager per il Parameter Store](#).

| Account                          | Numero di chiamate | Costi                                                                                                                                                                                                         |
|----------------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account A (account proprietario) | 10.000 chiamate    | <ul style="list-style-type: none"><li>Archiviazione dei parametri avanzati per un mese: 0,05 USD</li><li>10.000 chiamate verso <code>MyAdvancedParameter</code> : 0,05 USD</li><li>Totale: 0,10 USD</li></ul> |
| Conto B (account utente)         | 20.000 chiamate    | <ul style="list-style-type: none"><li>20.000 chiamate verso <code>MyAdvancedParameter</code> : 0,10 USD</li><li>Totale: 0,10 USD</li></ul>                                                                    |



| Account                  | Numero di chiamate | Costi                                                                                                                            |
|--------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Conto C (account utente) | 30.000 chiamate    | <ul style="list-style-type: none"> <li>30.000 chiamate verso MyAdvancedParameter : 0,15 USD</li> <li>Totale: 0,15 USD</li> </ul> |

## Cross-account accesso per persone chiuse Account AWS

Se il proprietario Account AWS di un parametro condiviso viene chiuso, tutti gli account di consumo perdono l'accesso al parametro condiviso. Quando l'account proprietario viene riaperto entro 90 giorni dalla chiusura dell'account, gli account utente riacquistano l'accesso ai parametri precedentemente condivisi. Per ulteriori informazioni sulla riapertura di un account durante il Post-Closure Periodo, vedi [Accedere al tuo account Account AWS dopo averlo chiuso](#) nella Guida Gestione dell'account AWS di riferimento.

## Utilizzo dei parametri in Parameter Store utilizzo di Run Command comandi

Puoi lavorare con i parametri in Run Command. Per ulteriori informazioni, consulta [AWS Systems Manager Run Command](#).

## Esecuzione di un parametro String utilizzando la console

La procedura seguente ti guiderà nel processo di creazione di un parametro in String e quindi nell'esecuzione di un comando che utilizza tale parametro.

Per eseguire un parametro String usando Parameter Store

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Run Command.
3. Seleziona Esegui comando.
4. Nell'elenco Command document (Documento comando) scegliere AWS-RunPowerShellScript (Windows) o AWS-RunShellScript (Linux).
5. In Command parameters (Parametri comando), immettere **echo {{ssm:parameter-name}}**  
Ad esempio: **echo {{ssm:/Test/helloWorld}}**.

6. Nella sezione Targets (Destinazioni), identificare i nodi in cui si desidera eseguire questa operazione specificando i tag, selezionando manualmente le istanze, i dispositivi edge o indicando un gruppo di risorse.

 Tip

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

7. In Altri parametri:

- In Commento, digita le informazioni su questo comando.
- In Timeout (secondi), specifica il numero di secondi che il sistema dovrà attendere prima di generare un errore per l'intera esecuzione del comando.

8. Per Controllo velocità:

- In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti presi di mira, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.
9. (Facoltativo) Nella sezione Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Scrivi l'output del comando in un bucket S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

 Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

10. Se vuoi che vengano inviate notifiche sullo stato dell'esecuzione del comando, nella sezione Notifiche SNS selezionare la casella di controllo Abilita notifiche SNS.

Per ulteriori informazioni sulla configurazione delle notifiche Amazon SNS per Run Command, consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

11. Scegli Esegui.
12. Nella pagina Command ID (ID comando), nell'area Targets and outputs (Destinazioni e uscite), seleziona il pulsante accanto all'ID di un nodo in cui è stato eseguito il comando, quindi scegliere View output (Visualizza output). Verificare che l'output del comando sia il valore fornito per il parametro, ad esempio **This is my first parameter**.

## Esecuzione di un parametro utilizzando il AWS CLI

### Esempio 1: comando semplice

Il comando di esempio seguente include un parametro Systems Manager denominato DNS-IP. Il valore di questo parametro è semplicemente l'indirizzo IP di un nodo. Questo esempio utilizza un comando AWS Command Line Interface (AWS CLI) per riprodurre il valore del parametro.

### Linux & macOS

```
aws ssm send-command \
 --document-name "AWS-RunShellScript" \
 --document-version "1" \
 --targets "Key=instanceids,Values=i-02573cafcfEXAMPLE" \
 --parameters "DNS-IP=192.168.1.1" --output-type text
```

```
--parameters "commands='echo {{ssm:DNS-IP}}'" \
--timeout-seconds 600 \
--max-concurrency "50" \
--max-errors "0" \
--region us-east-2
```

## Windows

```
aws ssm send-command ^
 --document-name "AWS-RunPowerShellScript" ^
 --document-version "1" ^
 --targets "Key=instanceids,Values=i-02573cafcfEXAMPLE" ^
 --parameters "commands='echo {{ssm:DNS-IP}}'" ^
 --timeout-seconds 600 ^
 --max-concurrency "50" ^
 --max-errors "0" ^
 --region us-east-2
```

Il comando restituisce informazioni simili alle seguenti.

```
{
 "Command": {
 "CommandId": "c70a4671-8098-42da-b885-89716EXAMPLE",
 "DocumentName": "AWS-RunShellScript",
 "DocumentVersion": "1",
 "Comment": "",
 "ExpiresAfter": "2023-12-26T15:19:17.771000-05:00",
 "Parameters": {
 "commands": [
 "echo {{ssm:DNS-IP}}"
]
 },
 "InstanceIds": [],
 "Targets": [
 {
 "Key": "instanceids",
 "Values": [
 "i-02573cafcfEXAMPLE"
]
 }
],
 "RequestedDateTime": "2023-12-26T14:09:17.771000-05:00",
```

```

 "Status": "Pending",
 "StatusDetails": "Pending",
 "OutputS3Region": "us-east-2",
 "OutputS3BucketName": "",
 "OutputS3KeyPrefix": "",
 "MaxConcurrency": "50",
 "MaxErrors": "0",
 "TargetCount": 0,
 "CompletedCount": 0,
 "ErrorCount": 0,
 "DeliveryTimedOutCount": 0,
 "ServiceRole": "",
 "NotificationConfig": {
 "NotificationArn": "",
 "NotificationEvents": [],
 "NotificationType": ""
 },
 "CloudWatchOutputConfig": {
 "CloudWatchLogGroupName": "",
 "CloudWatchOutputEnabled": false
 },
 "TimeoutSeconds": 600,
 "AlarmConfiguration": {
 "IgnorePollAlarmFailure": false,
 "Alarms": []
 },
 "TriggeredAlarms": []
}

```

Una volta completata l'esecuzione di un comando, è possibile visualizzare ulteriori informazioni su tale esecuzione utilizzando i comandi seguenti:

- [get-command-invocation](#): visualizza informazioni dettagliate sull'esecuzione del comando.
- [list-command-invocations](#): visualizza lo stato di esecuzione dei comandi su uno specifico nodo gestito.
- [list-commands](#): visualizza lo stato di esecuzione dei comandi su tutti i nodi gestiti.

Esempio 2: decriptazione del valore di un parametro **SecureString**

Il comando di esempio successivo utilizza un SecureString parametro denominato SecureMerchantId. Il comando utilizzato nel parameters campo recupera e decrittografa il valore del SecureString parametro senza includere il valore in testo normale direttamente nel comando.

## Linux

```
aws ssm send-command \
 --document-name "AWS-RunShellScript" \
 --document-version "1" \
 --targets "Key=instanceids,Values=i-02573cafcfEXAMPLE" \
 --parameters '{"commands":["merchant_id=$(aws ssm get-parameters --names
SecureMerchantId --with-decryption --query Parameters[0].Value --output text --
region us-east-2)","test -n "$merchant_id" && echo Retrieved SecureString parameter
value"]} \
 --timeout-seconds 600 \
 --max-concurrency "50" \
 --max-errors "0" \
 --region us-east-2
```

## Windows

```
aws ssm send-command ^
 --document-name "AWS-RunPowerShellScript" ^
 --document-version "1" ^
 --targets "Key=instanceids,Values=i-02573cafcfEXAMPLE" ^
 --parameters "commands=['$merchantId = (Get-SSMParameterValue -Names
SecureMerchantId -WithDecryption $True).Parameters[0].Value','if ($merchantId)
{ Write-Host ''Retrieved SecureString parameter value'' }']" ^
 --timeout-seconds 600 ^
 --max-concurrency "50" ^
 --max-errors "0" ^
 --region us-east-2
```

## Esempio 3: riferimento a un parametro in un documento SSM

È possibile fare riferimento ai parametri di Systems Manager anche nella sezione Parameters (Parametri) di un documento SSM, come illustrato nell'esempio seguente.

```
{
 "schemaVersion":"2.0",
 "description":"Sample version 2.0 document v2",
```

```

"parameters":{
 "commands" : {
 "type": "StringList",
 "default": ["{{ssm:parameter-name}}"]
 }
},
"mainSteps":[
 {
 "action":"aws:runShellScript",
 "name":"runShellScript",
 "inputs":{
 "runCommand": "{{commands}}"
 }
 }
]
}

```

Non confondere la sintassi simile per i parametri locali utilizzati nella sezione `runtimeConfig` dei documenti SSM con i parametri Parameter Store. Un parametro locale è diverso da un parametro di Systems Manager. I parametri locali si differenziano dai parametri di Systems Manager per l'assenza del prefisso `ssm:`.

```

"runtimeConfig":{
 "aws:runShellScript":{
 "properties":[
 {
 "id":"0.aws:runShellScript",
 "runCommand":"{{ commands }}",
 "workingDirectory":"{{ workingDirectory }}",
 "timeoutSeconds":"{{ executionTimeout }}"
 }
]
 }
}

```

#### Note

I documenti SSM non supportano i riferimenti ai parametri `SecureString`. Ciò significa che se vuoi usare i parametri `SecureString` con, ad esempio, Run Command, devi recuperare il valore del parametro prima di passarlo a Run Command, come illustrato negli esempi seguenti.

## Linux & macOS

```
merchant_id=$(aws ssm get-parameters --names parameter-name --with-decryption
--query Parameters[0].Value --output text)
```

```
aws ssm send-command \
 --document-name AWS-RunShellScript \
 --parameters commands="test \"\$merchant_id\" != \"\" && case
 \"\$merchant_id\" in merchant-*) echo Merchant ID value retrieved ;; *) echo
 Unexpected merchant ID value; exit 1 ;; esac" \
 --instance-ids instance-id
```

## Windows

```
aws ssm send-command ^
 --document-name AWS-RunPowerShellScript ^
 --parameters commands="$merchantId = (Get-SSMParameterValue -
Names parameter-name -WithDecryption $True).Parameters[0].Value; if
($merchantId -like 'merchant-*) { Write-Host 'Merchant ID value
retrieved' } else { Write-Host 'Unexpected merchant ID value'; exit 1 }" ^
 --instance-ids instance-id
```

## Powershell

```
$merchantId = (Get-SSMParameterValue -Names parameter-name -WithDecryption
$True).Parameters[0].Value
```

```
if ($merchantId -like "merchant-*) { Write-Host "Merchant ID value
retrieved" } else { Write-Host "Unexpected merchant ID value"; exit 1 }
```

## Utilizzo del supporto nativo dei parametri in Parameter Store per Amazon Machine Image ID

Quando crei un String parametro, puoi specificare il tipo di dati `aws:ec2:image` per assicurarti che il valore del parametro immesso sia un formato ID valido Amazon Machine Image (AMI).

Il supporto per i formati AMI ID consente di evitare di aggiornare tutti gli script e i modelli con un nuovo ID ogni volta AMI che viene modificato quello che si desidera utilizzare nei processi. È



possibile creare un parametro con il tipo di dati `aws:ec2:image` e, per il relativo valore, immettere l'ID di un'AMI. Si tratta dell'AMI da cui si desidera creare nuove istanze. È quindi possibile fare riferimento a questo parametro nei modelli, nei comandi e negli script.

Ad esempio, puoi specificare il parametro che contiene l'ID AMI quando esegui il comando `run-instances` Amazon Elastic Compute Cloud (Amazon EC2).

#### Note

L'utente che esegue questo comando deve disporre delle autorizzazioni AWS Identity and Access Management (IAM) che includono l'operazione `ssm:GetParameters` API per la convalida del valore del parametro. In caso contrario, il processo di creazione dei parametri non riesce.

## Linux & macOS

```
aws ec2 run-instances \
 --image-id resolve:ssm:/golden-ami \
 --count 1 \
 --instance-type t2.micro \
 --key-name my-key-pair \
 --security-groups my-security-group
```

## Windows

```
aws ec2 run-instances ^
 --image-id resolve:ssm:/golden-ami ^
 --count 1 ^
 --instance-type t2.micro ^
 --key-name my-key-pair ^
 --security-groups my-security-group
```

È inoltre possibile scegliere l'AMI preferita quando si crea un'istanza utilizzando la console Amazon EC2. Per ulteriori informazioni, consulta [Utilizzo di un parametro di Systems Manager per trovare un AMI](#) nella Guida per l'utente di Amazon EC2.

Quando è il momento di utilizzare un'AMI diversa nel flusso di lavoro di creazione dell'istanza, è necessario aggiornare solo il parametro con il nuovo valore dell'AMI. Parameter Store convalida nuovamente l'immissione di un ID nel formato corretto.

Concessione delle autorizzazioni per creare un parametro del tipo di dati `aws:ec2:image`

Utilizzando le policy AWS Identity and Access Management (IAM), puoi fornire o limitare l'accesso degli utenti alle operazioni e ai contenuti delle API. Parameter Store

Per creare un parametro relativo al tipo di dati `aws:ec2:image`, l'utente deve disporre di entrambe le autorizzazioni `ssm:PutParameter` e `ec2:DescribeImages`.

La policy dell'esempio seguente concede l'autorizzazione utenti per richiamare l'operazione API `PutParameter` per `aws:ec2:image`. Ciò significa che l'utente può aggiungere un parametro di tipo di dati `aws:ec2:image` al sistema.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "ssm:PutParameter",
 "Resource": "*"
 },
 {
 "Effect": "Allow",
 "Action": "ec2:DescribeImages",
 "Resource": "*"
 }
]
}
```

In che modo AMI la convalida del formato funziona

Quando si specifica `aws:ec2:image` come tipo di dati per un parametro, Systems Manager non crea immediatamente il parametro. Esegue invece un'operazione di convalida asincrona per assicurarsi che il valore del parametro soddisfi i requisiti di formattazione per un AMI ID e che il valore specificato sia disponibile nel tuo Account AWS.

Prima del completamento dell'operazione di convalida è possibile che venga generato un numero di versione del parametro. L'operazione potrebbe non essere completa anche se viene generato un numero di versione del parametro.

Per verificare se i parametri sono stati creati correttamente, ti consigliamo di utilizzare Amazon EventBridge per inviarti notifiche sulle tue operazioni e sui parametri. create update Queste notifiche segnalano se un'operazione con parametro ha avuto esito positivo o meno. Se un'operazione non riesce, la notifica include un messaggio di errore che indica il motivo dell'errore.

```
{
 "version": "0",
 "id": "eed4a719-0fa4-6a49-80d8-8ac65EXAMPLE",
 "detail-type": "Parameter Store Change",
 "source": "aws.ssm",
 "account": "111122223333",
 "time": "2020-05-26T22:04:42Z",
 "region": "us-east-2",
 "resources": [
 "arn:aws:ssm:us-east-2:111122223333:parameter/golden-ami"
],
 "detail": {
 "exception": "Unable to Describe Resource",
 "dataType": "aws:ec2:image",
 "name": "golden-ami",
 "type": "String",
 "operation": "Create"
 }
}
```

Per informazioni sulla sottoscrizione agli Parameter Store eventi in EventBridge, consulta [Impostazione delle notifiche o delle azioni di attivazione basate su Parameter Store eventi](#).

## Eliminazione dei parametri da Parameter Store

In questo argomento viene descritto come eliminare i parametri creati in Parameter Store, uno strumento di AWS Systems Manager.

### Warning

L'eliminazione di un parametro ne rimuove tutte le versioni. Una volta eliminato, non è possibile ripristinare il parametro e le rispettive versioni.

Per eliminare un parametro tramite la console

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Parameter Store.
3. Sulla scheda I miei parametri seleziona la casella di controllo di ciascun parametro da eliminare.
4. Scegli Elimina.
5. Nella finestra di dialogo di conferma, seleziona Elimina.

Per eliminare un parametro utilizzando AWS CLI

- Esegui il comando seguente:

```
aws ssm delete-parameter --name "my-parameter"
```

Sostituiscilo *my-parameter* con il nome del parametro da eliminare.

Per informazioni su tutte le opzioni disponibili per l'uso con il delete-parameter comando, vedere [delete-parameter](#) nella AWS Systems Manager sezione del AWS CLI Command Reference.

## Utilizzo di parametri pubblici in Parameter Store

Alcuni Servizi AWS pubblicano informazioni sugli artefatti comuni come parametri AWS Systems Manager pubblici. Ad esempio, il servizio Amazon Elastic Compute Cloud (Amazon EC2) pubblica le informazioni su Amazon Machine Images (AMIs) sotto forma di parametri pubblici.

Argomenti in questa guida

- [Alla scoperta dei parametri pubblici in Parameter Store](#)
- [Chiamata dei parametri pubblici AMI in Parameter Store](#)
- [Chiamare l'ECS ottimizzato AMI parametro pubblico in Parameter Store](#)
- [Chiamare l'EKS è ottimizzato AMI parametro pubblico in Parameter Store](#)
- [Richiamo di parametri pubblici per Servizi AWS, Regioni, endpoint, zone di disponibilità, zone locali e zone di lunghezza d'onda in Parameter Store](#)

## Post di blog correlati AWS

- [Utilizzo di Query for Regioni AWS, Endpoints e altro AWS Systems ManagerParameter Store](#)
- [Esecuzione di query per gli ID AMI Amazon Linux più recenti con il Parameter Store di AWS Systems Manager](#)
- [Esecuzione di query per l'AMI Windows più recente con il Parameter Store di AWS Systems Manager](#)

## Alla scoperta dei parametri pubblici in Parameter Store

È possibile ricercare parametri pubblici utilizzando la console Parameter Store o la AWS Command Line Interface.

Un nome di parametro pubblico inizia con `aws/service/list`. La parte successiva del nome corrisponde al servizio che possiede quel parametro.

Di seguito è riportato un elenco parziale di Servizi AWS e altre risorse che forniscono parametri pubblici:

- `ami-amazon-linux-latest`
- `ami-windows-latest`
- `ec2-macos`
- `appmesh`
- `aws-for-fluent-bit`
- `aws-sdk-pandas`
- `bottlerocket`
- `canonical`
- `cloud9`
- `datasync`
- `deeplearning`
- `ecs`
- `eks`
- `fis`
- `freebsd`

- `global-infrastructure`
- `marketplace`
- `neuron`
- `powertools`
- `sagemaker-distribution`
- `storagegateway`

Non tutti i parametri pubblici vengono pubblicati su tutti Regione AWS.

Trovare parametri pubblici tramite la console Parameter Store

È necessario disporre di almeno un parametro nel proprio Account AWS e Regione AWS prima di poter cercare parametri pubblici utilizzando la console.

Identificare parametri pubblici tramite la console

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Parameter Store.
3. Seleziona la scheda Public parameters (Parametri pubblici).
4. Seleziona il menu a discesa Select a service (Seleziona un servizio). Scegliere il servizio di cui si desidera utilizzare i parametri.
5. (Facoltativo) Filtrare i parametri di proprietà del servizio selezionato inserendo ulteriori informazioni nella barra di ricerca.
6. Scegliere il parametro pubblico che si desidera utilizzare.

Ricerca di parametri pubblici utilizzando il AWS CLI

Utilizza `describe-parameters` per la scoperta di parametri pubblici.

Utilizza `get-parameters-by-path` per ottenere il percorso effettivo per un servizio elencato in `/aws/service/list`. Per ottenere il percorso del servizio, rimuovere `/list` dal percorso. Ad esempio `/aws/service/list/ecs` diventa `/aws/service/ecs`.

Per recuperare un elenco di parametri pubblici di proprietà di diversi servizi in Parameter Store, eseguire il comando riportato di seguito.

```
aws ssm get-parameters-by-path --path /aws/service/list
```

Il comando restituisce informazioni simili alle seguenti. Questo esempio è stato troncato per motivi di spazio.

```
{
 "Parameters": [
 {
 "Name": "/aws/service/list/ami-al-latest",
 "Type": "String",
 "Value": "/aws/service/ami-al-latest/",
 "Version": 1,
 "LastModifiedDate": "2021-01-29T10:25:10.902000-08:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/list/ami-al-latest",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/list/ami-windows-latest",
 "Type": "String",
 "Value": "/aws/service/ami-windows-latest/",
 "Version": 1,
 "LastModifiedDate": "2021-01-29T10:25:12.567000-08:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/list/ami-windows-
latest",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/list/aws-storage-gateway-latest",
 "Type": "String",
 "Value": "/aws/service/aws-storage-gateway-latest/",
 "Version": 1,
 "LastModifiedDate": "2021-01-29T10:25:09.903000-08:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/list/aws-storage-
gateway-latest",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/list/global-infrastructure",
 "Type": "String",
 "Value": "/aws/service/global-infrastructure/",
 "Version": 1,
 "LastModifiedDate": "2021-01-29T10:25:11.901000-08:00",
```

```
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/list/global-
infrastructure",
 "DataType": "text"
 }
]
}
```

Se si desidera visualizzare i parametri di proprietà di un servizio specifico, scegliere il servizio dall'elenco prodotto dopo l'esecuzione del comando precedente. Quindi, effettua una chiamata `get-parameters-by-path` utilizzando il nome del servizio desiderato.

Ad esempio, `/aws/service/global-infrastructure`. Il percorso potrebbe essere a un livello (chiama solo parametri che corrispondono ai valori esatti forniti) o ricorsivo (contiene elementi nel percorso oltre a quello fornito).

#### Note

Il percorso `/aws/service/global-infrastructure` non è supportato per le query in tutte le Regioni. Per informazioni, consulta [Richiamo di parametri pubblici per Servizi AWS, Regioni, endpoint, zone di disponibilità, zone locali e zone di lunghezza d'onda in Parameter Store](#).

Se per il servizio specificato non si ottiene alcun risultato, aggiungere il flag `--recursive` ed eseguire nuovamente il comando.

```
aws ssm get-parameters-by-path --path /aws/service/global-infrastructure
```

Questo restituisce tutti i parametri di proprietà di `global-infrastructure`. Di seguito è riportato un esempio di :

```
{
 "Parameters": [
 {
 "Name": "/aws/service/global-infrastructure/current-region",
 "Type": "String",
 "LastModifiedDate": "2019-06-21T05:15:34.252000-07:00",
 "Version": 1,
 "Tier": "Standard",
 "Policies": [],
 }
]
}
```



```

 "DataType": "text"
 },
 {
 "Name": "/aws/service/global-infrastructure/version",
 "Type": "String",
 "LastModifiedDate": "2019-02-04T06:59:32.875000-08:00",
 "Version": 1,
 "Tier": "Standard",
 "Policies": [],
 "DataType": "text"
 }
]
}

```

È inoltre possibile visualizzare i parametri di proprietà di un servizio specifico utilizzando il filtro `Option:BeginsWith`.

```
aws ssm describe-parameters --parameter-filters "Key=Name, Option=BeginsWith, Values=/aws/service/ami-amazon-linux-latest"
```

Il comando restituisce informazioni simili alle seguenti. L'output di questo esempio è stato troncato per motivi di spazio.

```

{
 "Parameters": [
 {
 "Name": "/aws/service/ami-amazon-linux-latest/amzn-ami-hvm-x86_64-ebs",
 "Type": "String",
 "LastModifiedDate": "2021-01-26T13:39:40.686000-08:00",
 "Version": 25,
 "Tier": "Standard",
 "Policies": [],
 "DataType": "text"
 },
 {
 "Name": "/aws/service/ami-amazon-linux-latest/amzn-ami-hvm-x86_64-gp2",
 "Type": "String",
 "LastModifiedDate": "2021-01-26T13:39:40.807000-08:00",
 "Version": 25,
 "Tier": "Standard",
 "Policies": [],
 "DataType": "text"
 }
]
}

```

```
 },
 {
 "Name": "/aws/service/ami-amazon-linux-latest/amzn-ami-hvm-x86_64-s3",
 "Type": "String",
 "LastModifiedDate": "2021-01-26T13:39:40.920000-08:00",
 "Version": 25,
 "Tier": "Standard",
 "Policies": [],
 "DataType": "text"
 }
]
}
```

#### Note

I parametri restituiti potrebbero essere diversi quando si utilizza `Option=BeginsWith` perché utilizza un modello di ricerca diverso.

## Chiamata dei parametri pubblici AMI in Parameter Store

Sono disponibili parametri pubblici Amazon Elastic Compute Cloud (Amazon EC2) Amazon Machine Image (AMI) per Amazon Linux 2, Amazon Linux 2023 (AL2023), macOS e Windows Server dai percorsi seguenti:

- Amazon Linux 2 e Amazon Linux 2023: `/aws/service/ami-amazon-linux-latest`
- macOS: `/aws/service/ec2-macos`
- Windows Server: `/aws/service/ami-windows-latest`

## Chiamata di parametri pubblici AMI per Amazon Linux 2 e Amazon Linux 2023

Puoi visualizzare un elenco di tutti gli Amazon Linux 2 e Amazon Linux 2023 (AL2023) AMIs nella versione corrente Regione AWS utilizzando il seguente comando in AWS Command Line Interface (AWS CLI).

### Linux & macOS

```
aws ssm get-parameters-by-path \
```

```
--path /aws/service/ami-amazon-linux-latest \
--query 'Parameters[].Name'
```

## Windows

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

Il comando restituisce informazioni simili alle seguenti.

```
[
 "/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-arm64",
 "/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-x86_64",
 "/aws/service/ami-amazon-linux-latest/al2023-ami-minimal-kernel-6.1-arm64",
 "/aws/service/ami-amazon-linux-latest/al2023-ami-minimal-kernel-6.1-x86_64",
 "/aws/service/ami-amazon-linux-latest/al2023-ami-minimal-kernel-default-arm64",
 "/aws/service/ami-amazon-linux-latest/amzn-ami-hvm-x86_64-gp2",
 "/aws/service/ami-amazon-linux-latest/amzn-ami-hvm-x86_64-s3",
 "/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-ebs",
 "/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2",
 "/aws/service/ami-amazon-linux-latest/amzn2-ami-kernel-5.10-hvm-x86_64-ebs",
 "/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-arm64",
 "/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64",
 "/aws/service/ami-amazon-linux-latest/al2023-ami-minimal-kernel-default-x86_64",
 "/aws/service/ami-amazon-linux-latest/amzn-ami-hvm-x86_64-ebs",
 "/aws/service/ami-amazon-linux-latest/amzn-ami-minimal-hvm-x86_64-ebs",
 "/aws/service/ami-amazon-linux-latest/amzn-ami-minimal-hvm-x86_64-s3",
 "/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-arm64-gp2",
 "/aws/service/ami-amazon-linux-latest/amzn2-ami-kernel-5.10-hvm-arm64-gp2",
 "/aws/service/ami-amazon-linux-latest/amzn2-ami-kernel-5.10-hvm-x86_64-gp2",
 "/aws/service/ami-amazon-linux-latest/amzn2-ami-minimal-hvm-arm64-ebs",
 "/aws/service/ami-amazon-linux-latest/amzn2-ami-minimal-hvm-x86_64-ebs"
]
```

È possibile visualizzare i dettagli su questi AMIs, inclusi gli ID AMI e gli Amazon Resource Name (ARN), utilizzando il comando seguente.

## Linux & macOS

```
aws ssm get-parameters-by-path \
```

```
--path "/aws/service/ami-amazon-linux-latest" \
--region region
```

## Windows

```
aws ssm get-parameters-by-path ^
 --path "/aws/service/ami-amazon-linux-latest" ^
 --region region
```

*region* rappresenta l'identificatore di una regione AWS supportata da AWS Systems Manager, ad esempio `us-east-2` per la regione Stati Uniti orientali (Ohio). Per un elenco dei *region* valori supportati, vedere la colonna Regione negli [endpoint del servizio Systems Manager](#) in [Riferimenti generali di Amazon Web Services](#)

Il comando restituisce informazioni simili alle seguenti. L'output di questo esempio è stato troncato per motivi di spazio.

```
{
 "Parameters": [
 {
 "Name": "/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-arm64",
 "Type": "String",
 "Value": "ami-0b1b8b24a6c8e5d8b",
 "Version": 69,
 "LastModifiedDate": "2024-03-13T14:05:09.583000-04:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-arm64",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-x86_64",
 "Type": "String",
 "Value": "ami-0e0bf53f6def86294",
 "Version": 69,
 "LastModifiedDate": "2024-03-13T14:05:09.890000-04:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-x86_64",
 "DataType": "text"
 },
 {

```

```

 "Name": "/aws/service/ami-amazon-linux-latest/al2023-ami-minimal-
kernel-6.1-arm64",
 "Type": "String",
 "Value": "ami-09951bb66f9e5b5a5",
 "Version": 69,
 "LastModifiedDate": "2024-03-13T14:05:10.197000-04:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ami-amazon-linux-
latest/al2023-ami-minimal-kernel-6.1-arm64",
 "DataType": "text"
 }
]
}

```

È possibile visualizzare i dettagli di uno specifico AMI utilizzando l'operazione [GetParameters](#) API con il AMI nome completo, incluso il percorso. Di seguito è illustrato un esempio di comando.

## Linux & macOS

```

aws ssm get-parameters \
 --names /aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-arm64 \
 --region us-east-2

```

## Windows

```

aws ssm get-parameters ^
 --names /aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-arm64 ^
 --region us-east-2

```

Il comando restituisce le informazioni seguenti.

```

{
 "Parameters": [
 {
 "Name": "/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-arm64",
 "Type": "String",
 "Value": "ami-0b1b8b24a6c8e5d8b",
 "Version": 69,
 "LastModifiedDate": "2024-03-13T14:05:09.583000-04:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ami-amazon-linux-
latest/al2023-ami-kernel-6.1-arm64",
 "DataType": "text"
 }
]
}

```

```
 }
],
 "InvalidParameters": []
}
```

## Chiamata dei parametri pubblici AMI per macOS

È possibile visualizzare un elenco di tutti gli elementi presenti macOS AMIs nella versione corrente Regione AWS utilizzando il seguente comando in AWS CLI.

### Linux & macOS

```
aws ssm get-parameters-by-path \
 --path /aws/service/ec2-macos\
 --query 'Parameters[].Name'
```

### Windows

```
aws ssm get-parameters-by-path ^
 --path /aws/service/ec2-macos ^
 --query Parameters[].Name
```

Il comando restituisce informazioni simili alle seguenti.

```
[
 "/aws/service/ec2-macos/sonoma/x86_64_mac/latest/image_id",
 "/aws/service/ec2-macos/ventura/x86_64_mac/latest/image_id",
 "/aws/service/ec2-macos/sonoma/arm64_mac/latest/image_id",
 "/aws/service/ec2-macos/ventura/arm64_mac/latest/image_id"
]
```

È possibile visualizzare i dettagli su questi AMIs, inclusi gli ID AMI e gli Amazon Resource Name (ARN), utilizzando il comando seguente.

### Linux & macOS

```
aws ssm get-parameters-by-path \
 --path "/aws/service/ec2-macos" \
 --region region
```

## Windows

```
aws ssm get-parameters-by-path ^
 --path "/aws/service/ec2-macos" ^
 --region region
```

*region* rappresenta l'identificatore di una regione AWS supportata da AWS Systems Manager, ad esempio `us-east-2` per la regione Stati Uniti orientali (Ohio). Per un elenco dei *region* valori supportati, vedere la colonna Regione negli [endpoint del servizio Systems Manager](#) in. Riferimenti generali di Amazon Web Services

Il comando restituisce informazioni simili alle seguenti. L'output di questo esempio è stato troncato per motivi di spazio.

```
{
 "Parameters": [
 ...sample results pending...
]
}
```

È possibile visualizzare i dettagli di uno specifico AMI utilizzando l'operazione [GetParameters](#) API con il AMI nome completo, incluso il percorso. Di seguito è illustrato un esempio di comando.

## Linux & macOS

```
aws ssm get-parameters \
 --names /aws/service/ec2-macos/...pending... \
 --region us-east-2
```

## Windows

```
aws ssm get-parameters ^
 --names /aws/service/ec2-macos/...pending... ^
 --region us-east-2
```

Il comando restituisce le informazioni seguenti.

```
{
```

```

 "Parameters": [
 ...sample results pending...
],
 "InvalidParameters": []
}

```

## Chiamata dei parametri pubblici AMI per Windows Server

È possibile visualizzare un elenco di tutti gli elementi presenti Windows Server AMIs nella versione corrente Regione AWS utilizzando il seguente comando in AWS CLI.

## Linux & macOS

```

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

```

## Windows

```

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

```

Il comando restituisce informazioni simili alle seguenti. L'output di questo esempio è stato troncato per motivi di spazio.

```

[
 "/aws/service/ami-windows-latest/EC2LaunchV2-Windows_Server-2016-English-Full-Base",
 "/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-SQL_2014_SP3_Enterprise",
 "/aws/service/ami-windows-latest/Windows_Server-2016-German-Full-Base",
 "/aws/service/ami-windows-latest/Windows_Server-2016-Japanese-Full-SQL_2016_SP3_Standard",
 "/aws/service/ami-windows-latest/Windows_Server-2016-Japanese-Full-SQL_2017_Web",
 "/aws/service/ami-windows-latest/Windows_Server-2019-English-Core-EKS_Optimized-1.25",
 "/aws/service/ami-windows-latest/Windows_Server-2019-Italian-Full-Base",
 "/aws/service/ami-windows-latest/Windows_Server-2022-Japanese-Full-SQL_2019_Enterprise",
 "/aws/service/ami-windows-latest/Windows_Server-2022-Portuguese_Brazil-Full-Base",

```



```

"/aws/service/ami-windows-latest/amzn2-ami-hvm-2.0.20191217.0-x86_64-gp2-mono",
"/aws/service/ami-windows-latest/Windows_Server-2016-English-Deep-Learning",
"/aws/service/ami-windows-latest/Windows_Server-2016-Japanese-Full-
SQL_2016_SP3_Web",
"/aws/service/ami-windows-latest/Windows_Server-2016-Korean-Full-Base",
"/aws/service/ami-windows-latest/Windows_Server-2019-English-STIG-Core",
"/aws/service/ami-windows-latest/Windows_Server-2019-French-Full-Base",
"/aws/service/ami-windows-latest/Windows_Server-2019-Japanese-Full-
SQL_2017_Enterprise",
"/aws/service/ami-windows-latest/Windows_Server-2019-Korean-Full-Base",
"/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-SQL_2022_Web",
"/aws/service/ami-windows-latest/Windows_Server-2022-Italian-Full-Base",
"/aws/service/ami-windows-latest/amzn2-x86_64-SQL_2019_Express",
"/aws/service/ami-windows-latest/EC2LaunchV2-Windows_Server-2016-English-Core-
Base",
"/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-
SQL_2019_Enterprise",
"/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-
SQL_2019_Standard",
"/aws/service/ami-windows-latest/Windows_Server-2016-Portuguese_Portugal-Full-
Base",
"/aws/service/ami-windows-latest/Windows_Server-2019-English-Core-
EKS_Optimized-1.24",
"/aws/service/ami-windows-latest/Windows_Server-2019-English-Deep-Learning",
"/aws/service/ami-windows-latest/Windows_Server-2019-English-Full-SQL_2017_Web",
"/aws/service/ami-windows-latest/Windows_Server-2019-Hungarian-Full-Base
]

```

È possibile visualizzare i dettagli su questi AMIs, inclusi gli ID AMI e gli Amazon Resource Name (ARN), utilizzando il comando seguente.

## Linux & macOS

```

aws ssm get-parameters-by-path \
 --path "/aws/service/ami-windows-latest" \
 --region region

```

## Windows

```

aws ssm get-parameters-by-path ^
 --path "/aws/service/ami-windows-latest" ^
 --region region

```

**region** rappresenta l'identificatore di una regione AWS supportata da AWS Systems Manager, ad esempio `us-east-2` per la regione Stati Uniti orientali (Ohio). Per un elenco dei **region** valori supportati, vedere la colonna Regione negli [endpoint del servizio Systems Manager](#) in. Riferimenti generali di Amazon Web Services

Il comando restituisce informazioni simili alle seguenti. L'output di questo esempio è stato troncato per motivi di spazio.

```
{
 "Parameters": [
 {
 "Name": "/aws/service/ami-windows-latest/EC2LaunchV2-Windows_Server-2016-English-Full-Base",
 "Type": "String",
 "Value": "ami-0a30b2e65863e2d16",
 "Version": 36,
 "LastModifiedDate": "2024-03-15T15:58:37.976000-04:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ami-windows-latest/EC2LaunchV2-Windows_Server-2016-English-Full-Base",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-SQL_2014_SP3_Enterprise",
 "Type": "String",
 "Value": "ami-001f20c053dd120ce",
 "Version": 69,
 "LastModifiedDate": "2024-03-15T15:53:58.905000-04:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-SQL_2014_SP3_Enterprise",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/ami-windows-latest/Windows_Server-2016-German-Full-Base",
 "Type": "String",
 "Value": "ami-063be4935453e94e9",
 "Version": 102,
 "LastModifiedDate": "2024-03-15T15:51:12.003000-04:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ami-windows-latest/Windows_Server-2016-German-Full-Base",
 "DataType": "text"
 }
]
}
```

```
]
}
```

È possibile visualizzare i dettagli di uno specifico AMI utilizzando l'operazione [GetParameters](#) API con il nome completo, incluso il percorso. Di seguito è illustrato un esempio di comando.

## Linux & macOS

```
aws ssm get-parameters \
 --names /aws/service/ami-windows-latest/EC2LaunchV2-Windows_Server-2016-English-
Full-Base \
 --region us-east-2
```

## Windows

```
aws ssm get-parameters ^
 --names /aws/service/ami-windows-latest/EC2LaunchV2-Windows_Server-2016-English-
Full-Base ^
 --region us-east-2
```

Il comando restituisce le informazioni seguenti.

```
{
 "Parameters": [
 {
 "Name": "/aws/service/ami-windows-latest/EC2LaunchV2-Windows_Server-2016-
English-Full-Base",
 "Type": "String",
 "Value": "ami-0a30b2e65863e2d16",
 "Version": 36,
 "LastModifiedDate": "2024-03-15T15:58:37.976000-04:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ami-windows-latest/
EC2LaunchV2-Windows_Server-2016-English-Full-Base",
 "DataType": "text"
 }
],
 "InvalidParameters": []
}
```

## Chiamare l'ECS ottimizzato AMI parametro pubblico in Parameter Store

Il servizio Amazon Elastic Container Service (Amazon ECS) pubblica il nome dell'ultima Amazon ECS ottimizzata Amazon Machine Images (AMIs) come parametro pubblico. Gli utenti sono incoraggiati a utilizzare questa AMI durante la creazione di un nuovo cluster Amazon Elastic Compute Cloud (Amazon EC2) per Amazon ECS, perché le AMIs ottimizzate includono correzioni di bug e aggiornamenti delle funzionalità.

Utilizza il comando seguente per visualizzare il nome dell'ultima Amazon ECS ottimizzata AMI Per Amazon Linux 2. Per visualizzare i comandi per altri sistemi operativi, consulta [Recupero dei ECS-Optimized AMI metadati di Amazon](#) nella Amazon Elastic Container Service Developer Guide.

### Linux & macOS

```
aws ssm get-parameters \
 --names /aws/service/ecs/optimized-ami/amazon-linux-2/recommended
```

### Windows

```
aws ssm get-parameters ^
 --names /aws/service/ecs/optimized-ami/amazon-linux-2/recommended
```

Il comando restituisce informazioni simili alle seguenti.

```
{
 "Parameters": [
 {
 "Name": "/aws/service/ecs/optimized-ami/amazon-linux-2/recommended",
 "Type": "String",
 "Value": "{\"schema_version\":1,\"image_name\":\"amzn2-ami-ecs-hvm-2.0.20210929-x86_64-ebs\",\"image_id\":\"ami-0c38a2329ed4dae9a\",\"os\":\"Amazon Linux 2\",\"ecs_runtime_version\":\"Docker version 20.10.7\",\"ecs_agent_version\":\"1.55.4\"}\",",
 "Version": 73,
 "LastModifiedDate": "2021-10-06T16:35:10.004000-07:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ecs/optimized-ami/amazon-linux-2/recommended",
 "DataType": "text"
 }
],
}
```

```
"InvalidParameters": []
}
```

Chiamare l'EKS è ottimizzato AMI parametro pubblico in Parameter Store

Il servizio Amazon Elastic Kubernetes Service (Amazon EKS) pubblica il nome dell'ultima Amazon EKS ottimizzata Amazon Machine Image (AMI) come parametro pubblico. Si consiglia agli utenti di utilizzare quest'AMI quando si aggiungono nodi a un cluster Amazon EKS, poiché le nuove versioni includono patch Kubernetes e aggiornamenti di sicurezza. In precedenza, assicurarsi di utilizzare l'ultima AMI significava dover controllare la documentazione Amazon EKS e aggiornare manualmente eventuali modelli di implementazione o risorse con il nuovo ID AMI.

Utilizza il comando seguente per visualizzare il nome dell'ultima Amazon EKS ottimizzata AMI Per Amazon Linux 2.

Linux & macOS

```
aws ssm get-parameters \
 --names /aws/service/eks/optimized-ami/1.14/amazon-linux-2/recommended
```

Windows

```
aws ssm get-parameters ^
 --names /aws/service/eks/optimized-ami/1.14/amazon-linux-2/recommended
```

Il comando restituisce informazioni simili alle seguenti.

```
{
 "Parameters": [
 {
 "Name": "/aws/service/eks/optimized-ami/1.14/amazon-linux-2/recommended",
 "Type": "String",
 "Value": "{\"schema_version\":\"2\",\"image_id\":\"ami-08984d8491de17ca0\", \"image_name\":\"amazon-eks-node-1.14-v20201007\", \"release_version\": \"1.14.9-20201007\"}",
 "Version": 24,
 "LastModifiedDate": "2020-11-17T10:16:09.971000-08:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/eks/optimized-ami/1.14/amazon-linux-2/recommended",
 "DataType": "text"
 }
]
}
```

```
 }
],
 "InvalidParameters": []
}
```

Richiamo di parametri pubblici per Servizi AWS, Regioni, endpoint, zone di disponibilità, zone locali e zone di lunghezza d'onda in Parameter Store

Puoi chiamare le zone di servizio Regione AWS, endpoint, di disponibilità e di lunghezza d'onda dei parametri pubblici utilizzando il seguente percorso.

`/aws/service/global-infrastructure`

#### Note

Attualmente, il percorso `/aws/service/global-infrastructure` è supportato solo per le interrogazioni relative a: Regioni AWS

- Stati Uniti orientali (Virginia settentrionale) (us-east-1)
- Stati Uniti orientali (Ohio) (us-east-2)
- Stati Uniti occidentali (California settentrionale) (us-west-1)
- Stati Uniti occidentali (Oregon) (us-west-2)
- Asia Pacifico (Hong Kong) (ap-east-1)
- Asia Pacifico (Mumbai) (ap-south-1)
- Asia Pacifico (Seoul) (ap-northeast-2)
- Asia Pacifico (Singapore) (ap-southeast-1)
- Asia Pacifico (Sydney) (ap-southeast-2)
- Asia Pacifico (Tokyo) (ap-northeast-1)
- Canada (Centrale) (ca-central-1)
- Europa (Francoforte) (eu-central-1)
- Europa (Irlanda) (eu-west-1)
- Europa (Londra) (eu-west-2)
- Europa (Parigi) (eu-west-3)
- Europa (Stoccolma) (eu-north-1)

Se lavori in una [regione commerciale](#) diversa, è possibile specificare una regione supportata nella query per visualizzare i risultati. Ad esempio, se lavori nella regione Canada occidentale (Calgary) (ca-west-1), è possibile specificare Canada (Centrale) (ca-central-1) nella query:

```
aws ssm get-parameters-by-path \
 --path /aws/service/global-infrastructure/regions \
 --region ca-central-1
```

## Visualizza attivo Regioni AWS

È possibile visualizzare un elenco di tutti gli attivi Regioni AWS utilizzando il seguente comando in AWS Command Line Interface (AWS CLI).

### Linux & macOS

```
aws ssm get-parameters-by-path \
 --path /aws/service/global-infrastructure/regions \
 --query 'Parameters[].Name'
```

### Windows

```
aws ssm get-parameters-by-path ^
 --path /aws/service/global-infrastructure/regions ^
 --query Parameters[].Name
```

Il comando restituisce informazioni simili alle seguenti.

```
[
 "/aws/service/global-infrastructure/regions/af-south-1",
 "/aws/service/global-infrastructure/regions/ap-east-1",
 "/aws/service/global-infrastructure/regions/ap-northeast-3",
 "/aws/service/global-infrastructure/regions/ap-south-2",
 "/aws/service/global-infrastructure/regions/ca-central-1",
 "/aws/service/global-infrastructure/regions/eu-central-2",
 "/aws/service/global-infrastructure/regions/eu-west-2",
 "/aws/service/global-infrastructure/regions/eu-west-3",
 "/aws/service/global-infrastructure/regions/us-east-1",
```

```
"/aws/service/global-infrastructure/regions/us-gov-west-1",
"/aws/service/global-infrastructure/regions/ap-northeast-2",
"/aws/service/global-infrastructure/regions/ap-southeast-1",
"/aws/service/global-infrastructure/regions/ap-southeast-2",
"/aws/service/global-infrastructure/regions/ap-southeast-3",
"/aws/service/global-infrastructure/regions/cn-north-1",
"/aws/service/global-infrastructure/regions/cn-northwest-1",
"/aws/service/global-infrastructure/regions/eu-south-1",
"/aws/service/global-infrastructure/regions/eu-south-2",
"/aws/service/global-infrastructure/regions/us-east-2",
"/aws/service/global-infrastructure/regions/us-west-1",
"/aws/service/global-infrastructure/regions/ap-northeast-1",
"/aws/service/global-infrastructure/regions/ap-south-1",
"/aws/service/global-infrastructure/regions/ap-southeast-4",
"/aws/service/global-infrastructure/regions/ca-west-1",
"/aws/service/global-infrastructure/regions/eu-central-1",
"/aws/service/global-infrastructure/regions/il-central-1",
"/aws/service/global-infrastructure/regions/me-central-1",
"/aws/service/global-infrastructure/regions/me-south-1",
"/aws/service/global-infrastructure/regions/sa-east-1",
"/aws/service/global-infrastructure/regions/us-gov-east-1",
"/aws/service/global-infrastructure/regions/eu-north-1",
"/aws/service/global-infrastructure/regions/eu-west-1",
"/aws/service/global-infrastructure/regions/us-west-2"
]
```

## Visualizzazione disponibile Servizi AWS

È possibile visualizzare un elenco completo di tutti i disponibili Servizi AWS e ordinarli in ordine alfabetico utilizzando il seguente comando. L'output di questo esempio è stato troncato per motivi di spazio.

### Linux & macOS

```
aws ssm get-parameters-by-path \
 --path /aws/service/global-infrastructure/services \
 --query 'Parameters[].Name | sort(@)'
```

### Windows

```
aws ssm get-parameters-by-path ^
 --path /aws/service/global-infrastructure/services ^
```



```
--query "Parameters[].Name | sort(@)"
```

Il comando restituisce informazioni simili alle seguenti. Questo esempio è stato troncato per motivi di spazio.

```
[
 "/aws/service/global-infrastructure/services/accessanalyzer",
 "/aws/service/global-infrastructure/services/account",
 "/aws/service/global-infrastructure/services/acm",
 "/aws/service/global-infrastructure/services/acm-pca",
 "/aws/service/global-infrastructure/services/ahl",
 "/aws/service/global-infrastructure/services/aiq",
 "/aws/service/global-infrastructure/services/amazonlocationsservice",
 "/aws/service/global-infrastructure/services/amplify",
 "/aws/service/global-infrastructure/services/amplifybackend",
 "/aws/service/global-infrastructure/services/apigateway",
 "/aws/service/global-infrastructure/services/apigatewaymanagementapi",
 "/aws/service/global-infrastructure/services/apigatewayv2",
 "/aws/service/global-infrastructure/services/appconfig",
 "/aws/service/global-infrastructure/services/appconfigdata",
 "/aws/service/global-infrastructure/services/appflow",
 "/aws/service/global-infrastructure/services/appintegrations",
 "/aws/service/global-infrastructure/services/application-autoscaling",
 "/aws/service/global-infrastructure/services/application-insights",
 "/aws/service/global-infrastructure/services/applicationcostprofiler",
 "/aws/service/global-infrastructure/services/appmesh",
 "/aws/service/global-infrastructure/services/apprunner",
 "/aws/service/global-infrastructure/services/appstream",
 "/aws/service/global-infrastructure/services/appsync",
 "/aws/service/global-infrastructure/services/aps",
 "/aws/service/global-infrastructure/services/arc-zonal-shift",
 "/aws/service/global-infrastructure/services/artifact",
 "/aws/service/global-infrastructure/services/athena",
 "/aws/service/global-infrastructure/services/auditmanager",
 "/aws/service/global-infrastructure/services/augmentedairuntime",
 "/aws/service/global-infrastructure/services/aurora",
 "/aws/service/global-infrastructure/services/autoscaling",
 "/aws/service/global-infrastructure/services/aws-appfabric",
 "/aws/service/global-infrastructure/services/awshealthdashboard",
```

Visualizza le regioni supportate per un Servizio AWS

È possibile visualizzare un elenco di Regioni AWS dove è disponibile un servizio. Questo esempio utilizza AWS Systems Manager (ssm).

## Linux & macOS

```
aws ssm get-parameters-by-path \
 --path /aws/service/global-infrastructure/services/ssm/regions \
 --query 'Parameters[].Value'
```

## Windows

```
aws ssm get-parameters-by-path ^
 --path /aws/service/global-infrastructure/services/ssm/regions ^
 --query Parameters[].Value
```

Il comando restituisce informazioni simili alle seguenti.

```
[
 "ap-south-1",
 "eu-central-1",
 "eu-central-2",
 "eu-west-1",
 "eu-west-2",
 "eu-west-3",
 "il-central-1",
 "me-south-1",
 "us-east-2",
 "us-gov-west-1",
 "af-south-1",
 "ap-northeast-3",
 "ap-southeast-1",
 "ap-southeast-4",
 "ca-central-1",
 "ca-west-1",
 "cn-north-1",
 "eu-north-1",
 "eu-south-2",
 "us-west-1",
 "ap-east-1",
 "ap-northeast-1",
 "ap-northeast-2",
 "ap-southeast-2",
```

```
"ap-southeast-3",
"cn-northwest-1",
"eu-south-1",
"me-central-1",
"us-gov-east-1",
"us-west-2",
"ap-south-2",
"sa-east-1",
"us-east-1"
]
```

## Visualizzazione dell'endpoint regionale per un servizio

È possibile visualizzare un endpoint regionale per un servizio utilizzando il comando seguente. Questo comando esegue una query nella Regione Stati Uniti orientali (Ohio) (us-east-2).

### Linux & macOS

```
aws ssm get-parameter \
 --name /aws/service/global-infrastructure/regions/us-east-2/services/ssm/
endpoint \
 --query 'Parameter.Value'
```

### Windows

```
aws ssm get-parameter ^
 --name /aws/service/global-infrastructure/regions/us-east-2/services/ssm/
endpoint ^
 --query Parameter.Value
```

Il comando restituisce informazioni simili alle seguenti.

```
"ssm.us-east-2.amazonaws.com"
```

## Visualizzazione dei dettagli completi della zona di disponibilità

È possibile visualizzare le zone di disponibilità utilizzando il comando seguente.

### Linux & macOS

```
aws ssm get-parameters-by-path \
 --name /aws/service/global-infrastructure/regions/us-east-2/services/ssm/
endpoint ^
 --query 'ParameterList[*].Value'
```

```
--path /aws/service/global-infrastructure/availability-zones/
```

## Windows

```
aws ssm get-parameters-by-path ^
--path /aws/service/global-infrastructure/availability-zones/
```

Il comando restituisce informazioni simili alle seguenti. Questo esempio è stato troncato per motivi di spazio.

```
{
 "Parameters": [
 {
 "Name": "/aws/service/global-infrastructure/availability-zones/afs1-az3",
 "Type": "String",
 "Value": "afs1-az3",
 "Version": 1,
 "LastModifiedDate": "2020-04-21T12:05:35.375000-04:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
availability-zones/afs1-az3",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/global-infrastructure/availability-zones/aps1-az2",
 "Type": "String",
 "Value": "aps1-az2",
 "Version": 1,
 "LastModifiedDate": "2020-04-03T16:13:57.351000-04:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
availability-zones/aps1-az2",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/global-infrastructure/availability-zones/apse3-az1",
 "Type": "String",
 "Value": "apse3-az1",
 "Version": 1,
 "LastModifiedDate": "2021-12-13T08:51:38.983000-05:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
availability-zones/apse3-az1",
 "DataType": "text"
 }
]
}
```

```
]
}
```

## Visualizzazione dei soli nomi delle zone di disponibilità

È possibile visualizzare solo i nomi delle zone di disponibilità utilizzando il comando seguente.

### Linux & macOS

```
aws ssm get-parameters-by-path \
 --path /aws/service/global-infrastructure/availability-zones \
 --query 'Parameters[].Name | sort(@)'
```

### Windows

```
aws ssm get-parameters-by-path ^
 --path /aws/service/global-infrastructure/availability-zones ^
 --query "Parameters[].Name | sort(@)"
```

Il comando restituisce informazioni simili alle seguenti. Questo esempio è stato troncato per motivi di spazio.

```
[
 "/aws/service/global-infrastructure/availability-zones/afs1-az1",
 "/aws/service/global-infrastructure/availability-zones/afs1-az2",
 "/aws/service/global-infrastructure/availability-zones/afs1-az3",
 "/aws/service/global-infrastructure/availability-zones/ape1-az1",
 "/aws/service/global-infrastructure/availability-zones/ape1-az2",
 "/aws/service/global-infrastructure/availability-zones/ape1-az3",
 "/aws/service/global-infrastructure/availability-zones/apne1-az1",
 "/aws/service/global-infrastructure/availability-zones/apne1-az2",
 "/aws/service/global-infrastructure/availability-zones/apne1-az3",
 "/aws/service/global-infrastructure/availability-zones/apne1-az4"
```

## Visualizzazione dei nomi delle zone di disponibilità in una singola regione

È possibile visualizzare i nomi delle zone di disponibilità in una regione (us-east-2, in questo esempio) utilizzando il comando seguente.

## Linux & macOS

```
aws ssm get-parameters-by-path \
 --path /aws/service/global-infrastructure/regions/us-east-2/availability-zones \
 --query 'Parameters[].Name | sort(@)'
```

## Windows

```
aws ssm get-parameters-by-path ^
 --path /aws/service/global-infrastructure/regions/us-east-2/availability-zones ^
 --query "Parameters[].Name | sort(@)"
```

Il comando restituisce informazioni simili alle seguenti.

```
[
 "/aws/service/global-infrastructure/regions/us-east-2/availability-zones/use2-az1",
 "/aws/service/global-infrastructure/regions/us-east-2/availability-zones/use2-az2",
 "/aws/service/global-infrastructure/regions/us-east-2/availability-zones/use2-az3"
```

## Visualizzazione solo degli ARN delle zone di disponibilità

È possibile visualizzare solo gli Amazon Resource Name (ARN) delle zone di disponibilità utilizzando il comando seguente.

## Linux & macOS

```
aws ssm get-parameters-by-path \
 --path /aws/service/global-infrastructure/availability-zones \
 --query 'Parameters[].ARN | sort(@)'
```

## Windows

```
aws ssm get-parameters-by-path ^
 --path /aws/service/global-infrastructure/availability-zones ^
 --query "Parameters[].ARN | sort(@)"
```

Il comando restituisce informazioni simili alle seguenti. Questo esempio è stato troncato per motivi di spazio.

```
[
 "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/availability-zones/afs1-az1",
 "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/availability-zones/afs1-az2",
 "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/availability-zones/afs1-az3",
 "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/availability-zones/apel1-az1",
 "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/availability-zones/apel1-az2",
 "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/availability-zones/apel1-az3",
 "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/availability-zones/apne1-az1",
```

## Visualizzazione dei dettagli delle zone locali

È possibile visualizzare le zone locali utilizzando il seguente comando.

### Linux & macOS

```
aws ssm get-parameters-by-path \
 --path /aws/service/global-infrastructure/local-zones
```

### Windows

```
aws ssm get-parameters-by-path ^
 --path /aws/service/global-infrastructure/local-zones
```

Il comando restituisce informazioni simili alle seguenti. Questo esempio è stato troncato per motivi di spazio.

```
{
 "Parameters": [
 {
 "Name": "/aws/service/global-infrastructure/local-zones/afs1-los1-az1",
 "Type": "String",
 "Value": "afs1-los1-az1",
 "Version": 1,
```

```

 "LastModifiedDate": "2023-01-25T11:53:11.690000-05:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/afs1-los1-az1",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/global-infrastructure/local-zones/apne1-tpe1-az1",
 "Type": "String",
 "Value": "apne1-tpe1-az1",
 "Version": 1,
 "LastModifiedDate": "2024-03-15T12:35:41.076000-04:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/apne1-tpe1-az1",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/global-infrastructure/local-zones/aps1-ccu1-az1",
 "Type": "String",
 "Value": "aps1-ccu1-az1",
 "Version": 1,
 "LastModifiedDate": "2022-12-19T11:34:43.351000-05:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/aps1-ccu1-az1",
 "DataType": "text"
 }
]
}

```

Visualizza i dettagli delle zone di Wavelength

È possibile visualizzare le zone di Wavelength utilizzando il seguente comando.

Linux & macOS

```
aws ssm get-parameters-by-path \
 --path /aws/service/global-infrastructure/wavelength-zones
```

Windows

```
aws ssm get-parameters-by-path ^
 --path /aws/service/global-infrastructure/wavelength-zones
```



Il comando restituisce informazioni simili alle seguenti. Questo esempio è stato troncato per motivi di spazio.

```
{
 "Parameters": [
 {
 "Name": "/aws/service/global-infrastructure/wavelength-zones/apne1-wl1-nrt-wlz1",
 "Type": "String",
 "Value": "apne1-wl1-nrt-wlz1",
 "Version": 3,
 "LastModifiedDate": "2020-12-15T17:16:04.715000-05:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/wavelength-zones/apne1-wl1-nrt-wlz1",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/global-infrastructure/wavelength-zones/apne2-wl1-sel-wlz1",
 "Type": "String",
 "Value": "apne2-wl1-sel-wlz1",
 "Version": 1,
 "LastModifiedDate": "2022-05-25T12:29:13.862000-04:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/wavelength-zones/apne2-wl1-sel-wlz1",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/global-infrastructure/wavelength-zones/cac1-wl1-yto-wlz1",
 "Type": "String",
 "Value": "cac1-wl1-yto-wlz1",
 "Version": 1,
 "LastModifiedDate": "2022-04-26T09:57:44.495000-04:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/wavelength-zones/cac1-wl1-yto-wlz1",
 "DataType": "text"
 }
]
}
```

Visualizzazione di tutti i parametri e i valori in una zona locale

È possibile visualizzare tutti i dati dei parametri per una zona locale utilizzando il comando seguente.

## Linux & macOS

```
aws ssm get-parameters-by-path \
 --path "/aws/service/global-infrastructure/local-zones/usw2-lax1-az1/"
```

## Windows

```
aws ssm get-parameters-by-path ^
 --path "/aws/service/global-infrastructure/local-zones/use1-bos1-az1"
```

Il comando restituisce informazioni simili alle seguenti. Questo esempio è stato troncato per motivi di spazio.

```
{
 "Parameters": [
 {
 "Name": "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/
geolocationCountry",
 "Type": "String",
 "Value": "US",
 "Version": 3,
 "LastModifiedDate": "2020-12-15T14:16:17.641000-08:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/use1-bos1-az1/geolocationCountry",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/
geolocationRegion",
 "Type": "String",
 "Value": "US-MA",
 "Version": 3,
 "LastModifiedDate": "2020-12-15T14:16:17.794000-08:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/use1-bos1-az1/geolocationRegion",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/
location",
```

```

 "Type": "String",
 "Value": "US East (Boston)",
 "Version": 1,
 "LastModifiedDate": "2021-01-11T10:53:24.634000-08:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/use1-bos1-az1/location",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/
network-border-group",
 "Type": "String",
 "Value": "us-east-1-bos-1",
 "Version": 3,
 "LastModifiedDate": "2020-12-15T14:16:20.641000-08:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/use1-bos1-az1/network-border-group",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/
parent-availability-zone",
 "Type": "String",
 "Value": "use1-az4",
 "Version": 3,
 "LastModifiedDate": "2020-12-15T14:16:20.834000-08:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/use1-bos1-az1/parent-availability-zone",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/
parent-region",
 "Type": "String",
 "Value": "us-east-1",
 "Version": 3,
 "LastModifiedDate": "2020-12-15T14:16:20.721000-08:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/use1-bos1-az1/parent-region",
 "DataType": "text"
 },
 {
 "Name": "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/zone-
group",

```

```

 "Type": "String",
 "Value": "us-east-1-bos-1",
 "Version": 3,
 "LastModifiedDate": "2020-12-15T14:16:17.983000-08:00",
 "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/use1-bos1-az1/zone-group",
 "DataType": "text"
 }
]
}

```

## Visualizzazione dei soli nomi dei parametri delle zone locali

È possibile visualizzare solo i nomi dei parametri delle zone locali utilizzando il comando seguente.

### Linux & macOS

```

aws ssm get-parameters-by-path \
 --path /aws/service/global-infrastructure/local-zones/usw2-lax1-az1 \
 --query 'Parameters[].Name | sort(@)'

```

### Windows

```

aws ssm get-parameters-by-path ^
 --path /aws/service/global-infrastructure/local-zones/use1-bos1-az1 ^
 --query "Parameters[].Name | sort(@)"

```

Il comando restituisce informazioni simili alle seguenti.

```

[
 "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/geolocationCountry",
 "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/geolocationRegion",
 "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/location",
 "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/network-border-
group",
 "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/parent-availability-
zone",
 "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/parent-region",
 "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/zone-group"
]

```

## Spiegazioni passo per passo di Parameter Store

La procedura dettagliata in questa sezione mostra come creare, archiviare ed eseguire parametri Parameter Store in un ambiente di test. Questa procedura guidata illustra come utilizzare Parameter Store con altri strumenti di Systems Manager. È possibile anche usare Parameter Store con altri Servizi AWS. Per ulteriori informazioni, consulta [Riferimento Parameter Store](#).

### Indice

- [Creazione di un SecureString parametro in Parameter Store e unire un nodo a un Domain \(PowerShell\)](#)

### Creazione di un SecureString parametro in Parameter Store e unire un nodo a un Domain (PowerShell)

Questa procedura dettagliata mostra come unire un Windows Server nodo a un dominio utilizzando AWS Systems Manager SecureString parametri e Run Command. La procedura guidata utilizza i parametri di dominio standard, ad esempio il nome di dominio e un nome utente di dominio. Questi valori vengono passati come valori di stringa non criptati. La password del dominio viene crittografata con una Chiave gestita da AWS e viene passata come una stringa crittografata.

### Prerequisiti

In questa procedura guidata si presuppone che siano già stati specificati il nome di dominio e l'indirizzo IP del server DNS nel set di opzioni DHCP associato ad Amazon VPC. Per ulteriori informazioni, consulta [Utilizzo dei set di opzioni DHCP](#) nella Guida utente Amazon VPC.

Per creare un parametro **SecureString** e aggiungere un nodo a un dominio

1. Inserisci i parametri nel sistema utilizzando AWS Tools for Windows PowerShell.

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

```
Write-SSMParameter -Name "domainName" -Value "DOMAIN-NAME" -Type String
Write-SSMParameter -Name "domainJoinUserName" -Value "DOMAIN\USERNAME" -Type String
Write-SSMParameter -Name "domainJoinPassword" -Value "PASSWORD" -Type SecureString
```

Solo il valore di un parametro SecureString viene crittografato. I nomi dei parametri, le descrizioni e altre proprietà non sono crittografati.

2. Allega le seguenti politiche AWS Identity and Access Management (IAM) alle autorizzazioni del ruolo IAM per il tuo nodo:
- **AmazonSSMManagedInstanceCore**: obbligatorio Questa policy AWS gestita consente a un nodo gestito di utilizzare le funzionalità di base del servizio Systems Manager.
  - **AmazonSSMDirectoryServiceAccess**: obbligatorio Questa policy AWS gestita consente di accedere SSM Agent Servizio di directory AWS per conto dell'utente alle richieste di aggiunta al dominio da parte del nodo gestito.
  - Una politica personalizzata per l'accesso al bucket S3: obbligatoria. SSM Agent, che si trova sul tuo nodo ed esegue attività di Systems Manager, richiede l'accesso a bucket specifici di Amazon-owned Amazon Simple Storage Service (Amazon S3). Nella policy di bucket S3 creata, fornire anche l'accesso ai bucket S3 personali necessari per le operazioni di Systems Manager.

Esempi: è possibile scrivere l'output per i comandi `Run Command` o le sessioni `Session Manager` in un bucket S3 e quindi utilizzare questo output più tardi per l'audit o la risoluzione dei problemi. È possibile archiviare gli script di accesso o gli elenchi delle baseline delle patch personalizzati in un bucket S3 e quindi fare riferimento allo script o all'elenco quando si esegue un comando oppure quando viene applicata una baseline delle patch.

Per ulteriori informazioni su come creare una policy personalizzata per l'accesso ai bucket Amazon S3, consulta [Creare una policy di bucket S3 personalizzata per un profilo dell'istanza](#)

#### Note

La memorizzazione dei log di output in un bucket S3 è facoltativa ma, se si è deciso di utilizzarla, si consiglia di impostarla all'inizio del processo di configurazione di Systems Manager. Per ulteriori informazioni, consulta [Creazione di un bucket](#) nella Guida per l'utente di Amazon Simple Storage Service.

- **CloudWatchAgentServerPolicy**: opzionale. Questa policy AWS gestita consente di eseguire l' CloudWatch agente su nodi gestiti. Questa policy consente di leggere le informazioni su un nodo e scriverle su Amazon CloudWatch. Il tuo profilo di istanza necessita di questa policy solo se utilizzi servizi come Amazon EventBridge o CloudWatch Logs.

 Note

L'utilizzo CloudWatch EventBridge delle funzionalità è facoltativo, ma se hai deciso di utilizzarle, ti consigliamo di configurarle all'inizio del processo di configurazione di Systems Manager. Per ulteriori informazioni, consulta la [Amazon EventBridge User Guide](#) e la [Amazon CloudWatch Logs User Guide](#).

3. Modificare il ruolo IAM associato al nodo e aggiungere la policy seguente. Questa policy fornisce al nodo le autorizzazioni per chiamare `kms:Decrypt` e l'API `ssm:CreateDocument`.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "kms:Decrypt",
 "ssm:CreateDocument"
],
 "Resource": [
 "arn:aws:kms:us-east-1:111122223333:key/kms-key-id"
]
 }
]
}
```

4. Copiare e incollare il seguente elemento json di testo in un editor di testo e salvare il file come `JoinInstanceToDomain.json` nella seguente posizione: `c:\temp\JoinInstanceToDomain.json`.

```
{
 "schemaVersion": "2.2",
 "description": "Run a PowerShell script to securely join a Windows Server instance to a domain",
 "mainSteps": [
 {
 "action": "aws:runPowerShellScript",
 "name": "runPowerShellWithSecureString",
```

```

 "precondition": {
 "StringEquals": [
 "platformType",
 "Windows"
]
 },
 "inputs": {
 "runCommand": [
 "$domain = (Get-SSMParameterValue -Name
domainName).Parameters[0].Value",
 "if ((gwmi Win32_ComputerSystem).domain -eq $domain){write-host
\"Computer is part of $domain, exiting\"; exit 0}",
 "$username = (Get-SSMParameterValue -Name
domainJoinUserName).Parameters[0].Value",
 "$password = (Get-SSMParameterValue -Name domainJoinPassword -
WithDecryption $True).Parameters[0].Value | ConvertTo-SecureString -asPlainText -
Force",
 "$credential = New-Object
System.Management.Automation.PSCredential($username,$password)",
 "Add-Computer -DomainName $domain -Credential $credential -
ErrorAction SilentlyContinue -ErrorVariable domainjoinerror",
 "if($?){Write-Host \"Instance joined to domain successfully.
Restarting\"; exit 3010}else{Write-Host \"Instance failed to join domain with
error:\" $domainjoinerror; exit 1 }"
]
 }
]
}

```

5. Esegui il seguente comando in Tools for Windows PowerShell per creare un nuovo documento SSM.

```

$json = Get-Content C:\temp\JoinInstanceToDomain | Out-String
New-SSMDocument -Name JoinInstanceToDomain -Content $json -DocumentType Command

```

6. Esegui il comando seguente in Strumenti per Windows PowerShell per unire il nodo al dominio.

```

Send-SSMCommand -InstanceId instance-id -DocumentName JoinInstanceToDomain

```

Se il comando viene eseguito correttamente, il sistema restituisce informazioni simili alle seguenti.



```
WARNING: The changes will take effect after you restart the computer EC2ABCD-EXAMPLE.
```

```
Domain join succeeded, restarting
Computer is part of example.local, exiting
```

Se il comando non viene eseguito correttamente, il sistema restituisce informazioni simili alle seguenti.

```
Failed to join domain with error:
Computer 'EC2ABCD-EXAMPLE' failed to join domain 'example.local'
from its current workgroup 'WORKGROUP' with following error message:
The specified domain either does not exist or could not be contacted.
```

## Verifica e registrazione dell'attività Parameter Store

AWS CloudTrail acquisisce le chiamate API effettuate nella AWS Systems Manager console, AWS Command Line Interface (AWS CLI) e nell'SDK Systems Manager. Puoi visualizzare le informazioni nella CloudTrail console o in un bucket Amazon Simple Storage Service (Amazon S3). Tutti i CloudTrail log del tuo account utilizzano un bucket. Per ulteriori informazioni sulla visualizzazione e l'utilizzo dei CloudTrail registri delle attività di Systems Manager, vedere [Registrazione dei log AWS Systems Manager Chiamate API con AWS CloudTrail](#). Per ulteriori informazioni sulle opzioni di verifica e registrazione per Systems Manager, consulta [Registrazione e monitoraggio AWS Systems Manager](#).

## Risoluzione dei problemi Parameter Store

Utilizza le informazioni seguenti per risolvere i problemi relativi al Parameter Store.

### Risoluzione dei problemi di throughput

Utilizza le seguenti informazioni per risolvere i problemi di throughput in. Parameter Store Per informazioni sulle quote di throughput e sui motivi per cui si verifica la limitazione, consulta [Ottimizzazione della produttività in Parameter Store](#)

### Ricevute o errori dell'applicazione **ThrottlingException RateExceeded**

Problema: i log o CloudWatch i log dell'applicazione mostrano un errore come il seguente durante la chiamata `GetParameter`, `GetParameters`, oppure `GetParametersByPath`:

An error occurred (ThrottlingException) when calling the GetParameters operation (reached max retries: 4): Rate exceeded

- Soluzione: questo errore indica che la frequenza combinata delle chiamate per queste azioni API ha superato la quota di throughput dell'account corrente. Regione AWS Esegui una o più delle seguenti azioni:
- Riduci la frequenza delle chiamate dell'applicazioneParameter Store. Memorizza nella cache i valori dei parametri nell'applicazione anziché recuperarli a ogni chiamata o richiesta.

Per ulteriori informazioni, consulta [Parameters and Secrets Lambda Extension e Utilizzo dell'estensione Parameter and Secrets Lambda per memorizzare nella cache AWS parametri e segreti.](#)

- GetParametersConsente di recuperare più nomi di parametri noti in una singola chiamata, anziché GetParameter effettuare chiamate separate o una chiamata. GetParametersByPath
- Stagger legge quando molte istanze, contenitori o funzioni vengono avviate contemporaneamente, ad esempio durante una distribuzione o un evento di scalabilità.
- Se l'applicazione utilizza modelli di richiesta efficienti e continua a generare errori di limitazione, abilita un throughput più elevato per il tuo account e. Regione AWS Puoi abilitare e disabilitare un throughput più elevato in qualsiasi momento. Il costo è determinato dall'utilizzo. Per ulteriori informazioni, consulta [Prezzi di AWS Systems Manager per Parameter Store.](#)

La limitazione si verifica solo sulle chiamate **DescribeParameters**

Problema: la tua applicazione riceve un ThrottlingException errore durante DescribeParameters le chiamate, anche se le tue GetParameterGetParameters, e GetParametersByPath le chiamate non superano la quota.

- Soluzione: DescribeParameters ha un limite di throughput separato rispetto alle altre azioni di recupero dei parametri: 3 TPS per impostazione predefinita o 10 TPS con un throughput più elevato abilitato. Effettuare meno GetParameter GetParametersByPath chiamate o effettuare meno chiamate non GetParameters influisce su questo limite.

Una causa comune è la chiamata DescribeParameters con un filtro su un account con un numero elevato di parametri. L'API esamina tutti i parametri dell'account prima di applicare il filtro. Gli account con molti parametri possono superare la DescribeParameters quota anche quando il set di risultati filtrato è piccolo.

Ove possibile, utilizzalo `GetParametersByPath` in base a una gerarchia specifica anziché `DescribeParameters` con un filtro. Puoi anche ridurre la frequenza delle `DescribeParameters` chiamate negli script e nelle automazioni eseguiti in base a una pianificazione.

Nessun errore di limitazione, ma la latenza aumenta durante le distribuzioni

Problema: non viene visualizzato alcun `ThrottlingException` errore nei log, ma l'applicazione presenta una latenza elevata o errori intermittenti durante le distribuzioni, i riavvii o gli eventi di scalabilità.

- Soluzione: se l'applicazione o l'SDK riprova automaticamente le richieste limitate, un nuovo tentativo può avere esito positivo senza che si verifichi un errore di limitazione. Se la latenza aumenta, controlla il numero di tentativi nei log o nelle metriche del tuo SDK. Un numero di tentativi diverso da zero nelle Parameter Store chiamate durante questi eventi indica che ti stai avvicinando alla tua quota di throughput, anche senza che si verifichi un errore. Applica le stesse tecniche di ottimizzazione descritte in [Ottimizzazione della produttività in Parameter Store](#) per ridurre i tentativi prima che si trasformino in errori.

Risoluzione dei problemi relativi alla creazione dei parametri `aws:ec2:image`

Utilizzare le seguenti informazioni per risolvere i problemi relativi alla creazione di parametri del tipo di dati `aws:ec2:image`.

Nessuna autorizzazione a creare un'istanza

Problema: si tenta di creare un'istanza utilizzando un parametro `aws:ec2:image` ma viene visualizzato un messaggio di errore del tipo “Non si è autorizzati a eseguire questa operazione”.

- Soluzione: non disponi di tutte le autorizzazioni necessarie per creare un'istanza EC2 utilizzando un valore di parametro, come quelle per `ec2:RunInstances`, `ec2:DescribeImages` e `ssm:GetParameter`, tra gli altri. Contatta un utente IAM con autorizzazioni di amministratore all'interno dell'organizzazione per richiedere le autorizzazioni necessarie.

EventBridge riporta il messaggio di errore «Impossibile descrivere la risorsa»

Problema: è stato eseguito un comando per creare un parametro `aws:ec2:image`, ma la creazione dei parametri non è riuscita. Ricevi una notifica da Amazon EventBridge che riporta l'eccezione «Impossibile descrivere la risorsa».

Soluzione: questo messaggio può indicare quanto segue:

- Non disponi di tutte le autorizzazioni necessarie per l'operazione API `ec2:DescribeImages` oppure non disponi dell'autorizzazione per accedere all'immagine specifica a cui si fa riferimento nel parametro. Contatta un utente IAM con autorizzazioni di amministratore all'interno dell'organizzazione per richiedere le autorizzazioni necessarie.
- L'ID Amazon Machine Image (AMI) immesso come valore di parametro non è valido. Assicurati di inserire l'ID di un AMI utente disponibile nell'account corrente Regione AWS e in cui lavori.

Il nuovo **parametro `aws:ec2:image`** non è disponibile

Problema: hai appena eseguito un comando per creare un parametro `aws:ec2:image` ed è stato indicato un numero di versione, ma il parametro non è disponibile.

- Soluzione: quando si esegue il comando per creare un parametro che utilizza il tipo di dati `aws:ec2:image`, viene generato immediatamente un numero di versione per il parametro, ma il formato del parametro deve essere convalidato prima che il parametro sia disponibile. Questo processo può richiedere alcuni minuti. Per monitorare il processo di creazione e la convalida dei parametri, è possibile effettuare le seguenti operazioni:
  - EventBridge Usalo per inviarti notifiche sulle tue operazioni e sui parametri create. update e Queste notifiche segnalano se un'operazione con parametro ha avuto esito positivo o meno. Per informazioni sulla sottoscrizione agli Parameter Store eventi in EventBridge, consulta [Impostazione delle notifiche o delle azioni di attivazione basate su Parameter Store eventi](#).
  - Nella sezione Parameter Store della console Systems Manager aggiornare periodicamente l'elenco dei parametri per ricercare i dettagli dei parametri nuovi o aggiornati.
  - Utilizzare il comando `GetParameter` per verificare il parametro nuovo o aggiornato. Ad esempio, utilizzando l' AWS Command Line Interface (AWS CLI):

```
aws ssm get-parameter name MyParameter
```

Per un nuovo parametro, viene restituito un messaggio `ParameterNotFound` fino a quando il parametro non viene convalidato. Per un parametro esistente che si sta aggiornando, le informazioni sulla nuova versione non vengono incluse fino a quando il parametro non viene convalidato.

Se si tenta di creare o aggiornare nuovamente il parametro prima del completamento del processo di convalida, il sistema segnala che la convalida è ancora in corso. Se il parametro non viene creato o aggiornato, è possibile riprovare dopo 5 minuti dal primo tentativo.

## Riferimento Parameter Store

Un parametro è qualsiasi dato memorizzato in Parameter Store, ad esempio un blocco di testo, un elenco di nomi, un AMI ID, un ID commerciante o un altro valore di configurazione. Puoi fare riferimento centralmente a questi dati nei tuoi script, comandi e documenti SSM.

Quando si fa riferimento a un parametro, si specifica il nome del parametro utilizzando la seguente convenzione.

`{{ssm:parameter-name}}`

### Note

I parametri non possono essere referenziati o nidificati nei valori di altri parametri. Non è possibile includere `{{}}` o `{{ssm:parameter-name}}` in un valore di parametro.

Parameter Store fornisce il supporto per tre tipi di parametri. `String`, `StringList` e `SecureString`.

Con un'eccezione, quando si crea o si aggiorna un parametro, si immette il valore del parametro come testo normale e Parameter Store non esegue alcuna convalida sul testo immesso. Per i parametri `String`, tuttavia, è possibile specificare il tipo di dati come `aws:ec2:image` e Parameter Store convalida che il valore immesso sia nel formato corretto per un'AMI Amazon EC2, ad esempio: `ami-12345abcdeEXAMPLE`.

Tipo di parametro: `String`

Per impostazione predefinita, il valore di un parametro `String` consiste in qualsiasi blocco di testo immesso. Ad esempio:

- abc123
- Example Corp
- ``

Tipo di parametro: `StringList`

I valori dei parametri `StringList` contengono un elenco di valori separati da virgole, come illustrato nell'esempio seguente.

Monday,Wednesday,Friday

CSV,TSV,CLF,ELF,JSON

Tipo di parametro: `SecureString`

Da utilizzare `SecureString` per valori di configurazione che richiedono la crittografia, ad esempio endpoint di servizio e identificatori di account. Per informazioni segrete, come credenziali di database, chiavi API o token, consigliamo di utilizzare questa soluzione che fornisce controlli di sicurezza appositamente progettati AWS Secrets Manager, tra cui la rotazione automatica e la replica tra regioni.

Solo il valore del parametro è crittografato. Il nome, la descrizione e gli altri metadati del parametro non sono crittografati.

Parameter Store crittografa e decrittografa i `SecureString` valori dei parametri utilizzando una chiave. AWS KMS È possibile utilizzare la chiave predefinita Parameter Store o una Chiave gestita da AWS chiave gestita dal cliente. Utilizza una chiave gestita dal cliente quando devi limitare i principali che possono decrittografare determinati parametri. Per ulteriori informazioni, consulta [Crittografia e decrittografia dei parametri utilizzando AWS KMS keys](#).

#### Important

Prendi nota delle seguenti informazioni importanti.

- Se gestisci credenziali che richiedono la rotazione automatica, l'accesso tra più account o una registrazione di controllo dettagliata, ti consigliamo di utilizzarle. [AWS Secrets Manager](#) Secrets Manager è stato creato appositamente per la gestione di informazioni segrete quali credenziali di database, chiavi API e informazioni segrete supportate da software di terze parti. Per ulteriori informazioni, vedi Che cos'è? [AWS Secrets Manager](#) nella Guida AWS Secrets Manager per l'utente.

- Non memorizzare dati sensibili in un parametro `String` o `StringList`. Per tutti i dati sensibili che devono rimanere crittografati, utilizzare solo il tipo di parametro `SecureString`.
- Solo il valore di un parametro `SecureString` viene crittografato. I nomi dei parametri, le descrizioni e altre proprietà non sono crittografati.

È possibile utilizzare `SecureString` i parametri con altri Servizi AWS. La seguente funzione Lambda recupera un ID venditore crittografato dal parametro. `/myapp/dev/vendor/merchant-id`. La funzione utilizza il valore senza scriverlo nei log delle funzioni o restituirlo nella risposta.

```
import json
import boto3

ssm = boto3.client("ssm", region_name="us-east-1")

def lambda_handler(event, context):
 response = ssm.get_parameter(
 Name="/myapp/dev/vendor/merchant-id",
 WithDecryption=True
)

 merchant_id = response["Parameter"]["Value"]

 # Use merchant_id when communicating with the vendor system.
 # Don't write the value to logs or include it in the response.

 return {
 "statusCode": 200,
 "body": json.dumps("Vendor configuration retrieved.")
 }
```

## AWS KMS crittografia e determinazione dei prezzi

Quando si crea un `SecureString` parametro, Systems Manager utilizza AWS KMS per crittografare il valore del parametro.

### Important

Parameter Store supporta solo [Chiavi KMS simmetriche](#). Non è possibile utilizzare una [chiave KMS asimmetrica](#) per crittografare i parametri. Per informazioni su come determinare se una

chiave KMS è simmetrica o asimmetrica, consulta [Identificazione di chiavi KMS simmetriche e asimmetriche](#) nella Guida per gli sviluppatori di AWS Key Management Service

La creazione di Parameter Store un SecureString parametro è gratuita, ma AWS KMS possono essere applicati costi di utilizzo. Per ulteriori informazioni, consulta [Prezzi di AWS Key Management Service](#).

Per ulteriori informazioni sulle chiavi gestite dal cliente Chiavi gestite da AWS e sulle chiavi gestite dal cliente, consulta [AWS Key Management Service Concepts](#) nella AWS Key Management Service Developer Guide. Per ulteriori informazioni sulle modalità di Parameter Store utilizzo AWS KMS, consulta [Modalità di AWS Systems ManagerParameter Store utilizzo AWS KMS](#).

#### Note

Per visualizzare l'impostazione predefinita Chiave gestita da AWS perParameter Store, esegui il comando seguente.

```
aws kms describe-key \
 --region us-east-1 \
 --key-id alias/aws/ssm
```

## Vincoli relativi ai nomi dei parametri

Utilizza le informazioni riportate in questo argomento per specificare valori validi per i nomi di parametro durante il processo di creazione di un parametro.

Queste informazioni integrano i dettagli dell'argomento [PutParameter](#) dell'AWS Systems Manager API Reference, che fornisce anche informazioni sui valori AllowedPattern, sulla descrizione, sulla sovrascrittura KeyId, sul tipo e sul valore.

I requisiti e i vincoli relativi ai nomi di parametro sono descritti di seguito:

- Distinzione tra lettere maiuscole e minuscole: i nomi di parametro fanno distinzione tra maiuscole e minuscole.
- Spazi: i nomi di parametro non possono contenere spazi.
- Caratteri validi: i nomi di parametro possono contenere solo i seguenti simboli e lettere: a-zA-Z0-9\_.-



Inoltre, il carattere barra (/) viene utilizzato per delineare le gerarchie nei nomi dei parametri. Ad esempio, `/Dev/Production/East/Project-ABC/MyParameter`

- **Formato AMI valido:** quando si sceglie `aws:ec2:image` come tipo di dati per un parametro `String`, l'ID immesso deve essere convalidato per il formato ID AMI `ami-12345abcdeEXAMPLE`.
- **Pienamente qualificato:** quando si crea o si fa riferimento a un parametro in una gerarchia, è necessario includere una barra iniziale (/). Quando si fa riferimento a un parametro che fa parte di una gerarchia, è necessario specificare l'intero percorso della gerarchia, inclusa la barra iniziale (/).
  - **Nomi di parametri completi:** `MyParameter1`, `/MyParameter2`, `/Dev/Production/East/Project-ABC/MyParameter`
  - **Nome del parametro non completo:** `MyParameter3/L1`
- **Lunghezza:** la lunghezza massima per il nome del parametro creato è 1.011 caratteri. Questa somma di 1.011 caratteri include i caratteri nell'ARN che precedono il nome specificato, ad esempio i 45 caratteri in `arn:aws:ssm:us-east-2:111122223333:parameter/`.
- **Prefissi:** un nome di parametro non può essere associato al prefisso "aws" o "ssm" (non prevede distinzione tra lettere maiuscole e minuscole). Ad esempio, il tentativo di creare parametri con i seguenti nomi ha esito negativo con un'eccezione:
  - `awsTestParameter`
  - `SSM-testparameter`
  - `/aws/testparam1`

#### Note

Quando specifichi un parametro in un documento SSM, un comando o uno script, includi `ssm` come parte della sintassi. Ad esempio, `{{ssm:parameter-name}}` e `{{ssm:parameter-name}}`, come, e `{{ssm:MyParameter}}` `{{ ssm:MyParameter }}`.

- **Unicità:** un nome di parametro deve essere univoco all'interno di una Regione AWS. Ad esempio, Systems Manager considera i seguenti elementi come parametri distinti, se presenti nella stessa regione:
  - `/Test/TestParam1`
  - `/TestParam1`

I seguenti esempi sono tutti elementi univoci:

- /Test/TestParam1/Logpath1
- /Test/TestParam1

I seguenti esempi, tuttavia, se presenti nella stessa regione, non sono elementi univoci:

- /TestParam1
- TestParam1
- Profondità della gerarchia: se specifichi una gerarchia di parametri, tale gerarchia può avere un massimo di quindici livelli. È possibile definire un parametro a qualsiasi livello della gerarchia. Entrambi gli esempi seguenti sono strutturalmente validi:
  - /Level-1/L2/L3/L4/L5/L6/L7/L8/L9/L10/L11/L12/L13/L14/parameter-name
  - parameter-name

Il tentativo di creare il parametro seguente avrà esito negativo e restituirà un'eccezione `HierarchyLevelLimitExceededException`:

- /Level-1/L2/L3/L4/L5/L6/L7/L8/L9/L10/L11/L12/L13/L14/L15/L16/parameter-name

#### Important

Parameter Store autorizza l'operazione `GetParametersByPath` in base al percorso specificato nella richiesta, non in base a ciascun parametro restituito dall'operazione. Un principale a cui è consentito richiamare `GetParametersByPath` il percorso `/a` riceve tutti i parametri inclusi in quel percorso, inclusi `/a/b`. Ciò è vero anche se la stessa politica nega esplicitamente l'accesso `/a/b` ad altre azioni.

Per impedire la restituzione di un parametro `GetParametersByPath`, negare l'azione `ssm:GetParametersByPath` su ogni percorso predecessore che potrebbe includere il parametro nei risultati. Ad esempio, per `/a/b` evitare che venga restituito, nega sia `ssm:GetParametersByPath` per `/a` che `/a/b`.

Per indicazioni sulla stesura di policy IAM che tengano conto di questo comportamento, consulta [Limitazione dell'accesso a parametri e percorsi specifici](#).

# AWS Systems Manager strumenti operativi

Gli strumenti operativi sono una serie di funzionalità che consentono di gestire al meglio le risorse AWS .

- I [CloudWatch dashboard Amazon ospitati da Systems Manager](#) sono home page personalizzabili nella CloudWatch console che puoi utilizzare per monitorare le tue risorse Regioni AWS in un'unica visualizzazione.
- [Explorer](#) è una dashboard operativa personalizzabile che riporta informazioni sulle tue AWS risorse. Explorer mostra una visualizzazione aggregata dei dati operativi (OpsData) per te Account AWS e per tutti Regioni AWS.
- [Incident Manager](#) consente di mitigare e ripristinare gli incidenti che interessano le applicazioni ospitate su. AWS
- [OpsCenter](#) fornisce una posizione centrale in cui gli ingegneri operativi e i professionisti IT possono visualizzare, esaminare e risolvere gli elementi di lavoro operativi (OpsItems) relativi alle AWS risorse.

## Argomenti

- [Strumento di gestione degli incidenti AWS Systems Manager](#)
- [AWS Systems Manager Explorer](#)
- [AWS Systems Manager OpsCenter](#)
- [Utilizzo delle CloudWatch dashboard Amazon ospitate da Systems Manager](#)

## Strumento di gestione degli incidenti AWS Systems Manager

### Modifica della disponibilità di Incident Manager

Strumento di gestione degli incidenti AWS Systems Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzare Incident Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [Strumento di gestione degli incidenti AWS Systems Manager la modifica della disponibilità](#).

Usa Incident Manager per gestire gli incidenti che si verificano nelle tue applicazioni AWS ospitate. Incident Manager combina il coinvolgimento degli utenti, l'escalation, i runbook, i piani di risposta, i canali di chat e l'analisi post-incidente. Queste funzionalità aiutano il team a valutare più rapidamente gli incidenti e a riportare le applicazioni alla normalità. Per ulteriori informazioni sullo Strumento di gestione degli incidenti, consultare la [Guida utente dello Strumento di gestione degli incidenti](#).

## AWS Systems Manager Explorer

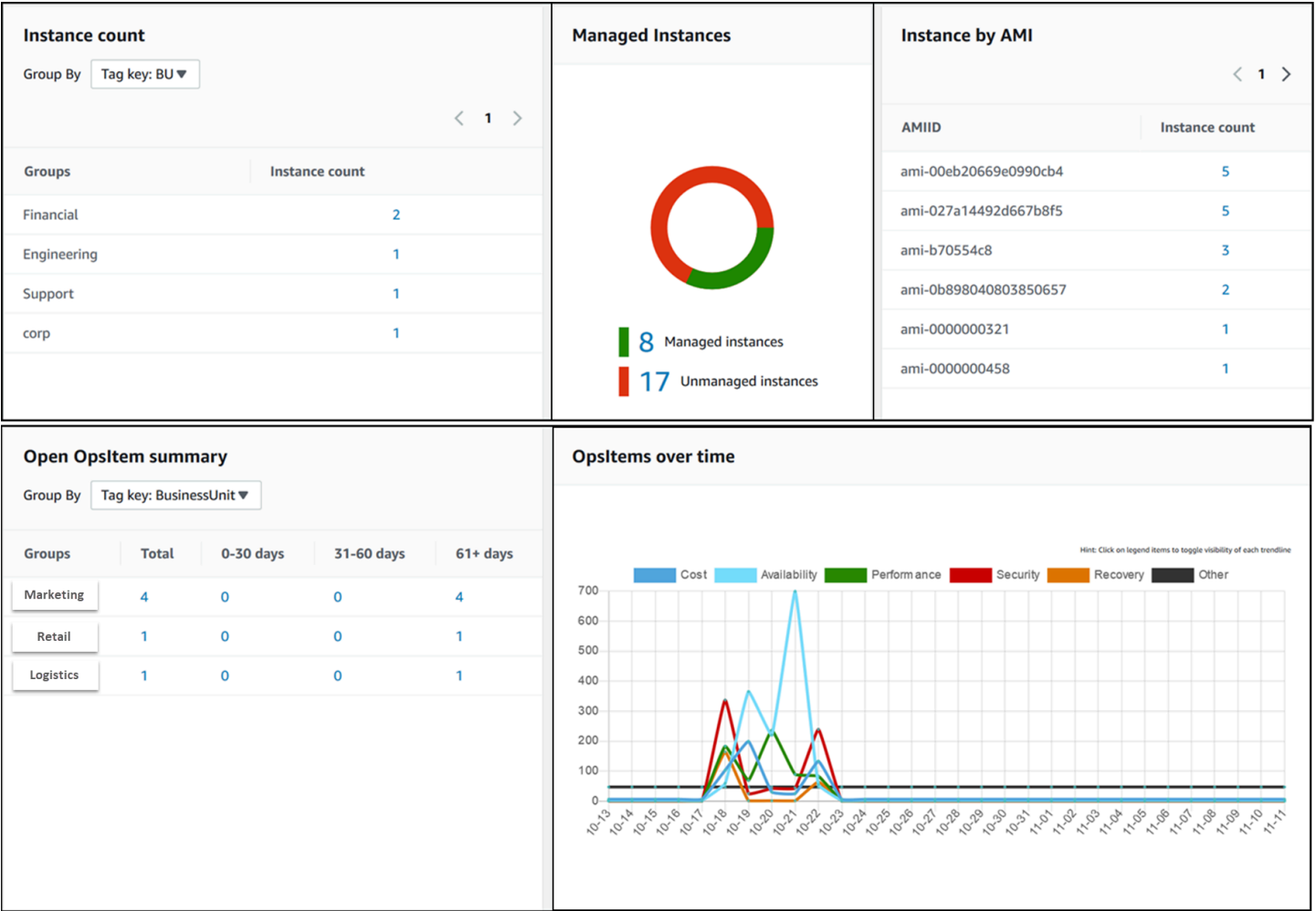
 Il Explorer la pagina sarà obsoleta il 31 dicembre 2026.

Man mano che semplifichiamo l'esperienza della console di Systems Manager, Resource Data Sync passerà a. OpsCenter Tutti i tuoi dati operativi rimangono disponibili tramite API e visualizzabili nelle relative console AWS di servizio. [Ulteriori informazioni](#)

AWS Systems Manager Explorer è una dashboard operativa personalizzabile che riporta informazioni sulle tue AWS risorse. Explorer mostra una vista aggregata dei dati operativi (OpsData) per te Account AWS e per tutti Regioni AWS. In Explorer, OpsData include i metadati sui nodi gestiti nell'ambiente [ibrido e multicloud](#). OpsData include anche le informazioni fornite da altri strumenti di Systems Manager, inclusi i dettagli Patch Manager sulla conformità delle patch e State Manager sulle associazioni. Per semplificare ulteriormente le modalità di accesso OpsData, Explorer visualizza informazioni provenienti da AWS servizi di supporto come AWS Config AWS Trusted Advisor, AWS Compute Optimizer, e Supporto AWS (casi di supporto).

Per aumentare la consapevolezza operativa, Explorer visualizza anche gli elementi di lavoro operativi (OpsItems). Explorer fornisce un contesto su come gli OpsItems vengono distribuiti tra le business unit o le applicazioni, quali sono le tendenze nel tempo e come variano in base alla categoria. È possibile raggruppare e filtrare le informazioni Explorer per concentrarti sugli elementi rilevanti e per cui è necessario prendere misure. Quando si identificano problemi con priorità elevata, è possibile utilizzare OpsCenter di Systems Manager per eseguire runbook Automation e risolvere rapidamente tali problemi. Per iniziare a utilizzare Explorer, apri la [console di Systems Manager](#). Nel pannello di navigazione, scegli Explorer.

L'immagine seguente mostra alcune delle singole caselle di report, chiamate widget, che sono disponibili in Explorer.



Quali sono le caratteristiche di Explorer?

Explorer ha le funzionalità seguenti:

- Visualizzazione personalizzabile di informazioni utilizzabili: Explorer include widget drag-and-drop che visualizzano automaticamente informazioni utilizzabili sulle tue risorse. AWS Explorer visualizza le informazioni in due tipi di widget.
- Widget informativi: questi widget riassumono i dati provenienti da Amazon EC2,, e supportano, ad Servizi AWS esempio Patch Manager State Manager AWS Trusted Advisor, Compute Optimizer e. AWS Supporto Questi widget forniscono un contesto importante per aiutarti a comprendere lo stato e i rischi operativi delle tue risorse. AWS Esempi di widget informativi includono Conteggio istanze, Istanza per AMI, Totale nodi non conformi (applicazione di patch), Associazioni non conformi e Casi del centro di assistenza.
- OpsItemwidget: un Systems Manager OpsItem è un elemento di lavoro operativo correlato a una o più AWS risorse. OpsItemssono una funzionalità di Systems ManagerOpsCenter.

OpsItems potrebbero richiedere DevOps agli ingegneri di indagare e potenzialmente risolvere un problema. Esempi di possibili OpsItems includono utilizzo elevato della CPU da parte dell'istanza EC2, volumi scollegati Amazon Elastic Block Store (Amazon EBS), errore di distribuzione AWS CodeDeploy o errore di esecuzione di Systems Manager Automation. Esempi di widget OpsItem includono il riepilogo Open (Apertura)OpsItem,OpsItem per stato , e OpsItems nel corso del tempo.

- Filtri: ogni widget offre la possibilità di filtrare le informazioni in base a Account AWS Regione AWS, e tag. I filtri consentono di perfezionare rapidamente le informazioni visualizzate in Explorer.
- Collegamenti diretti alle schermate di servizio: per aiutarti a risolvere i problemi relativi alle AWS risorse, i Explorer widget contengono collegamenti diretti alle schermate di servizio correlate. I filtri applicati a un widget rimangono attivi se si passa a una schermata di servizio correlata.
- Gruppi: per comprendere i tipi di problemi operativi nell'organizzazione, alcuni widget consentono di raggruppare i dati in base a account, regione e tag.
- Segnalazione chiavi tag: quando si imposta Explorer, è possibile specificare fino a cinque chiavi tag. Queste chiavi consentono di raggruppare e filtrare i dati in Explorer. Se una chiave specificata corrisponde a una chiave su una risorsa che genera un OpsItem, la chiave e il valore sono inclusi negli OpsItems.
- Tre modalità di Regione AWS visualizzazione Account AWS e visualizzazione: Explorer include le seguenti modalità di visualizzazione per OpsData e OpsItems in entrata Account AWS e Regioni AWS:
  - Single-account/single-Region: Questa è la visualizzazione predefinita. Questa modalità consente agli utenti di visualizzare i dati e OpsItems dal proprio account e dalla regione corrente.
  - Single-account/multiple-Region: questa modalità richiede la creazione di una o più sincronizzazioni dei dati delle risorse utilizzando la pagina Explorer Impostazioni. Una sincronizzazione dei dati delle risorse si aggrega OpsData da una o più regioni. Dopo aver creato una sincronizzazione dei dati delle risorse, è possibile attivare la sincronizzazione da utilizzare nel dashboard Explorer. È quindi possibile filtrare e raggruppare i dati in base alla regione.
  - Multiple-account/multiple-Region: questa modalità richiede che l'organizzazione o l'azienda utilizzi tutte [AWS Organizations](#) le funzionalità attivate. Dopo aver effettuato la configurazione AWS Organizations nell'ambiente informatico, è possibile aggregare tutti i dati dell'account in un account di gestione. È quindi possibile creare sincronizzazioni dei dati delle risorse in modo da poter filtrare e raggruppare i dati in base all'area geografica. Per ulteriori informazioni sulla modalità Organizations Tutte le caratteristiche, consulta [Abilitazione di tutte le caratteristiche nell'organizzazione](#).

- Creazione di report: è possibile esportare Explorer report come file con valore separato da virgole (csv) in un bucket Amazon Simple Storage Service (Amazon S3). Quando un'esportazione è completata, riceverai un avviso da Amazon Simple Notification Service (Amazon SNS).

## Come fa Explorer si riferiscono a OpsCenter?

[Systems Manager OpsCenter](#) offre una posizione centrale in cui gli ingegneri operativi e i professionisti IT visualizzano, esaminano e risolvono le OpsItems questioni relative alle AWS risorse. Explorer è un hub di report in cui DevOps i manager visualizzano i riepiloghi aggregati dei dati operativi OpsItems, compresi quelli relativi agli account Regioni AWS. Explorer aiuta gli utenti a scoprire tendenze e modelli e, se necessario, a risolvere rapidamente i problemi utilizzando i runbook di Systems Manager Automation.

La configurazione Explorer è ora integrata con quella di OpsCenter. Se è già impostato OpsCenter, Explorer visualizza automaticamente i dati delle operazioni, comprese le informazioni aggregate su OpsItems. Se non hai configurato OpsCenter, è possibile utilizzare la configurazione di Explorer per iniziare a utilizzare entrambi gli strumenti. Per ulteriori informazioni, consulta [Nozioni di base su Systems Manager Explorer e OpsCenter](#).

## Che cos'è OpsData?

OpsData sono i dati operativi visualizzati nella dashboard di Systems Manager Explorer. Explorer OpsData recupera dalle seguenti fonti:

- Amazon Elastic Compute Cloud (Amazon EC2)

I dati visualizzati in Explorer includono: numero totale di nodi, numero totale di nodi gestiti e non gestiti e un numero di nodi che utilizzano una specifica Amazon Machine Image (AMI).

- Systems Manager OpsCenter

I dati visualizzati in Explorer includono: un conteggio di OpsItems per stato, un conteggio di OpsItems per gravità, un conteggio di OpsItems aperti tra gruppi e in periodi di tempo di 30 giorni e dati cronologici OpsItems nel tempo.

- Systems Manager Patch Manager

I dati visualizzati in Explorer includono un conteggio dei nodi non conformi e dei nodi critici non conformi.

- AWS Trusted Advisor

I dati visualizzati in Explorer includono: controllo dello stato delle best practice per le istanze riservate EC2 nelle aree di ottimizzazione dei costi, sicurezza, tolleranza ai guasti, prestazioni e limiti di servizio.

- AWS Compute Optimizer

I dati visualizzati in Explorer includono: un conteggio delle istanze EC2 sottoposte a provisioning e a overprovisioning, esiti dell'ottimizzazione, dettagli sui prezzi su richiesta e suggerimenti per il tipo e il prezzo dell'istanza.

- Supporto Centra i casi

I dati visualizzati in Explorer includono: ID caso, gravità, stato, ora di creazione, oggetto, servizio e categoria.

- AWS Config

I dati visualizzati Explorer includono: un riepilogo generale delle AWS Config regole conformi e non conformi, il numero di risorse conformi e non conformi e dettagli specifici su ciascuna di esse (se si approfondisce una regola o una risorsa non conforme).

- AWS Security Hub CSPM

I dati visualizzati in Explorer includono: riepilogo generale dei risultati del CSPM di Security Hub, il numero di ciascun risultato raggruppato per gravità e dettagli specifici sui risultati.

#### Note

Per visualizzare AWS Trusted Advisor e Supporto archiviare i casi Explorer, è necessario disporre di un account Enterprise o Business configurato con. Supporto AWS

Puoi visualizzare e gestire le OpsData fonti dalla pagina Explorer Impostazioni. Per informazioni sull'impostazione e la configurazione dei servizi che popolano i Explorer widget con OpsData, consulta. [Impostazione di servizi correlati per Explorer](#)

## L'utilizzo è a pagamento Explorer?

Sì. Quando si attivano le regole predefinite per la creazione di OpsItems durante l'installazione integrata, si avvia un processo che crea automaticamente OpsItems. L'addebito sull'account viene effettuato in base al numero di OpsItems creato al mese. L'addebito sull'account viene effettuato



anche in base al numero di chiamate API `GetOpsItem`, `DescribeOpsItem`, `UpdateOpsItem` e `GetOpsSummary` al mese. Inoltre, è possibile addebitare l'addebito per le chiamate API pubbliche ad altri servizi che espongono informazioni diagnostiche pertinenti. Per ulteriori informazioni, consulta [AWS Systems Manager Prezzi](#).

## Modifiche a AWS Systems Manager Explorer

Il luogo in cui visualizzi i dati operativi (OpsData) AWS Systems Manager sta cambiando. A partire dal 31 dicembre 2026, il Explorer dashboard non fa più parte della console di Systems Manager. Si continua a visualizzare lo stesso OpsData nella console Servizio AWS o nello strumento Systems Manager che lo produce.

Cambia solo il pannello di controllo. Nessuno dei tuoi dati OpsData viene eliminato e il modo in cui Systems Manager li raccoglie rimane invariato. Explorervisualizza i dati che gli strumenti di Systems Manager e altri Servizi AWS raccolgono e archiviano, in modo che i dati rimangano dove si trovano oggi. Le sincronizzazioni dei dati delle risorse continuano ad essere aggregate all' OpsData interno dell' Account AWS azienda e Regioni AWS ogni operazione dell'API di Systems Manager che Explorer utilizza, inclusa`GetOpsSummary`, continua a essere supportata negli SDK AWS CLI e negli AWS SDK.

Utilizza le seguenti sezioni per scoprire dove è disponibile ciascuna delle tue Explorer visualizzazioni e per esaminare le risposte alle domande più frequenti su questa modifica.

Dove trovare ognuno dei tuoi Explorer viste

Explorerdispone di diversi widget che forniscono dati operativi. La tabella seguente mostra dove sono disponibili i dati di ciascun widget. Alcune alternative richiedono una configurazione prima di visualizzare i dati per più Account AWS e Regioni AWS.

| Explorerwidget o visualizz azione                   | Dove trovare questi dati                                                  | Cosa occorre sapere                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Istanze gestite, numero di istanze, istanze per AMI | Console di Systems Manager, pagine Review Nodes Insights ed Explore nodes | Queste pagine aggregano i dettagli dei nodi per la tua organizzazione o il tuo account. Per ulteriori informazioni, consulta <a href="#">Esaminare approfondimenti nodo</a> e <a href="#">Esplorazione dei nodi</a> .<br><br>Queste pagine richiedono la console unificata di Systems Manager. Per |

| Explorerwidget o visualizzazione                           | Dove trovare questi dati                                                 | Cosa occorre sapere                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                            |                                                                          | saperne di più su Regioni AWS dove è disponibile la console unificata, vedi <a href="#">Supportato. Regioni AWS</a> In altre regioni, utilizza l'Fleet ManagerAPI Systems Manager per elencare i nodi gestiti.                                                                                                                                                                                                       |
| Numero totale di nodi non conformi (applicazione di patch) | Patch Managerconsole, scheda Dashboard                                   | Patch Managerpresenta questi dati in modo diverso da come Explorer li presenta. Invece della cronologia visualizzata dal Explorer widget, la scheda Dashboard mostra il numero di nodi gestiti conformi e non conformi e un rapporto sulla conformità delle patch negli ultimi 7 giorni. Per ulteriori informazioni, consulta <a href="#">Visualizzazione dei riepiloghi del pannello di controllo delle patch</a> . |
| Associazioni non conformi (conformità statale desiderata)  | Console, pagina di conformità e console di Systems Manager State Manager | Per ulteriori informazioni, consulta <a href="#">AWS Systems Manager Conformità</a> e <a href="#">AWS Systems Manager State Manager</a> . Se si utilizza Quick Setup per creare associazioni, è anche possibile rivedere lo stato di ciascuna configurazione nella Quick Setup console. Per ulteriori informazioni, consulta <a href="#">AWS Systems Manager Configurazione rapida</a> .                             |

| Explorerwidget o visualizzazione | Dove trovare questi dati      | Cosa occorre sapere                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AWS Trusted Advisor              | AWS Trusted Advisor console   | È necessario disporre di un piano di supporto aziendale o aziendale . La AWS Trusted Advisor console mostra i controlli relativi all'account corrente. Per esaminare i controlli in un'organizzazione, attiva la visualizzazione organizzativa e genera un rapporto. Per ulteriori informazioni, vedere Visualizzazione <a href="#">organizzativa per Trusted Advisor</a> .                                                                                                                   |
| AWS Config conformità            | AWS Config console            | Per verificare la conformità per più account e regioni, crea un aggregatore in AWS Config. Per ulteriori informazioni, consulta <a href="#">Creazione di un aggregatore</a> .                                                                                                                                                                                                                                                                                                                 |
| AWS Security Hub CSPM risultati  | AWS Security Hub CSPM console | Per esaminare i risultati per più account e regioni, attiva la configurazione centrale in Security Hub CSPM. Per ulteriori informazioni, consulta <a href="#">Avvio della configurazione centrale</a> .                                                                                                                                                                                                                                                                                       |
| AWS Compute Optimizer            | AWS Compute Optimizer console | Scegli il tuo account o la tua organizzazione. Compute Optimizer aggrega i risultati relativi alle risorse il cui provisioning è insufficiente ed elenca le risorse sovradimensionate per tipo di risorsa anziché in un'unica visualizzazione aggregata. Per ulteriori informazioni, consulta Attivazione dell'account. <a href="https://docs.aws.amazon.com/compute-optimizer/latest/ug/account-opt-in.html">https://docs.aws.amazon.com/compute-optimizer/latest/ug/account-opt-in.html</a> |

| Explorerwidget o visualizzazione                                                      | Dove trovare questi dati                            | Cosa occorre sapere                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Casi del Centro assistenza                                                            | Supporto AWS Centro di supporto                     | Il Centro assistenza mostra i casi attivi e la cronologia dei casi per l'account corrente. Non fornisce una visualizzazione dei casi su più account. Per crearne uno, consulta <a href="#">Creare una visione completa dei casi di AWS supporto con Amazon QuickSight</a> . |
| OpsItemRiepilogo aperto, OpsItems per stato, OpsItems per gravità, OpsItems nel tempo | Console OpsCenter                                   | La OpsCenter console fornisce informazioni sul tuoOpsItems. Per ulteriori informazioni, consulta <a href="#">AWS Systems Manager OpsCenter</a> .                                                                                                                            |
| Esporta OpsData nel bucket Amazon S3                                                  | Console di automazione di Systems Manager o AWS CLI | Explorerutilizza il AWS-ExportOpsDataToS3 runbook per l'esportazione OpsData. Puoi continuare a eseguire questo runbook direttamente dalla console di automazione o dal. AWS CLI Per ulteriori informazioni, consulta <a href="#">AWS-ExportOpsDataToS3</a> .               |

I conteggi aggregati visualizzati dai Explorer widget vengono restituiti dall'[GetOpsSummary](#) operazione API. Puoi utilizzare un GetOpsSummary AWS SDK o l' AWS CLI API di Systems Manager per creare report personalizzati, anche per gli account e le regioni coperti dalla sincronizzazione dei dati delle risorse.

È inoltre possibile creare una visualizzazione personalizzata di questi dati. Per un esempio che combini la sincronizzazione dei dati Explorer delle risorse, il AWS-ExportOpsDataToS3 runbook e la creazione Amazon Quick Sight di un grafico Supporto dei casi tra gli account di un'organizzazione, consulta [Creare una visione completa dei casi di AWS supporto con Amazon. QuickSight](#)

Le sincronizzazioni dei dati delle risorse che hai già creato continuano ad essere aggregate OpsData per i tuoi account e le tue regioni. La gestione della sincronizzazione dei dati delle risorse nella console passerà a. OpsCenter È possibile gestirli con l'API Systems Manager utilizzando le

operazioni [CreateResourceDataSync](#), [ListResourceDataSync](#), [UpdateResourceDataSync](#), e [DeleteResourceDataSync](#) API.

## Domande frequenti

Il mio viene OpsData eliminato quando Explorer viene interrotto?

No. Explorer visualizza i dati raccolti Servizi AWS e archiviati da altri strumenti e da Systems Manager. I dati rimangono in tali servizi e rimangono disponibili tramite le relative console e API.

Le operazioni API vengono rimosse?

No. Questa modifica influisce solo sull'esperienza della console. Le operazioni API Explorer utilizzate, incluse `GetOpsSummary` le operazioni di sincronizzazione dei dati delle risorse, continuano a essere disponibili.

Devo eliminare o ricreare le sincronizzazioni dei dati delle mie risorse?

No. Le sincronizzazioni dei dati delle risorse esistenti continuano a funzionare e puoi gestirle con l'API Systems Manager.

Posso ancora visualizzare i dati per più account e regioni?

Nella maggior parte dei casi sì, ma la configurazione e il livello di aggregazione dipendono dal servizio. Consulta la colonna Cosa devi sapere [Dove trovare ognuno dei tuoi Explorer viste](#) per conoscere le fonti di dati che utilizzi.

Se hai altre domande, contattaci tramite il Centro [AWS assistenza](#).

## Argomenti

- [Nozioni di base su Systems Manager Explorer e OpsCenter](#)
- [Uso di Explorer](#)
- [Esportazione OpsData da Systems Manager Explorer](#)
- [Risoluzione dei problemi di Systems Manager Explorer](#)

## Nozioni di base su Systems Manager Explorer e OpsCenter

AWS Systems Manager utilizza un'esperienza di configurazione integrata per aiutarti a iniziare a usare Systems Manager Explorer e Systems Manager OpsCenter. In questa documentazione, Explorer e il OpsCenter Setup sono chiamati Integrated Setup (Installazione integrata). Se hai già

configurato OpsCenter, è comunque necessario completare l'installazione integrata per verificare le impostazioni e le opzioni. Se non è stato configurato OpsCenter, è possibile utilizzare l'installazione integrata per iniziare a utilizzare entrambe gli strumenti.

#### Note

L'installazione integrata è disponibile solo nella console Systems Manager. Non è possibile impostare Explorer o OpsCenter a livello di programmazione.

Il programma di installazione integrato esegue i seguenti processi:

- [Configura ruoli e autorizzazioni](#): la configurazione integrata crea un ruolo AWS Identity and Access Management (IAM) che consente EventBridge ad Amazon di creare automaticamente in OpsItems base a regole predefinite. Dopo l'impostazione, è necessario configurare le autorizzazioni utente, gruppo o ruolo per OpsCenter, come descritto in questa sezione.
- [Consente la OpsItem creazione di regole predefinite](#): Integrated Setup crea regole predefinite in EventBridge. Queste regole creano automaticamente OpsItems in risposta agli eventi. Esempi di questi eventi sono: modifica dello stato di una AWS risorsa, modifica delle impostazioni di sicurezza o indisponibilità di un servizio.
- Attiva le OpsData fonti: la configurazione integrata attiva le seguenti fonti di dati che Explorer popolano i widget.
  - Supporto Center (è necessario disporre di un piano Business o Enterprise Support per attivare questa fonte).
  - AWS Compute Optimizer (È necessario disporre di un piano Business o Enterprise Support per attivare questa fonte.)
  - Conformità associazioni di State Manager in Systems Manager
  - ConformitàAWS Config
  - OpsCenter di Systems Manager
  - Conformità patch Patch Manager di Systems Manager
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - Inventario Systems Manager
  - AWS Trusted Advisor (È necessario disporre di un piano Business o Enterprise Support per attivare questa fonte.)
  - AWS Security Hub CSPM

 Note

È possibile modificare le impostazioni di configurazione in qualsiasi momento nella pagina Settings (Impostazioni).

Dopo aver completato la configurazione integrata, si consiglia di eseguire la [configurazione in Explorer modo da visualizzare i dati provenienti da più regioni e account](#). Explorer e OpsCenter si sincronizzano automaticamente OpsData e OpsItems per l'Account AWS e Regione AWS utilizzato al termine della configurazione integrata. È possibile aggregare dati OpsData OpsItems provenienti da altri account e regioni creando una sincronizzazione dei dati delle risorse.

### Impostazione di servizi correlati per Explorer

AWS Systems Manager Esplora e AWS Systems Manager OpsCenter raccoglie informazioni o interagisci con altri strumenti Servizi AWS e Systems Manager. Si consiglia di impostare e configurare questi altri servizi o strumenti prima di utilizzare il servizio Configurazione integrata.

La tabella seguente include le attività che consentono Explorer e OpsCenter consentono di raccogliere informazioni da o interagire con altri strumenti Servizi AWS e Systems Manager.

| Operazione                                                 | Informazioni                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Verificare le autorizzazioni in Systems Manager Automation | Explorer e OpsCenter consentono di risolvere i problemi con le risorse AWS utilizzando i runbook di Systems Manager Automation. Per utilizzare questo strumento di correzione, è necessario disporre delle autorizzazioni per eseguire i runbook dell'automazione Systems Manager. Per ulteriori informazioni, consulta <a href="#">Configurazione del servizio di automazione</a> . |
| Impostare e configurare Patch Manager di Systems Manager   | Explorer include un widget che fornisce informazioni sulla conformità delle patch. Per visualizzare questi dati in Explorer, è necessari o configurare l'applicazione di patch. Per ulteriori informazioni, consulta <a href="#">AWS Systems Manager Patch Manager</a> .                                                                                                             |

| Operazione                                               | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Impostare e configurare State Manager di Systems Manager | Explorer include un widget che fornisce informazioni sulla conformità delle associazioni di State Manager in Systems Manager. Per visualizzare questi dati in Explorer, è necessario configurare State Manager. Per ulteriori informazioni, consulta <a href="#">AWS Systems Manager State Manager</a> .                                                                                                                                                                                                                                                                                                                                                               |
| Attiva AWS Config Configuration Recorder                 | <p>Explorer utilizza i dati forniti dal registratore di AWS Config configurazione per popolare i widget con informazioni sulle istanze EC2. Per visualizzare questi dati, attiva il registratore di configurazione Explorer. AWS Config Per ulteriori informazioni, vedere <a href="#">Gestione del registratore di configurazione</a>.</p> <div> <b>Note</b><p>Dopo aver attivato il registratore di configurazione, Systems Manager può richiedere fino a sei ore fino alla visualizzazione dei dati nei widget Explorer che indicano le informazioni sulle istanze EC2.</p></div> |
| Accendi AWS Trusted Advisor                              | Explorer utilizza i dati forniti da Trusted Advisor per visualizzare lo stato dei controlli delle best practice per le istanze riservate Amazon EC2 nelle aree di ottimizzazione dei costi, sicurezza, tolleranza ai guasti, prestazioni e limiti di servizio. Per visualizzare questi dati in Explorer, è necessario disporre di un piano di supporto aziendale o di business. Per ulteriori informazioni, consulta <a href="#">Supporto</a> .                                                                                                                                                                                                                        |



| Operazione                    | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Attiva AWS Compute Optimizer  | Explorer utilizza i dati forniti da Compute Optimizer per visualizzare i dettagli, un conteggio delle istanze EC2 sottoposte a provisioning e a overprovisioning, esiti dell'ottimizzazione, dettagli sui prezzi su richiesta e suggerimenti per il tipo e il prezzo dell'istanza. Per visualizzare questi dati in Explorer, attiva Compute Optimizer. Per ulteriori informazioni, vedi <a href="#">Guida introduttiva AWS Compute Optimizer</a> . |
| Accendi AWS Security Hub CSPM | Explorer utilizza i dati forniti da Security Hub CSPM per popolare i widget con informazioni sui risultati di sicurezza. Per visualizzare questi dati Explorer, attiva l'integrazione CSPM di Security Hub. Per ulteriori informazioni, consulta <a href="#">Cos'è</a> . AWS Security Hub CSPM                                                                                                                                                     |

## Configurazione di ruoli e autorizzazioni per Systems Manager Explorer

Integrated Setup crea e configura automaticamente i ruoli AWS Identity and Access Management (IAM) per AWS Systems Manager Explorer e AWS Systems Manager OpsCenter. Se è stata completata l'installazione integrata, non è necessario eseguire alcun processo aggiuntivo per la configurazione di ruoli e autorizzazioni per Explorer. Tuttavia, è necessario configurare le autorizzazioni per OpsCenter, come descritto più avanti in questo argomento.

Il programma di installazione integrata crea e configura i seguenti ruoli per lavorare con Explorer e OpsCenter.

- `AWSServiceRoleForAmazonSSM`: fornisce l'accesso a risorse AWS gestite o utilizzate da Systems Manager.
- `OpsItem-CWE-Role`: consente la creazione di CloudWatch eventi e EventBridge la creazione OpsItems in risposta a eventi comuni.
- `AWSServiceRoleForAmazonSSM_AccountDiscovery`: consente a Systems Manager di chiamare altri utenti Servizi AWS per scoprire Account AWS informazioni durante la

sincronizzazione dei dati. Per ulteriori informazioni su questo ruolo, consulta [Usare i ruoli per raccogliere Account AWS informazioni per OpsCenter and Explorer](#).

- `AmazonSSMExplorerExport`: consente di Explorer OpsData esportare in un file con valori separati da virgole (CSV).

Se si configura Explorer la visualizzazione dei dati di più account e regioni utilizzando AWS Organizations una sincronizzazione dei dati delle risorse, Systems Manager crea il ruolo collegato al servizio. `AWSServiceRoleForAmazonSSM_AccountDiscovery` Systems Manager utilizza questo ruolo per ottenere informazioni sul tuo Account AWS account. AWS Organizations Il ruolo utilizza la policy di autorizzazioni riportato di seguito.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "organizations:DescribeAccount",
 "organizations:DescribeOrganization",
 "organizations:ListAccounts",
 "organizations:ListAWSServiceAccessForOrganization",
 "organizations:ListChildren",
 "organizations:ListParents"
],
 "Resource": "*"
 }
]
}
```

Per ulteriori informazioni sul ruolo `AWSServiceRoleForAmazonSSM_AccountDiscovery`, consulta [Usare i ruoli per raccogliere Account AWS informazioni per OpsCenter and Explorer](#).

Configurazione delle autorizzazioni per Systems Manager OpsCenter

Dopo aver completato la configurazione integrata, è necessario configurare le autorizzazioni utente, gruppo o ruolo in modo che gli utenti possano eseguire operazioni in OpsCenter.

## Prima di iniziare

È possibile configurare OpsCenter per creare e gestire OpsItems su più account o su un solo account. Se si configura OpsCenter la creazione e la gestione OpsItems su più account, è possibile utilizzare l'account amministratore delegato di Systems Manager o l'account di AWS Organizations gestione per creare, visualizzare o modificare OpsItems manualmente altri account. Per ulteriori informazioni sull'account amministratore delegato di Systems Manager, consulta [Configurazione di un amministratore delegato per Explorer](#).

Se configuri OpsCenter per un singolo account, è possibile visualizzare o modificare gli OpsItems solo nell'account in cui gli OpsItems sono stati creati. Non è possibile condividere o trasferire dati OpsItems. Account AWS Per questo motivo, ti consigliamo di configurare le autorizzazioni per OpsCenter l' Account AWS area utilizzata per eseguire i AWS carichi di lavoro. È quindi possibile creare utenti o gruppi in tale account. In questo modo, più tecnici operativi o professionisti IT possono creare, visualizzare e modificare OpsItems nello stesso Account AWS.

Explorer e OpsCenter usano le seguenti operazioni delle API. È possibile utilizzare tutte le funzionalità di Explorer e OpsCenter se l'utente, il gruppo o il ruolo hanno accesso a tali operazioni. È anche possibile creare un accesso più restrittivo, come descritto più avanti in questa sezione.

- [CreateOpsItem](#)
- [CreateResourceDataSync](#)
- [DescribeOpsItems](#)
- [DeleteResourceDataSync](#)
- [GetOpsItem](#)
- [GetOpsSummary](#)
- [ListResourceDataSync](#)
- [UpdateOpsItem](#)
- [UpdateResourceDataSync](#)

Se preferisci, puoi specificare l'autorizzazione di sola lettura assegnando la seguente policy inline all'account, gruppo o ruolo.

## JSON

```
{
```

```
"Version": "2012-10-17",
"Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:GetOpsItem",
 "ssm:GetOpsSummary",
 "ssm:DescribeOpsItems",
 "ssm:GetServiceSetting",
 "ssm:ListResourceDataSync"
],
 "Resource": "*"
 }
]
```

Per informazioni sulla creazione di una policy IAM, consulta [Creazione di policy IAM](#) nella Guida per l'utente di IAM. Per informazioni su come assegnare questa policy a un gruppo IAM, consulta [Attaching a Policy to an IAM Group \(Collegamento di una policy a un gruppo IAM\)](#).

Crea un'autorizzazione utilizzando quanto segue e aggiungila ai tuoi utenti, gruppi o ruoli:

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:GetOpsItem",
 "ssm:UpdateOpsItem",
 "ssm:DescribeOpsItems",
 "ssm:CreateOpsItem",
 "ssm:CreateResourceDataSync",
 "ssm>DeleteResourceDataSync",
 "ssm:ListResourceDataSync",
 "ssm:UpdateResourceDataSync"
],
 "Resource": "*"
 }
]
}
```

```
}
]
}
```

A seconda dell'applicazione di identità utilizzata nell'organizzazione, è possibile selezionare una sequenti opzioni per configurare l'accesso degli utenti.

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.

Limitazione dell'accesso a OpsItems utilizzando i tag

È inoltre possibile limitare l'accesso a OpsItems utilizzando una policy IAM inline che specifica i tag. Ecco un esempio che specifica una chiave tag di Dipartimento e un valore di tag di Finanza. Con questa policy, l'utente può chiamare l'operazione `GetOpsItem` API solo per visualizzare OpsItems le visualizzazioni precedentemente contrassegnate con `Key=Department` e `Value=Finance`. Gli utenti non sono in grado di visualizzare qualsiasi altro OpsItems.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Deny",
 "Principal": "*",
 "Action": "ops:GetOpsItem",
 "Resource": "arn:aws:opsitem:*:*:*:*",
 "Condition": {
 "tag:Department": "Finance"
 }
 }
]
}
```

```
{
 "Effect": "Allow",
 "Action": [
 "ssm:GetOpsItem"
],
 "Resource": "*"
},
{
 "Condition": { "StringEquals": { "ssm:resourceTag/Department":
"Finance" } }
}
]
```

Ecco un esempio che specifica le operazioni API per la visualizzazione e l'aggiornamento degli OpsItems. Questa policy specifica anche due set di coppie chiave-valore di tag: e. Department-Finance Project-Unity

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:GetOpsItem",
 "ssm:UpdateOpsItem"
],
 "Resource": "*",
 "Condition": {
 "StringEquals": {
 "ssm:resourceTag/Department": "Finance",
 "ssm:resourceTag/Project": "Unity"
 }
 }
 }
]
}
```

Per ulteriori informazioni sull'aggiunta di tag a un OpsItem, consulta [Crea OpsItems manualmente](#).

## Comprensione EventBridge delle regole predefinite create da Integrated Setup

Durante il processo di configurazione integrato di Explorer eOpsCenter, puoi scegliere di abilitare diverse regole predefinite basate sugli eventi rilevati da Amazon EventBridge. Quando vengono rilevati questi eventi, il sistema crea automaticamente OpsItems in AWS Systems Manager e OpsCenter.

Per esempio, questa regola `SSMOpsItems-Autoscaling-instance-termination-failure` crea OpsItem quando la chiusura di un'istanza di dimensionamento automatico EC2 non riesce.

La regola `SSMOpsItems-SSM-maintenance-window-execution-failed` crea OpsItem quando una finestra di manutenzione di Systems Manager non viene completata correttamente.

Per le istruzioni di configurazione e le descrizioni di tutte le EventBridge regole che puoi abilitare durante il processo di configurazione, consulta [Configurazione di OpsCenter](#).

Se non desideri creare EventBridge OpsItems per questi eventi, puoi scegliere di non abilitare questa opzione in Configurazione integrata. Se preferisci, puoi specificare OpsCenter come obiettivo di EventBridge eventi specifici. Per ulteriori informazioni, consulta [Configura EventBridge le regole per creare OpsItems](#).

È possibile disabilitare una regola predefinita o modificarne la categoria e il livello di gravità nella pagina Impostazioni OpsCenter scegliendo OpsCenter, Impostazioni e quindi scegliendo Modifica nell'area delle Regole OpsItem.

È inoltre possibile modificare la categoria o la gravità assegnata a un singolo OpsItem creato da queste regole nella console Systems Manager. Per informazioni, consulta [Modifica di un OpsItem](#).

| OpsItem rules <span>Edit</span>                                       |              |          |           |
|-----------------------------------------------------------------------|--------------|----------|-----------|
| <input type="text"/>                                                  |              |          |           |
| Rule                                                                  | Category     | Severity | State     |
| <a href="#">SSMOpsItems-Autoscaling-instance-launch-failure</a>       | Availability | 2-High   | ✔ enabled |
| <a href="#">SSMOpsItems-Autoscaling-instance-termination-failure</a>  | Availability | 2-High   | ✔ enabled |
| <a href="#">SSMOpsItems-EBS-snapshot-copy-failed</a>                  | Availability | 2-High   | ✔ enabled |
| <a href="#">SSMOpsItems-EBS-snapshot-creation-failed</a>              | Availability | 2-High   | ✔ enabled |
| <a href="#">SSMOpsItems-EBS-volume-performance-issue</a>              | Performance  | 3-Medium | ✔ enabled |
| <a href="#">SSMOpsItems-EC2-issue</a>                                 | Availability | 2-High   | ✔ enabled |
| <a href="#">SSMOpsItems-EC2-scheduled-change</a>                      | Availability | 3-Medium | ✔ enabled |
| <a href="#">SSMOpsItems-RDS-issue</a>                                 | Availability | 2-High   | ✔ enabled |
| <a href="#">SSMOpsItems-RDS-scheduled-change</a>                      | Availability | 3-Medium | ✔ enabled |
| <a href="#">SSMOpsItems-SSM-maintenance-window-execution-failed</a>   | Availability | 3-Medium | ✔ enabled |
| <a href="#">SSMOpsItems-SSM-maintenance-window-execution-timedout</a> | Availability | 2-High   | ✔ enabled |

## Configurazione di un amministratore delegato per Explorer

Se aggregi i dati di AWS Systems Manager Explorer da più account Regioni AWS e utilizzando la sincronizzazione dei dati delle risorse con AWS Organizations, ti consigliamo di configurare un amministratore delegato per Explorer. Un amministratore delegato migliora la sicurezza Explorer nei modi seguenti.

- Puoi limitare il numero di amministratori Explorer in grado di creare o eliminare le sincronizzazioni dei dati delle risorse di più account e dell'area a un singolo Account AWS.
- Non è più necessario accedere all'account di AWS Organizations gestione per amministrare le sincronizzazioni dei dati delle risorse. Explorer

Un amministratore delegato può utilizzare le seguenti API di sincronizzazione dei dati Explorer delle risorse utilizzando la console, l'SDK, () oppure: AWS Command Line Interface AWS CLI AWS Tools for Windows PowerShell



- [CreateResourceDataSync](#)
- [DeleteResourceDataSync](#)
- [ListResourceDataSync](#)
- [UpdateResourceDataSync](#)

Un amministratore delegato può cercare, filtrare e aggregare Explorer i dati dalla console o utilizzando strumenti programmatici come SDK, o. AWS CLI AWS Tools for Windows PowerShell La ricerca, il filtro e l'aggregazione dei dati utilizzano l'operazione API. [GetOpsSummary](#)

Un amministratore delegato può creare un massimo di cinque sincronizzazioni dei dati delle risorse per un'intera organizzazione o per un sottoinsieme di unità organizzative. Le sincronizzazioni dei dati delle risorse create da un amministratore delegato sono disponibili solo nell'account amministratore delegato. Non è possibile visualizzare le sincronizzazioni o i dati aggregati nell'account di gestione AWS Organizations .

#### Note

Non puoi utilizzare un account amministratore delegato per creare una sincronizzazione dei dati delle risorse in [Regioni AWS opt-in](#). È necessario utilizzare un account di AWS Organizations gestione.

Per informazioni sulla sincronizzazione dei dati delle risorse, consultare [Configurazione di Systems Manager Explorer per visualizzare dati da più account e regioni](#). Per ulteriori informazioni su AWS Organizations, vedi [Cos'è AWS Organizations?](#) nella Guida AWS Organizations per l'utente.

#### Argomenti

- [Prima di iniziare](#)
- [Configurare un amministratore delegato Explorer](#)
- [Annullare la registrazione di un amministratore delegato Explorer](#)

#### Prima di iniziare

Nell'elenco seguente sono incluse informazioni importanti sull'amministrazione Explorer delegata.

- È possibile delegare un solo account per l'amministrazione Explorer.

- L'ID account specificato come amministratore delegato Explorer deve essere elencato come account membro in AWS Organizations. Per ulteriori informazioni, consulta [Creare un account Account AWS nella tua organizzazione](#) nella Guida AWS Organizations per l'utente.
- Un amministratore delegato può utilizzare tutte le operazioni dell'API di sincronizzazione dei dati delle Explorer risorse nella console o utilizzando strumenti programmatici come SDK, AWS Command Line Interface (AWS CLI) o AWS Tools for Windows PowerShell. Le operazioni dell'API di sincronizzazione dei dati delle risorse includono quanto segue: [CreateResourceDataSync](#), [DeleteResourceDataSync](#), [ListResourceDataSync](#) e [UpdateResourceDataSync](#).
- Un amministratore delegato può cercare, filtrare e aggregare i dati Explorer nella console o utilizzando strumenti a livello di programmazione quali SDK, AWS CLI o AWS Tools for Windows PowerShell. La ricerca, il filtro e l'aggregazione dei dati utilizzano l'operazione [GetOpsSummary](#) API.
- Le sincronizzazioni dei dati delle risorse create da un amministratore delegato sono disponibili solo nell'account amministratore delegato. Non puoi visualizzare le sincronizzazioni o i dati aggregati nell'account di gestione. AWS Organizations
- Un amministratore delegato può creare un massimo di cinque sincronizzazioni di dati delle risorse.
- Un amministratore delegato può creare una sincronizzazione dei dati delle risorse per un'intera organizzazione AWS Organizations o per un sottoinsieme di unità organizzative.

## Configurare un amministratore delegato Explorer

Per registrare un Explorer amministratore delegato, attenersi alla procedura descritta di seguito.

Per registrare un Explorer amministratore delegato

1. Accedi al tuo account AWS Organizations di gestione.
2. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
3. Nel pannello di navigazione, scegli Explorer.
4. Seleziona Impostazioni.
5. Nella sezione Amministratore delegato per Explorer, verifica di aver configurato le opzioni di accesso al servizio e al ruolo collegato al servizio necessarie. Se necessario, scegli i pulsanti Crea ruolo e Abilitazione dell'accesso per configurare queste opzioni.
6. Per Account ID, inserisci l' Account AWS ID. Questo account deve essere un account membro in AWS Organizations.

## 7. Scegliere Registra amministratore delegato.

L'amministratore delegato ha ora accesso alle AWS Organizations opzioni Includi tutti gli account dalla mia AWS Organizations configurazione e Seleziona le unità organizzative nella pagina Crea sincronizzazione dei dati delle risorse.

### Annullare la registrazione di un amministratore delegato Explorer

Utilizza la procedura seguente per annullare la registrazione di un amministratore delegato Explorer. Un account amministratore delegato può essere annullato solo dall'account di gestione AWS Organizations . Quando viene annullata la registrazione di un account amministratore delegato, il sistema elimina tutte le sincronizzazioni dei dati AWS Organizations delle risorse create dall'amministratore delegato.

Per annullare la registrazione di un amministratore delegato Explorer

1. Accedi al tuo account di gestione. AWS Organizations
2. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
3. Nel pannello di navigazione, scegli Explorer.
4. Seleziona Impostazioni.
5. Nella sezione Amministratore delegato per Explorer scegli Annulla registrazione. Il sistema visualizza un avviso.
6. Digita l'ID account e scegli Rimuovi.

L'account non ha più accesso alle operazioni dell'API di sincronizzazione dei dati delle AWS Organizations risorse. Il sistema elimina tutte le sincronizzazioni dei dati AWS Organizations sulle risorse create dall'account.

### Configurazione di Systems Manager Explorer per visualizzare dati da più account e regioni

AWS Systems Manager utilizza un'esperienza di configurazione integrata per aiutarti a iniziare a usare AWS Systems Manager Explorer e AWS Systems Manager OpsCenter. Dopo aver completato l'installazione integrata, Explorer e OpsCenter sincronizzano automaticamente i dati. In particolare, questi strumenti consentono OpsItems di sincronizzare OpsData Account AWS e Regione AWS utilizzare al termine della configurazione integrata. Se si desidera OpsData aggregare dati OpsItems

provenienti da altri account e regioni, è necessario creare una sincronizzazione dei dati delle risorse, come descritto in questo argomento.

#### Note

Per ulteriori informazioni sulla configurazione integrata, consulta [Nozioni di base su Systems Manager Explorer e OpsCenter](#).

## Argomenti

- [Comprendere le sincronizzazioni dei dati delle risorse per Explorer](#)
- [Comprendere la sincronizzazione dei dati delle risorse di più account e Regioni](#)
- [Creazione di una sincronizzazione dati dei dati delle risorse](#)

## Comprendere le sincronizzazioni dei dati delle risorse per Explorer

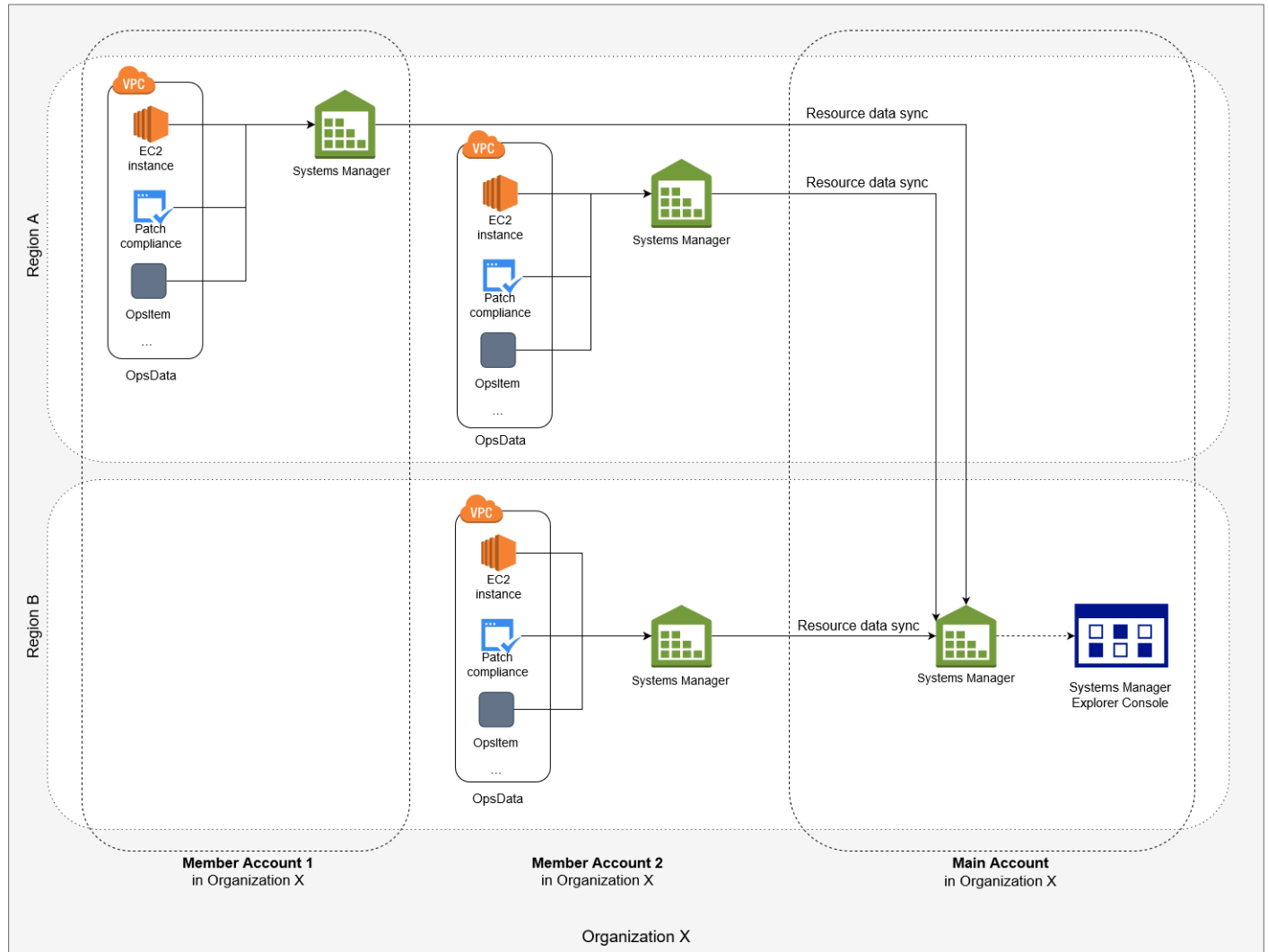
La sincronizzazione dei dati delle risorse per Explorer offre due opzioni di aggregazione:

- Single-account/Multiple-regions: puoi configurare l'aggregazione Explorer OpsItems di OpsData dati provenienti da più dati Regioni AWS, ma il set di dati è limitato a quello corrente. Account AWS
- Multiple-accounts/Multiple-regions: è possibile Explorer configurare l'aggregazione dei dati provenienti da più account Regioni AWS . Questa opzione richiede l'impostazione e la configurazione di AWS Organizations. Dopo aver impostato e configurato AWS Organizations, puoi aggregare i dati per unità organizzativa (OU) o per un'intera organizzazione. Explorer Systems Manager aggrega i dati nell'account di gestione AWS Organizations prima di visualizzarlo in Explorer. Per ulteriori informazioni, vedi [Che cos'è AWS Organizations?](#) nella Guida AWS Organizations per l'utente.

#### Warning

Se si configura Explorer l'aggregazione dei dati di un'organizzazione in AWS Organizations, il sistema abilita OpsData tutti gli account membri dell'organizzazione. L'abilitazione OpsData delle fonti in tutti gli account dei membri aumenta il numero di chiamate ad OpsCenter API come [CreateOpsItem](#) e [GetOpsSummary](#) Per le chiamate a queste operazioni API ti sarà addebitato un costo.

Il diagramma seguente mostra una sincronizzazione dei dati delle risorse configurata per funzionare con AWS Organizations. In questo scenario, l'utente dispone di due account definiti in AWS Organizations. La sincronizzazione dei dati delle risorse aggrega i dati di entrambi gli account e di più account Regioni AWS nell'account di AWS Organizations gestione in cui vengono poi visualizzati. Explorer



## Comprendere la sincronizzazione dei dati delle risorse di più account e Regioni

In questa sezione vengono descritti i dettagli importanti sulla sincronizzazione dei dati delle risorse di più account e Regioni che utilizzano AWS Organizations. In particolare, le informazioni contenute in questa sezione si applicano se si sceglie una delle opzioni seguenti nella pagina Create resource data sync (Crea sincronizzazione dei dati delle risorse):

- Includi tutti gli account della mia configurazione AWS Organizations

- Seleziona le unità organizzative in AWS Organizations

Se non si prevede di utilizzare una di queste opzioni, è possibile ignorare questa sezione.

Quando si crea una sincronizzazione dei dati delle risorse nella console SSM e si sceglie una delle AWS Organizations opzioni, Systems Manager consente automaticamente tutte le OpsData fonti nelle regioni selezionate per tutti i Account AWS componenti dell'organizzazione o delle unità organizzative selezionate. Ad esempio, anche se non è stata attivata l'opzione Explorer in una regione, la selezione di un' AWS Organizations opzione fa sì che Systems Manager effettui automaticamente la raccolta OpsData da tale regione. Per creare una sincronizzazione dei dati delle risorse senza consentire OpsData le fonti, specifica `EnableAllOpsDataSources` come false durante la creazione della sincronizzazione dei dati. Per ulteriori informazioni, consulta i dettagli `EnableAllOpsDataSources` dei parametri per il tipo di [ResourceDataSyncSource](#) dati nell'API Reference di Amazon EC2 Systems Manager.

Se non scegli una delle AWS Organizations opzioni per la sincronizzazione dei dati delle risorse, devi completare la configurazione integrata in ogni account e regione in cui desideri accedere Explorer ai dati. In caso contrario, Explorer non verrà visualizzato OpsData né OpsItems per gli account e le regioni in cui non hai completato la configurazione integrata.

Se aggiungi un account figlio alla tua organizzazione, abilita Explorer automaticamente tutte le OpsData fonti dell'account. Se, in un secondo momento, rimuovi l'account figlio dalla tua organizzazione, Explorer continua a raccogliere OpsData fondi dall'account.

Se aggiorni la sincronizzazione dei dati di una risorsa esistente che utilizza una delle AWS Organizations opzioni, il sistema richiede di approvare la raccolta di tutte le OpsData fonti per tutti gli account e le regioni interessati dalla modifica.

Se aggiungi un nuovo servizio al tuo e se effettua una Explorer raccolta OpsData per quel servizio Account AWS, Systems Manager si configura Explorer automaticamente per raccoglierlo. OpsData Ad esempio, se l'organizzazione non ha utilizzato AWS Trusted Advisor quando in precedenza hai creato una sincronizzazione dei dati delle risorse, ma l'organizzazione si iscrive a questo servizio, aggiorna Explorer automaticamente le sincronizzazioni dei dati delle risorse per raccoglierle. OpsData

#### Important

Tenere presente le seguenti informazioni importanti sulla sincronizzazione dei dati delle risorse di più account e Regioni:

- L'eliminazione della sincronizzazione dei dati di una risorsa non disattiva l'accesso alla OpsData fonte. Explorer
- Per visualizzare OpsData e OpsItems da più account, devi avere la modalità AWS Organizations Tutte le funzionalità attivata e devi aver effettuato l'accesso all'account di AWS Organizations gestione.
- La Regione AWS maggior parte è attiva per impostazione predefinita Account AWS, ma alcune regioni vengono attivate solo quando le selezioni manualmente. Queste Regioni sono chiamate [Regioni opt-in](#). Per impostazione predefinita, Explorer le sincronizzazioni dei dati delle risorse tra account/cross regioni non supportano l'aggregazione dei dati nelle regioni con consenso esplicito. È stato aggiunto il supporto per le seguenti Regioni con consenso esplicito il 30 giugno 2025.
  - Europa (Milano)
  - Africa (Città del Capo)
  - Medio Oriente (Bahrein)
  - Asia Pacifico (Hong Kong)

Tieni presente che non puoi utilizzare un account amministratore delegato per creare una sincronizzazione dei dati delle risorse nelle Regioni che hanno aderito. È necessario utilizzare un account di gestione AWS Organizations .

## Creazione di una sincronizzazione dati dei dati delle risorse

Prima di configurare una sincronizzazione dei dati delle risorse per Explorer, prendere nota dei seguenti dettagli.

- Explorer supporta un massimo di cinque sincronizzazioni dei dati delle risorse.
- Dopo aver creato una sincronizzazione dei dati delle risorse per una Regione, non è possibile modificare le opzioni dell'account per tale sincronizzazione. Ad esempio, se crei una sincronizzazione nella regione us-east-2 (Ohio) e scegli l'opzione Includi solo l'account corrente, non puoi modificare la sincronizzazione in un secondo momento e scegliere l'opzione Includi tutti gli account dalla mia configurazione. AWS Organizations Al contrario, è necessario eliminare la prima sincronizzazione dei dati delle risorse e crearne una nuova.
- OpsData visualizzato in Explorer è di sola lettura.

Utilizzare la procedura seguente per creare una sincronizzazione dei dati delle risorse per Explorer.

Come creare una sincronizzazione dei dati delle risorse

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Explorer.
3. Seleziona Impostazioni.
4. Nella sezione Configure resource data sync (Configura sincronizzazione dati risorsa), scegliere Create resource data sync (Crea sincronizzazione dati risorsa).
5. Per Resource data sync name (Nome sincronizzazione dati risorsa), immettere un nome.
6. Nella sezione Add accounts (Aggiungi account), scegliere un'opzione.

 Note

Per utilizzare una delle AWS Organizations opzioni, è necessario accedere all'account di AWS Organizations gestione o accedere a un account amministratore Explorer delegato. Per ulteriori informazioni sull'account amministratore delegato, vedere [Configurazione di un amministratore delegato per Explorer](#).

7. Nella sezione Regions to include (Regioni da includere) scegliere una delle seguenti opzioni.
  - Scegli Tutte le regioni attuali e future per sincronizzare automaticamente i dati di tutte le regioni attuali Regioni AWS e di tutte le nuove regioni che saranno online in futuro.
  - Scegli Tutte le regioni per sincronizzare automaticamente i dati di tutte le regioni correnti Regioni AWS.
  - Scegliere singolarmente le regioni da includere.
8. Scegli Crea sincronizzazione dei dati di risorsa.

Il sistema può richiedere alcuni minuti per compilare Explorer con i dati dopo aver creato una sincronizzazione dei dati delle risorse. È possibile visualizzare la sincronizzazione selezionandola dall'elenco Select a resource data sync (Selezionare una sincronizzazione dati risorsa) in Explorer.

## Uso di Explorer

Questa sezione include informazioni su come personalizzare AWS Systems Manager Explorer modificando il layout del widget e modificando i dati visualizzati nella dashboard.



## Indice

- [EventBridge Regole di modifica create per Explorer](#)
- [Modifica delle origini dei dati in Systems Manager Explorer](#)
- [Personalizzazione del Explorer display](#)
- [Ricezione di risultati da AWS Security Hub CSPM in Explorer](#)
- [Cancellazione della Sincronizzazione dei dati delle risorse di Systems Manager Explorer](#)

## EventBridge Regole di modifica create per Explorer

Una volta completata la configurazione integrata, il sistema consente più di una dozzina di regole in Amazon EventBridge. Queste regole vengono create OpsItems automaticamente. AWS Systems Manager OpsCenter AWS Systems Manager Explorer quindi visualizza informazioni aggregate su OpsItems

Ogni regola include un valore di Categoria e Gravità preimpostati. Quando il sistema crea OpsItems da un evento, assegna automaticamente Categoria e Gravità preimpostati.

### Important

Attualmente, non è possibile modificare i valori Categoria e Gravità per le regole predefinite, ma è possibile modificare questi valori sugli OpsItems creati sulla base delle regole predefinite.

**OpsItem rules**

Edit

| Rule                                                                  | Category     | Severity | State     |
|-----------------------------------------------------------------------|--------------|----------|-----------|
| <a href="#">SSMOpsItems-Autoscaling-instance-launch-failure</a>       | Availability | 2-High   | ✔ enabled |
| <a href="#">SSMOpsItems-Autoscaling-instance-termination-failure</a>  | Availability | 2-High   | ✔ enabled |
| <a href="#">SSMOpsItems-EBS-snapshot-copy-failed</a>                  | Availability | 2-High   | ✔ enabled |
| <a href="#">SSMOpsItems-EBS-snapshot-creation-failed</a>              | Availability | 2-High   | ✔ enabled |
| <a href="#">SSMOpsItems-EBS-volume-performance-issue</a>              | Performance  | 3-Medium | ✔ enabled |
| <a href="#">SSMOpsItems-EC2-issue</a>                                 | Availability | 2-High   | ✔ enabled |
| <a href="#">SSMOpsItems-EC2-scheduled-change</a>                      | Availability | 3-Medium | ✔ enabled |
| <a href="#">SSMOpsItems-RDS-issue</a>                                 | Availability | 2-High   | ✔ enabled |
| <a href="#">SSMOpsItems-RDS-scheduled-change</a>                      | Availability | 3-Medium | ✔ enabled |
| <a href="#">SSMOpsItems-SSM-maintenance-window-execution-failed</a>   | Availability | 3-Medium | ✔ enabled |
| <a href="#">SSMOpsItems-SSM-maintenance-window-execution-timedout</a> | Availability | 2-High   | ✔ enabled |

Per modificare le regole predefinite per la creazione OpsItems

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Explorer.
3. Seleziona Impostazioni.
4. Nella sezione Regole OpsItems, scegli Modifica.
5. Espandi Regole CWE.
6. Deselezionare la casella di controllo accanto alle regole che non si desidera utilizzare.
7. Utilizza gli elenchi Categoria e Gravità per modificare queste informazioni per una regola.
8. Scegli Salva.

Le modifiche avranno effetto alla successiva creazione di un OpsItem da parte del sistema.

## Modifica delle origini dei dati in Systems Manager Explorer

Per Regioni AWS questo sono disponibili per [impostazione predefinita](#), AWS Systems Manager Explorer visualizza i dati provenienti dalle seguenti fonti. È possibile modificare le impostazioni in Explorer per aggiungere o rimuovere origini dati:

- Amazon Elastic Compute Cloud (Amazon EC2)
- AWS Systems Manager Inventory
- AWS Systems Manager OpsCenter OpsItems
- Conformità patch AWS Systems Manager Patch Manager
- AWS Systems Manager State Manager conformità dell'associazione
- AWS Trusted Advisor
- AWS Compute Optimizer
- Supporto AWS Casi centrali
- AWS Config conformità a regole e risorse
- AWS Security Hub CSPM risultati

### Note

Per la regione Asia Pacifico (Osaka), Explorer non visualizza i dati AWS Compute Optimizer e i AWS Security Hub CSPM risultati.

Per le [Regioni AWS opt-in](#), Explorer visualizza i dati provenienti dalle seguenti fonti:

- Amazon Elastic Compute Cloud (Amazon EC2)
- AWS Systems Manager Inventory
- AWS Systems Manager OpsCenter OpsItems
- Conformità patch AWS Systems Manager Patch Manager
- AWS Systems Manager State Manager conformità all'associazione
- AWS Trusted Advisor
- Supporto AWS Casi centrali
- AWS Config conformità a regole e risorse

 Note

- Per visualizzare i casi del Supporto CentroExplorer, è necessario disporre di un account Enterprise o Business configurato con Supporto.
- Non è possibile configurare Explorer per interrompere la visualizzazione dei dati OpsCenter OpsItem.

## Prima di iniziare

Verificare di aver impostato e configurato i servizi che popolano i widget Explorer con i dati. Per ulteriori informazioni, consulta [Impostazione di servizi correlati per Explorer](#).

## Per modificare le origini dati

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Explorer.
3. Scegli Settings, quindi seleziona la scheda Configure Dashboard (Configura pannello di controllo).
4. Nella sezione OpsData sorgenti, nella colonna Stato, attiva o disattiva le fonti in base ai dati che desideri visualizzare.

## Personalizzazione del Explorer display

Puoi personalizzare il layout dei widget in AWS Systems Manager Explorer utilizzando una funzionalità drag-and-drop. Puoi anche personalizzare gli annunci OpsData OpsItems visualizzati Explorer utilizzando i filtri, come descritto in questo argomento.

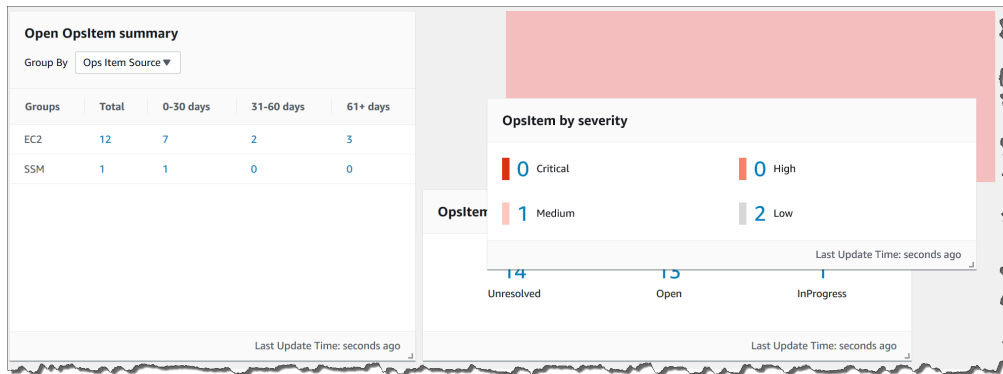
Prima di personalizzare il layout dei widget, verifica che i widget siano attualmente visualizzati in Explorer. Per visualizzare alcuni widget in Explorer (ad esempio il widget di conformità AWS Config ), è necessario abilitarli nella pagina Configura pannello di controllo.

## Per abilitare la visualizzazione dei widget in Explorer

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>

2. Nel pannello di navigazione, scegli Explorer.
3. Scegli Operazioni del pannello di controllo, Configura pannello di controllo.
4. Scegli la scheda Configura pannello di controllo.
5. Scegli Abilita tutto o attiva un singolo widget o una singola origine dati.
6. Scegli Explorer per visualizzare le modifiche.

Per personalizzare il layout del widget di Explorer, scegli un widget che desideri spostare. Tieni premuto il nome del widget, quindi trascinalo nella nuova posizione.



Ripeti questo processo per ogni widget che desideri riposizionare.

Se il nuovo layout non piace, scegli Ripristina layout per spostare tutti i widget nella loro posizione originale.

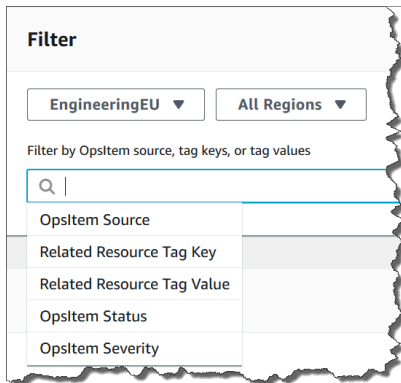
Utilizzo dei filtri per modificare i dati visualizzati in Explorer

Per impostazione predefinita, Explorer visualizza i dati per la regione corrente Account AWS e quella corrente. Se si creano una o più sincronizzazioni dei dati delle risorse, è possibile utilizzare i filtri per modificare la sincronizzazione attiva. È quindi possibile scegliere di visualizzare i dati per una regione specifica o per tutte le regioni. È inoltre possibile utilizzare la barra di ricerca per filtrare i diversi criteri OpsItem e tag-chiave.

Per modificare i dati visualizzati in Explorer utilizzando i filtri

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Explorer.
3. Nella sezione Filtro, utilizza l'elenco Seleziona una sincronizzazione dati risorsa per scegliere una sincronizzazione.

4. Utilizza l'elenco Regioni per scegliere una Regione AWS specifica o Tutte le Regioni.
5. Scegliere la barra di ricerca, quindi scegliere i criteri su cui filtrare i dati.



6. Premere Invio.

Explorer mantiene le opzioni di filtro selezionate se si chiude e si riapre la pagina.

Ricezione di risultati da AWS Security Hub CSPM in Explorer

[AWS Security Hub CSPM](#) fornisce una visione completa del tuo stato di sicurezza in AWS. Il servizio raccoglie dati di sicurezza, denominati esiti, da tutti gli Account AWS, i servizi e dai prodotti di terze parti supportati. I risultati del CSPM di Security Hub possono aiutarvi a verificare il vostro ambiente rispetto agli standard e alle best practice del settore della sicurezza, analizzare le tendenze di sicurezza e identificare i problemi di sicurezza con la massima priorità.

Security Hub CSPM invia i risultati ad Amazon EventBridge, che utilizza una regola di evento a cui inviare i risultati. Explorer Dopo aver abilitato l'integrazione, come descritto qui, puoi visualizzare i risultati di Security Hub CSPM in un Explorer widget e visualizzare i dettagli dei risultati in OpsCenter OpsItems. Il widget fornisce un riepilogo di tutti i risultati di Security Hub CSPM in base alla gravità. I nuovi risultati in Security Hub CSPM sono generalmente visibili Explorer entro pochi secondi dalla creazione.

#### Warning

Prendi nota delle seguenti informazioni importanti.

- Explorer è integrato con OpsCenter. Dopo aver abilitato Explorer l'integrazione con Security Hub CSPM, crea OpsCenter OpsItems automaticamente i risultati di Security Hub CSPM. A seconda AWS dell'ambiente, l'abilitazione dell'integrazione può comportare un numero elevato di OpsItems, a un costo.

Prima di continuare, leggi OpsCenter l'integrazione con Security Hub CSPM. L'argomento include dettagli specifici su come le modifiche e gli aggiornamenti a esiti e OpsItems vengono addebitati sul tuo account. Per ulteriori informazioni, consulta [Comprensione OpsCenter integrazione con AWS Security Hub CSPM](#). Per informazioni sui prezzi, consulta OpsCenter [Prezzi di AWS Systems Manager](#).

- Se si crea una sincronizzazione dei dati delle risorse Explorer mentre si accede all'account amministratore, l'integrazione di Security Hub CSPM viene abilitata automaticamente per l'amministratore e per tutti gli account membri coinvolti nella sincronizzazione. Una volta abilitata, crea OpsCenter automaticamente i risultati OpsItems di Security Hub CSPM, a un costo. Per informazioni sulla sincronizzazione dei dati delle risorse, consulta [Configurazione di Systems Manager Explorer per visualizzare dati da più account e regioni](#).

## Tipi di risultati che Explorer riceve

Explorer riceve [tutti i risultati](#) da Security Hub CSPM. Puoi visualizzare tutti i risultati in base alla gravità nel Explorer widget quando attivi le impostazioni predefinite di Security Hub CSPM. Per impostazione predefinita, Explorer crea i risultati OpsItems relativi alla gravità critica. È possibile configurare manualmente Explorer la creazione OpsItems per altri livelli di gravità (Alto, Medio e Basso).

Sebbene Explorer non crei risultati OpsItems informativi, è possibile visualizzare i dati operativi informativi (OpsData) nel widget di riepilogo dei risultati del Security Hub CSPM. Explorer crea OpsData per tutti i risultati indipendentemente dalla gravità. Per ulteriori informazioni sui livelli di gravità CSPM di Security Hub, consulta [Severity](#) in the AWS Security Hub API Reference.

## Abilitazione dell'integrazione

Questa sezione descrive come abilitare e configurare Explorer l'avvio della ricezione dei risultati CSPM di Security Hub.

### Prima di iniziare

Completa le seguenti attività prima di configurare Explorer per iniziare a ricevere i risultati CSPM di Security Hub.

- Abilita e configura Security Hub CSPM. Per ulteriori informazioni, vedere [Configurazione di Security Hub CSPM](#) nella Guida per l'utente. AWS Security Hub

- Accedere all'account di AWS Organizations gestione. Systems Manager richiede l'accesso per creare AWS Organizations a OpsItems partire dai risultati del CSPM di Security Hub. Dopo aver effettuato l'accesso all'account di gestione, è possibile abilitare questo accesso dalla scheda Explorer Configure dashboard, come descritto nella procedura seguente. Se il pulsante Abilita accesso non è visualizzato, l'accesso affidabile è già abilitato. Se non accedi all'account di AWS Organizations gestione, non puoi consentire l'accesso e non puoi creare in base ai Explorer risultati del CSPM OpsItems di Security Hub.

#### Note

Se il tuo account non fa parte di un'organizzazione in AWS Organizations, non è necessario abilitare l'accesso affidabile di OpsData Sync. Il requisito dell'account di gestione descritto in questa sezione non si applica. Attiva AWS Security Hub CSPM in ognuno dei punti in Regione AWS cui desideri ricevere i risultati, quindi, nella scheda Explorer Configura dashboard, attiva l'interruttore dei risultati CSPM OpsItems creato da Security Hub.

Per iniziare a ricevere i risultati di Security Hub CSPM

1. (account di gestione) Attiva AWS Security Hub CSPM in ognuno dei punti Regione AWS in cui desideri ricevere i risultati. Per ulteriori informazioni, vedere [Configurazione di Security Hub CSPM](#) nella Guida per l'AWS Security Hub utente.
2. (account di gestione) Abilita l'accesso affidabile di OpsData Sync per. AWS OrganizationsÈ necessario abilitare l'accesso affidabile prima di poter attivare la OpsData fonte propria dell'account di gestione nel passaggio 3. I passaggi 4 e 5, per gli account membri e amministratori delegati, non dipendono dall'accesso affidabile. Scegli una delle seguenti opzioni:
  - Nella scheda Configura dashboardExplorer, nella sezione dei risultati del CSPM OpsItems creata da Security Hub, scegli il pulsante Abilita l'accesso.
  - Esegui il comando seguente utilizzando. AWS CLI

```
aws organizations enable-aws-service-access --service-principal
opsdatasync.ssm.amazonaws.com
```



 Note

Se hai effettuato l'accesso all'account di gestione e il pulsante **Abilita accesso** non è visualizzato, l'accesso affidabile è già abilitato. Per confermare, esegui il comando seguente.

```
aws organizations list-aws-service-access-for-organization
```

 Note

L'avviso **Abilita accesso** viene visualizzato anche nella procedura guidata di sincronizzazione dei dati delle risorse, un punto di ingresso comune nell'account di gestione.

3. (account di gestione, opzionale) Completa questo passaggio solo se desideri ottenere informazioni anche dall'account di gestione stesso. Attiva l'interruttore dei risultati CSPM OpsItems creato da Security Hub. Per impostazione predefinita, Explorer crea OpsItems i risultati di gravità critici ed è possibile configurarlo OpsItems per creare livelli di gravità aggiuntivi.
4. (Account di ogni membro o amministratore delegato) Abilita AWS Security Hub CSPM nel relativo Regione AWS account.
5. (Ogni account membro o amministratore delegato) Attiva l'interruttore dei risultati del OpsItems CSPM creato da Security Hub. Questi account possono completare questo passaggio in qualsiasi momento, senza dipendere dal passaggio 2. Se si crea una sincronizzazione dei dati delle risorse con ambito organizzativo Explorer dall'account di gestione (ovvero una sincronizzazione la cui origine è l'intera organizzazione o unità organizzative specifiche), questa OpsData fonte viene abilitata automaticamente per tutti gli account membri inclusi nella sincronizzazione.

Come visualizzare i risultati di Security Hub CSPM

La procedura seguente descrive come visualizzare i risultati di Security Hub CSPM.

## Per visualizzare i risultati di Security Hub CSPM

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Explorer.
3. Trova il widget Riepilogo degli esiti AWS Security Hub CSPM . Questo mostra i risultati del Security Hub CSPM. È possibile selezionare un livello di gravità per visualizzare una descrizione dettagliata del corrispondente OpsItem.

## Come interrompere l'invio degli esiti

La procedura seguente descrive come interrompere la ricezione dei risultati CSPM di Security Hub.

Per interrompere la ricezione dei risultati CSPM di Security Hub

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Explorer.
3. Seleziona Impostazioni.
4. Selezionare la scheda Configure dashboard (Configura il pannello di controllo).
5. Selezionare il Enabled (Abilitato) cursore per disattivare il AWS Security Hub CSPM.

### Important

Se l'opzione per disattivare i risultati CSPM di Security Hub è disattivata nella console, è possibile disabilitare questa impostazione eseguendo il seguente comando in AWS CLI. È necessario eseguire il comando mentre si è connessi all'account di AWS Organizations gestione o all'account amministratore delegato di Systems Manager. Per il `region` parametro, specificate il Regione AWS punto in cui non desiderate più ricevere i risultati CSPM di Security Hub. Explorer

```
aws ssm update-service-setting --setting-id /ssm/opsdata/SecurityHub --setting-value Disabled --region Regione AWS
```

Ecco un esempio:

```
aws ssm update-service-setting --setting-id /ssm/opsdata/SecurityHub --setting-value Disabled --region us-east-1
```

## Cancellazione della Sincronizzazione dei dati delle risorse di Systems Manager Explorer

In AWS Systems Manager Explorer, puoi aggregare i OpsData dati OpsItems provenienti da altri account e regioni creando una sincronizzazione dei dati delle risorse.

Non è possibile modificare le opzioni dell'account per una sincronizzazione dei dati delle risorse. Ad esempio, se hai creato una sincronizzazione nella regione us-east-2 (Ohio) e hai scelto l'opzione Includi solo l'account corrente, non puoi modificare la sincronizzazione in un secondo momento e scegliere l'opzione Includi tutti gli account dalla mia configurazione. AWS Organizations Al contrario, è necessario eliminare la sincronizzazione dei dati delle risorse e crearne una nuova, come descritto nella procedura seguente.

Come eliminare una sincronizzazione dei dati delle risorse

1. Apri la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Explorer.
3. Seleziona Impostazioni.
4. Nella sezione Configura sincronizzazione dei dati della risorsa, scegli la sincronizzazione dei dati della risorsa che si desidera eliminare.
5. Scegli Elimina.

## Esportazione OpsData da Systems Manager Explorer

Puoi esportare 5.000 OpsData articoli come file con valori separati da virgole (.csv) in un bucket Amazon Simple Storage Service (Amazon S3) da Explorer. AWS Systems Manager Explorer utilizza il runbook di [AWS-ExportOpsDataToS3](#) automazione per l'esportazione. OpsData Durante l'esportazione OpsData, il sistema visualizza la pagina del runbook di automazione in cui è possibile specificare dettagli, come Assumerole, nome del bucket Amazon S3, ARN dell'argomento SNS e campi da esportare.

Per OpsData esportare:

- [Fase 1: Indicazione di un argomento SNS](#)
- [Fase 2: \(facoltativa\) Configurazione dell'esportazione dei dati](#)
- [Fase 3: Esportazione OpsData](#)

## Fase 1: Indicazione di un argomento SNS

Quando configuri l'esportazione dei dati, devi specificare un argomento di Amazon Simple Notification Service (Amazon SNS) presente Regione AWS nello stesso luogo in cui desideri esportare i dati. Systems Manager invia una notifica all'argomento Amazon SNS quando l'esportazione è completata. Per informazioni su come creare un argomento Amazon SNS, consulta [Creazione di un argomento Amazon SNS](#).

## Fase 2: (facoltativa) Configurazione dell'esportazione dei dati

Puoi configurare le impostazioni di esportazione dei dati dalla pagina Impostazioni o Esporta Ops Data in un bucket S3.

Per configurare l'esportazione dei dati da Explorer

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Explorer.
3. Seleziona Impostazioni.
4. Nella sezione Configure data export (Configura esportazione dati) scegliere Edit (Modifica).
5. Per caricare il file di esportazione dei dati in un bucket Amazon S3 esistente, scegli Seleziona un bucket S3 esistente e scegli il bucket dall'elenco.

Per caricare il file di esportazione dei dati in un nuovo bucket Amazon S3, scegli Crea un nuovo bucket S3, quindi immetti il nome che desideri utilizzare per il nuovo bucket.

### Note

Puoi modificare il nome del bucket Amazon S3 e l'ARN dell'argomento Amazon SNS solo dalla pagina in cui hai configurato tali impostazioni per la prima volta in Explorer. Se configuri il bucket Amazon S3 e l'ARN dell'argomento Amazon SNS dalla pagina Impostazioni, puoi modificare tali impostazioni solo dalla pagina Impostazioni.

6. Per Seleziona un ARN di un argomento Amazon SNS scegli l'argomento che desideri notificare al termine dell'esportazione.
7. Scegli Create (Crea).

### Fase 3: Esportazione OpsData

Quando si esportano Explorer dati, Systems Manager crea un ruolo AWS Identity and Access Management (IAM) denominato `AmazonSSMExplorerExportRole`. Questo ruolo utilizza la policy IAM seguente.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "OpsSummaryExportAutomationServiceRoleStatement1",
 "Effect": "Allow",
 "Action": [
 "s3:PutObject"
],
 "Resource": [
 "arn:aws:s3:::amzn-s3-demo-bucket/*"
]
 },
 {
 "Sid": "OpsSummaryExportAutomationServiceRoleStatement2",
 "Effect": "Allow",
 "Action": [
 "s3:GetBucketAcl",
 "s3:GetBucketLocation"
],
 "Resource": [
 "arn:aws:s3:::amzn-s3-demo-bucket"
]
 },
 {
 "Sid": "OpsSummaryExportAutomationServiceRoleStatement3",
 "Effect": "Allow",
 "Action": [
 "sns:Publish"
]
 }
]
}
```

```

],
 "Resource": [
 "arn:aws:sns:us-east-1:111122223333:SNSTopicName"
]
},
{
 "Sid": "OpsSummaryExportAutomationServiceRoleStatement4",
 "Effect": "Allow",
 "Action": [
 "logs:DescribeLogGroups",
 "logs:DescribeLogStreams"
],
 "Resource": [
 "arn:aws:logs:us-east-1:111122223333:log-group:MyLogGroup"
]
},
{
 "Sid": "OpsSummaryExportAutomationServiceRoleStatement5",
 "Effect": "Allow",
 "Action": [
 "logs:CreateLogGroup",
 "logs:PutLogEvents",
 "logs:CreateLogStream"
],
 "Resource": [
 "*"
]
},
{
 "Sid": "OpsSummaryExportAutomationServiceRoleStatement6",
 "Effect": "Allow",
 "Action": [
 "ssm:GetOpsSummary"
],
 "Resource": [
 "*"
]
}
]
}

```

Il ruolo include l'entità di attendibilità seguente.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "OpsSummaryExportAutomationServiceRoleTrustPolicy",
 "Effect": "Allow",
 "Principal": {
 "Service": "ssm.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
]
}
```

Per esportare OpsData da Explorer

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Explorer.
3. Scegli un collegamento dati in un widget di Explorer. Ad esempio, scegli Problemi irrisolti o aperti nel widget OpsItems per stato. Oppure scegli il link Dati critici o OpsItemElevati nel widget Per gravità. Explorer apre la OpsData pagina per il set di dati selezionato.
4. Scegli Esporta tabella.

 Note

Quando si esporta OpsData per la prima volta, il sistema crea un ruolo secondario per l'esportazione. Non è possibile modificare il ruolo di assunzione predefinito.

5. Per Nome bucket S3, scegli un bucket esistente. Puoi scegliere Crea per creare un bucket Amazon S3, se necessario.

Se non riesci a modificare il nome del bucket S3, significa che hai configurato il nome del bucket dalla pagina Impostazioni. Puoi modificare il nome del bucket solo dalla pagina Impostazioni.

 Note

Puoi modificare il nome del bucket Amazon S3 e l'ARN dell'argomento Amazon SNS solo dalla pagina in cui hai configurato tali impostazioni per la prima volta in Explorer.

6. Per Arn argomento SNS, scegli un ARN di un argomento Amazon SNS per notificare il completamento del download.

Se non riesci a modificare l'ARN dell'argomento Amazon SNS, significa che hai configurato l'ARN dell'argomento Amazon SNS dalla pagina Impostazioni. Puoi modificare l'ARN dell'argomento solo dalla pagina Impostazioni.

7. (Facoltativo) Per Messaggio di successo SNS, specifica un messaggio di successo da visualizzare quando l'esportazione viene completata correttamente.
8. Seleziona Invia. Il sistema passa alla pagina precedente e visualizza il messaggio Fare clic per visualizzare lo stato del processo di esportazione. View details (Visualizza i dettagli)

Puoi scegliere Visualizza dettagli per visualizzare lo stato del runbook e l'avanzamento in Systems Manager Automation.

Ora puoi Explorer esportare OpsData dal bucket Amazon S3 specificato.

Se non è possibile esportare i dati utilizzando questa procedura, verifica che l'utente, il gruppo o il ruolo includa le operazioni `iam:CreatePolicyVersion` e `iam:DeletePolicyVersion`. Per informazioni sull'aggiunta di queste operazioni all'utente, al gruppo o al ruolo, consulta la pagina [Modifica delle policy IAM](#) nella Guida per l'utente IAM.

## Risoluzione dei problemi di Systems Manager Explorer

Questo argomento include informazioni sulla risoluzione di problemi comuni relativi a AWS Systems Manager Explorer.

La sincronizzazione dei dati delle risorse non funziona più

Se la sincronizzazione dei dati delle risorse ha smesso di funzionare per una Regione AWS opt-in, verifica che la Regione sia stata scelta sia per l'account di gestione AWS Organizations che per l'account membro, per cui è configurata la sincronizzazione.



La maggior parte Regioni AWS sono attive per impostazione predefinita per l'utente Account AWS, ma alcune regioni vengono attivate solo quando vengono selezionate manualmente. Queste Regioni sono chiamate [Regioni opt-in](#). Per impostazione predefinita, Explorer le sincronizzazioni dei dati delle risorse tra account/cross regioni non supportano l'aggregazione dei dati nelle regioni che accettano l'adesione. È stato aggiunto il supporto per le seguenti Regioni con consenso esplicito il 30 giugno 2025.

- Europa (Milano)
- Africa (Città del Capo)
- Medio Oriente (Bahrein)
- Asia Pacifico (Hong Kong)

Tieni presente che non puoi utilizzare un account amministratore delegato per creare una sincronizzazione dei dati delle risorse nelle Regioni che hanno aderito. È necessario utilizzare un account di gestione. AWS Organizations

Non è possibile filtrare AWS le risorse Explorer dopo aver aggiornato i tag nella pagina Impostazioni

Se si aggiornano le chiavi dei tag o altre impostazioni dei dati in Explorer, il sistema può richiedere fino a sei ore per sincronizzare i dati in base alle modifiche apportate.

Le AWS Organizations opzioni nella pagina Crea sincronizzazione dei dati delle risorse sono disattivate

Le AWS Organizations opzioni Includi tutti gli account dalla mia AWS Organizations configurazione e Seleziona le unità organizzative nella pagina Crea sincronizzazione dei dati delle risorse sono disponibili solo se sono state impostate e configurate AWS Organizations. Se le impostazioni sono state eseguite e configurate AWS Organizations, l'account di AWS Organizations gestione o un amministratore Explorer delegato possono creare sincronizzazioni dei dati delle risorse che utilizzano queste opzioni.

Per ulteriori informazioni, consultare [Configurazione di Systems Manager Explorer per visualizzare dati da più account e regioni](#) e [Configurazione di un amministratore delegato per Explorer](#).

Explorer non visualizza alcun dato

- Verificare di aver completato l'installazione integrata in ogni account e regione in cui si desidera che Explorer acceda e visualizzare i dati. In caso contrario, Explorer non verrà visualizzato OpsData e OpsItems per quegli account e regioni in cui non hai completato la configurazione

integrata. Per ulteriori informazioni, consulta [Nozioni di base su Systems Manager Explorer e OpsCenter](#).

- Se lo utilizzi Explorer per visualizzare i dati di più account e regioni, verifica di aver effettuato l'accesso all'account di AWS Organizations gestione o all'account amministratore Explorer delegato. Per visualizzare OpsData e utilizzare OpsItems più account e aree geografiche, devi aver effettuato l'accesso a questo account.

I widget sulle istanze Amazon EC2 non visualizzano i dati

Se i widget sulle istanze Amazon Elastic Compute Cloud (Amazon EC2), ad esempio Instance count (Conteggio istanze), Managed instances (Istanze gestite) e i widget Instance by AMI (Istanza per AMI) non visualizzano i dati, verificare quanto segue:

- Verifica di aver atteso diversi minuti. OpsData la visualizzazione può richiedere alcuni minuti Explorer dopo aver completato la configurazione integrata.
- Verificate di aver configurato il registratore di AWS Config configurazione. Explorer utilizza i dati forniti dal registratore di AWS Config configurazione per popolare i widget con informazioni sulle istanze EC2. Per ulteriori informazioni, vedere [Gestione del registratore di configurazione](#).
- Verifica che la OpsData fonte Amazon EC2 sia attiva nella pagina Impostazioni. Inoltre, verificare che siano trascorse più di 6 ore da quando è stato attivato il registratore di configurazione o da quando sono state apportate modifiche alle istanze. Systems Manager può impiegare fino a sei ore per visualizzare i dati dai AWS Config widget Explorer EC2 dopo aver inizialmente attivato il registratore di configurazione o aver apportato modifiche alle istanze.
- Tenere presente che se un'istanza viene arrestata o terminata, Explorer smette di mostrare tali istanze dopo 24 ore.
- Verifica di trovarti nella posizione corretta in Regione AWS cui hai configurato le tue istanze Amazon EC2. Explorer non visualizza dati sulle istanze locali.
- Se è stata configurata una sincronizzazione dei dati delle risorse per più account e Regioni, verificare di aver effettuato l'accesso all'account di gestione o a quello dell'amministratore delegato Explorer dell'organizzazione.

Il widget di patch non visualizza i dati

Il widget Non-compliant Istanze per l'applicazione di patch mostra solo i dati sulle istanze di patch che non sono conformi. Questo widget non visualizza dati se le istanze sono conformi. Se sospetti di avere istanze non conformi, verifica di aver impostato e configurato l'applicazione delle patch di

Systems Manager e l'utilizzo AWS Systems Manager Patch Manager per verificare la conformità delle patch. Per ulteriori informazioni, consulta [AWS Systems Manager Patch Manager](#).

## Questioni varie

Explorer non consente di modificare o correggere OpsItems: gli OpsItems visualizzati tra account o regioni sono di sola lettura. Possono essere aggiornati e riparati solo dal proprio account domestico o dalla propria regione.

## AWS Systems Manager OpsCenter

OpsCenter fornisce una posizione centrale in cui gli ingegneri operativi e i professionisti IT possono visualizzare, esaminare e risolvere gli elementi di lavoro operativi (OpsItems) relativi alle AWS risorse. OpsCenter è progettato per ridurre i tempi medi di risoluzione dei problemi che influiscono sulle AWS risorse. OpsCenter aggrega e standardizza OpsItems tutti i servizi fornendo al contempo dati di indagine contestuali su ciascuna risorsa correlata OpsItem e OpsItems correlata. OpsCenter fornisce anche runbook di Systems Manager Automation che è possibile utilizzare per risolvere rapidamente i problemi. È possibile specificare i dati ricercabili e personalizzati per ogni OpsItem. È inoltre possibile visualizzare i report di riepilogo generati in automatico su OpsItems in base allo stato e all'origine. Per iniziare a utilizzare OpsCenter, apri la [console di Systems Manager](#). Nel pannello di navigazione, scegli OpsCenter.

OpsCenter è integrato con Amazon EventBridge e Amazon CloudWatch. Ciò significa che puoi configurare questi servizi per creare automaticamente un segnale OpsCenter quando un CloudWatch allarme entra OpsItem in ALARM uno stato o quando EventBridge elabora un evento da qualsiasi AWS servizio che pubblica eventi. La configurazione di CloudWatch allarmi ed EventBridge eventi per la creazione automatica OpsItems consente di diagnosticare e risolvere rapidamente i problemi con AWS le risorse da un'unica console.

Per aiutarti a diagnosticare i problemi, ognuno OpsItem include informazioni contestualmente rilevanti come il nome e l'ID della AWS risorsa che ha generato i problemi, i dettagli dell'allarme o dell'eventoOpsItem, la cronologia degli allarmi e un grafico della sequenza temporale degli allarmi.

Per quanto riguarda la AWS risorsa, OpsCenter aggrega informazioni provenienti da AWS Config, AWS CloudTrail registri e Amazon CloudWatch Events, in modo da non dover navigare su più pagine della console durante l'indagine.

L'elenco seguente include i tipi di AWS risorse e metriche per i quali i clienti configurano gli CloudWatch allarmi che creano. OpsItems

- Amazon DynamoDB: le operazioni di lettura e scrittura del database raggiungono una soglia
- Amazon EC2: l'utilizzo della CPU raggiunge una soglia
- AWS fatturazione: gli addebiti stimati raggiungono una soglia
- Amazon EC2: un'istanza ha esito negativo su un controllo dello stato
- Amazon Elastic Block Store (EBS): l'utilizzo dello spazio su disco raggiunge una soglia

L'elenco seguente include i tipi di EventBridge regole che il cliente configura per la creazioneOpsItems.

- AWS Security Hub CSPM: avviso di sicurezza emesso
- DynamoDB: un evento di limitazione (della larghezza di banda della rete)
- Amazon EC2 Auto Scaling: impossibile avviare un'istanza
- Systems Manager: mancata esecuzione di un'automazione
- AWS Health: un avviso per la manutenzione programmata
- EC2: lo stato dell'istanza cambia da Running a Stopped

OpsCenterè inoltre integrato con Amazon CloudWatch Application Insights for .NET e SQL Server. Ciò significa che è possibile creare automaticamente OpsItems per i problemi rilevati nelle applicazioni. Puoi anche integrarlo OpsCenter AWS Security Hub CSPM per aggregare e intervenire sui tuoi problemi di sicurezza, prestazioni e operativi in Systems Manager.

Gli ingegneri operativi e i professionisti IT possono creare, visualizzare e modificare OpsItems utilizzando la OpsCenter pagina nella AWS Systems Manager console, le operazioni API pubbliche, AWS Command Line Interface (AWS CLI) o gli AWS SDK. AWS Tools for Windows PowerShellOpsCenterLe operazioni API pubbliche ti consentono inoltre di integrarti OpsCenter con i tuoi sistemi di gestione dei casi e le dashboard sanitarie.

## Come può OpsCenter avvantaggiare la mia organizzazione?

OpsCenteroffre un'esperienza standard e unificata per visualizzare, lavorare e risolvere i problemi relativi alle AWS risorse. Un'esperienza standard e unificata migliora il tempo necessario per risolvere i problemi, individuare i problemi correlati e preparare nuovi tecnici operativi e professionisti IT. Un'esperienza standard e unificata riduce inoltre il numero di errori manuali immessi nel sistema di gestione e risoluzione dei problemi.

Più precisamente, OpsCenter offre i seguenti vantaggi per i tecnici operativi e le organizzazioni:

- Non è più necessario navigare su più pagine della console per visualizzare, analizzare e risolvere le risorse OpsItems correlate. AWS OpsItem sono aggregati, tra i servizi, in una posizione centrale.
- È possibile visualizzare dati specifici del servizio e contestualmente pertinenti, generati automaticamente da CloudWatch allarmi, EventBridge eventi e CloudWatch Application Insights for OpsItems .NET e SQL Server.
- È possibile specificare l'Amazon Resource Name (ARN) di una risorsa correlata a un OpsItem. Specificando risorse correlate, OpsCenter utilizza una logica incorporata per aiutare a evitare la creazione di duplicati OpsItems.
- È possibile visualizzare dettagli e informazioni sulla risoluzione riguardo a OpsItems simili.
- È possibile visualizzare rapidamente informazioni ed eseguire i runbook di Systems Manager Automation per risolvere problemi.

## Quali sono le funzionalità di OpsCenter?

- Creazione automatica e manuale di OpsItem

OpsCenter è integrato con Amazon CloudWatch. Ciò significa che puoi configurare OpsItem in modo CloudWatch da creare automaticamente un avviso OpsCenter quando un allarme entra in ALARM uno stato o quando Amazon EventBridge elabora un evento da qualsiasi AWS servizio che pubblica eventi. È anche possibile creare manualmente OpsItems.

OpsCenter è inoltre integrato con Amazon CloudWatch Application Insights for .NET e SQL Server. Ciò significa che è possibile creare automaticamente OpsItems per i problemi rilevati nelle applicazioni.

- OpsItems dettagliato e ricercabile

Ciascuno OpsItem include più campi di informazioni, tra cui titolo, ID, priorità, descrizione OpsItem, origine e data dell' ultimo aggiornamento. Ogni OpsItem include inoltre le seguenti funzionalità configurabili:

- Stato: aperto, in corso, risolto oppure aperto e in corso.
- Risorse correlate: una risorsa correlata è la risorsa interessata o la risorsa che ha avviato l' EventBridge evento che ha creato il. OpsItem Ogni OpsItem include una sezione Related resources (Risorse correlate) dove OpsCenter elenca automaticamente l'Amazon Resource Name (ARN) della risorsa correlata. È anche possibile specificare manualmente i nomi ARN di risorse correlate. Per alcuni tipi di ARN, OpsCenter crea automaticamente un deep link che visualizza i dettagli sulle risorse senza dover consultare altre pagine della console per

visualizzare tali informazioni. Ad esempio, se si specifica l'ARN di un'istanza EC2, è possibile visualizzare tutti i EC2-provided dettagli su tale istanza in. OpsCenter È possibile aggiungere manualmente i nomi ARN di altre risorse correlate. Ogni OpsItem può elencare un massimo di 100 ARN di risorse correlate. Per ulteriori informazioni, consulta [Aggiungere risorse correlate a un OpsItem](#).

- **Correlati e simili OpsItems:** con la funzionalità OpsItems correlati, è possibile specificare gli ID di OpsItems che sono in qualche modo legati alla OpsItem corrente. La funzionalità OpsItem simile esegue la revisione automatica di titoli e descrizioni OpsItem e quindi elenca altre OpsItems che potrebbero essere correlate o di tuo interesse.
- **Dati operativi disponibili per la ricerca e privati:** i dati operativi sono i dati personalizzati che forniscono dettagli di riferimento utili riguardo a OpsItem. Ad esempio, è possibile specificare i file di log, le stringhe di errore, le chiavi di licenza, i suggerimenti per la risoluzione dei problemi o altri dati. I dati operativi vengono inseriti come coppie chiave-valore. La chiave deve essere composta da un massimo di 128 caratteri. Il valore ha una dimensione massima di 20 KB.

Questi dati personalizzati sono disponibili per la ricerca, ma con limitazioni. Per la funzione Dati operativi ricercabili, tutti gli utenti con accesso alla pagina Panoramica di OpsItem (grazie all'operazione API [Descrivere OpsItem](#)) possono visualizzare ed effettuare ricerche sui dati specificati. Per la funzione Dati operativi privati, i dati sono visualizzabili solo dagli utenti che hanno accesso a OpsItem (come fornito dall'operazione [GetOpsItem](#) API).

- **Deduplicazione:** specificando le risorse correlate, OpsCenter utilizza una logica incorporata per aiutarti a evitare la creazione di duplicati OpsItems. OpsCenter include anche una funzionalità chiamata approfondimenti sulle operazioni, che visualizza le informazioni sui duplicati OpsItems. Per limitare ulteriormente il numero di duplicati OpsItems nel tuo account, puoi specificare manualmente una stringa di deduplicazione per una regola di evento. EventBridge Per ulteriori informazioni, consulta [Gestione dei OpsItems duplicati](#).
- **Modifica in bloccoOpsItems:** È possibile selezionare più OpsItems nel OpsCenter e modificare uno dei seguenti campi: Stato, Priority (Priorità), Gravità, Categoria.
- **Processo di correzione semplice utilizzando runbook**

Ciascuno OpsItem include una sezione Runbook con un elenco di runbook di Systems Manager Automation che è possibile utilizzare per risolvere automaticamente i problemi più comuni relativi alle risorse. AWS Se ne apri unoOpsItem, scegli una AWS risorsa a tale scopoOpsItem, quindi scegli il pulsante Esegui automazione nella console, quindi OpsCenter fornisce un elenco di runbook di automazione che puoi eseguire sulla AWS risorsa che ha generato il. OpsItem Dopo aver eseguito un runbook Automation da un OpsItem, il runbook viene associato automaticamente

alla risorsa correlata di OpsItem per riferimento futuro. Inoltre, se imposti automaticamente OpsItem le regole EventBridge utilizzando OpsCenter, allora associa EventBridge automaticamente i runbook per gli eventi comuni. OpsCenter mantiene un registro di 30 giorni dei runbook di Automation eseguiti per uno specifico periodo. OpsItem Per ulteriori informazioni, consulta [Rimediare OpsItem problemi](#).

- Modifica notifica: è possibile specificare l'ARN di un argomento Amazon Simple Notification Service (SNS) e pubblicare le notifiche ogni volta che un OpsItem viene cambiato o modificato. L'argomento SNS deve coincidere con. Regione AWS OpsItem
- Ampie funzionalità di ricerca OpsItem: OpsCenter offre diverse opzioni di ricerca per aiutare a individuare OpsItems rapidamente. Seguono alcuni esempi di come è possibile eseguire ricerche: OpsItem ID, titolo, ultima modifica dell'ora, valore dati operativi, origine e ID dell'automazione dell'esecuzione di un runbook sono solo alcuni esempi. È possibile limitare ulteriormente i risultati di ricerca utilizzando filtri di stato.
- Report di riepilogo OpsItem

OpsCenter include una pagina di report di riepilogo che visualizza automaticamente le seguenti sezioni:

- Status summary (Riepilogo dello stato): un riepilogo di OpsItems in base allo stato (aperto, in corso, risolto, aperto e in corso).
- Fonti con più aperture OpsItems: una ripartizione dei principali AWS servizi con apertura. OpsItems
- OpsItems per origine ed età: un conteggio di OpsItems raggruppati per origine e giorni dopo la creazione.

Per ulteriori informazioni sulla visualizzazione dei report di riepilogo OpsCenter, consulta [Visualizzazione dei report di riepilogo OpsCenter](#).

- Supporto delle funzionalità di registrazione e verifica

Puoi controllare e registrare le azioni OpsCenter degli utenti nel tuo account Account AWS tramite l'integrazione con altri AWS servizi. Per ulteriori informazioni, consulta [Visualizzazione di log e report di OpsCenter](#).

- Accesso allo strumento tramite console PowerShell, CLI e SDK OpsCenter

Puoi lavorarci OpsCenter usando la AWS Systems Manager console, AWS Command Line Interface (AWS CLI) o l' AWS SDK di tua scelta. AWS Strumenti per PowerShell



## Lo fa OpsCenter si integra con il mio sistema di gestione dei casi esistente?

OpsCenter è stato progettato per integrare i sistemi di gestione dei casi esistenti. È possibile integrare OpsItems nel sistema di gestione dei casi esistente utilizzando operazioni API pubbliche. È anche possibile mantenere flussi di lavoro manuali del ciclo di vita nei sistemi correnti e utilizzare OpsCenter come hub delle verifiche e del processo di correzione.

Per ulteriori informazioni su operazioni API pubbliche OpsCenter, consulta le seguenti operazioni API nella Documentazione di riferimento API di AWS Systems Manager .

- [CreateOpsItem](#)
- [DescribeOpsItems](#)
- [GetOpsItem](#)
- [GetOpsSummary](#)
- [UpdateOpsItem](#)

## L'utilizzo è a pagamento OpsCenter?

Sì. Per ulteriori informazioni, consulta [AWS Systems Manager Prezzi](#).

## Lo fa OpsCenter funziona con i miei nodi gestiti locali e ibridi?

Sì. È possibile utilizzare OpsCenter per analizzare e risolvere i problemi con i nodi on-premises gestiti e configurati per Systems Manager. Per ulteriori informazioni sulla configurazione di server on-premises e macchine virtuali per Systems Manager, consulta [Gestione dei nodi in ambienti ibridi e multicloud con Systems Manager](#).

## A cosa servono le quote OpsCenter?

È possibile visualizzare le quote per tutti gli strumenti di Systems Manager nella sezione [Service Quotas di Systems Manager](#) nella Riferimenti generali di Amazon Web Services. Salvo diversa indicazione, ogni quota è Region-specific.

## Configurazione di OpsCenter

AWS Systems Manager utilizza un'esperienza di configurazione integrata per aiutarti a iniziare a usare OpsCenter e Explorer quali sono gli strumenti di Systems Manager. Explorer è una dashboard operativa personalizzabile che riporta informazioni sulle AWS risorse. In questa documentazione, la configurazione di Explorer e OpsCenter viene chiamata configurazione integrata.



Per configurare OpsCenter con Explorer, devi utilizzare la configurazione integrata. La configurazione integrata è disponibile solo nella AWS Systems Manager console. Non è possibile impostare Explorer e OpsCenter a livello di programmazione. Per ulteriori informazioni, consulta [Nozioni di base su Systems Manager Explorer e OpsCenter](#).

### Prima di iniziare

Al momento della configurazione OpsCenter, abiliti le regole predefinite in Amazon EventBridge che creano automaticamente OpsItems. La tabella seguente descrive le EventBridge regole predefinite che vengono create automaticamente OpsItems. È possibile disabilitare EventBridge le regole nella pagina OpsCenter Impostazioni alla voce OpsItemRegole.

#### Important

All'account in uso vengono addebitati i costi relativi agli elementi OpsItems creati dalle regole predefinite. Per ulteriori informazioni, consulta la sezione [Prezzi di AWS Systems Manager](#).

| Nome regola                                          | Description                                                                                                                           |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| SSMOpsItems-Autoscaling-instance-launch-failure      | Questa regola crea OpsItems quando l'avvio di un'istanza di dimensionamento automatico EC2 non riesce.                                |
| SSMOpsItems-Autoscaling-instance-termination-failure | Questa regola crea OpsItems quando la chiusura di un'istanza di dimensionamento automatico EC2 non riesce.                            |
| SSMOpsItems-EBS-snapshot-copy-failed                 | Questa regola crea OpsItems quando il sistema non riesce a copiare uno snapshot di Amazon Elastic Block Store (Amazon EBS).           |
| SSMOpsItems-EBS-snapshot-creation-failed             | Questa regola crea OpsItems quando il sistema non riesce a creare uno snapshot di Amazon EBS.                                         |
| SSMOpsItems-EBS-volume-performance-issue             | Questa regola corrisponde a una regola AWS Health di tracciamento. Questa regola crea OpsItems ogni volta che si verifica un problema |

| Nome regola                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                  | di prestazioni con il volume Amazon EBS (evento di integrità = AWS_EBS_DEGRADED_EBS_VOLUME_PERFORMANCE ).                                                                                                                                                                                                                                                                                                                                |
| SSMOpsItems-EC2-issue            | Questa regola corrisponde a una regola di AWS Health tracciamento degli eventi imprevisti che influiscono su AWS servizi o risorse. La regola crea OpsItems quando, ad esempio, un servizio invia comunicazioni su problemi operativi che causano il peggioramento del servizio o per segnalare problemi a livello di risorsa localizzati. Ad esempio, questa regola crea un OpsItem per il seguente evento: AWS_EC2_OPERATIONAL_ISSUE . |
| SSMOpsItems-EC2-scheduled-change | Questa regola corrisponde a una regola AWS Health di tracciamento. AWS può pianificare eventi per le istanze, come il riavvio, l'arresto o l'avvio delle istanze. La regola crea OpsItems per gli eventi pianificati di EC2. Per ulteriori informazioni sugli eventi pianificati, consulta <a href="#">Eventi pianificati per le istanze</a> nella Guida per l'utente di Amazon EC2.                                                     |

| Nome regola                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSMOpsItems-RDS-issue            | <p>Questa regola corrisponde a una regola di AWS Health tracciamento degli eventi imprevisti che influiscono su servizi o risorse. AWS La regola crea OpsItems quando, ad esempio, un servizio invia comunicazioni su problemi operativi che causano il peggioramento del servizio o per segnalare problemi a livello di risorsa localizzati. Ad esempio, questa regola crea un OpsItem per i seguenti eventi: <code>AWS_RDS_MYSQL_DATABASE_CRASHING_REPEATEDLY</code> , <code>AWS_RDS_EXPORT_TASK_FAILED</code> e <code>AWS_RDS_CONNECTIVITY_ISSUE</code> .</p>                                                                                                                                                                                                                                                                                      |
| SSMOpsItems-RDS-scheduled-change | <p>Questa regola corrisponde a una regola AWS Health di tracciamento. La regola crea OpsItems per gli eventi pianificati di Amazon RDS. Gli eventi pianificati forniscono informazioni sulle modifiche imminenti alle risorse Amazon RDS. Alcuni eventi potrebbero consigliarti di agire per evitare interruzioni del servizio. Gli altri eventi si verificano automaticamente senza alcuna azione da parte tua. Durante l'attività di modifica pianificata, la tua risorsa potrebbe essere temporaneamente non disponibile. Ad esempio, questa regola crea un OpsItem per i seguenti eventi: <code>AWS_RDS_SYSTEM_UPGRADE_SCHEDULED</code> e <code>AWS_RDS_MAINTENANCE_SCHEDULED</code> . Per ulteriori informazioni sugli eventi programmati, consulta le <a href="#">Categorie dei tipi di evento</a> nella Guida per l'utente di AWS Health .</p> |

| Nome regola                                           | Description                                                                                                     |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| SSMOpsItems-SSM-maintenance-window-execution-failed   | Questa regola crea OpsItems quando l'elaborazione della finestra di manutenzione di Systems Manager non riesce. |
| SSMOpsItems-SSM-maintenance-window-execution-timedout | Questa regola crea OpsItems quando l'avvio della finestra di manutenzione di Systems Manager va in timeout.     |

Completa la procedura seguente per configurare OpsCenter.

### Configurazione di OpsCenter

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli OpsCenter.
3. Nella home page di OpsCenter, scegli Inizia.
4. Nella pagina di OpsCenter configurazione, scegli Abilita questa opzione per fare in modo che CloudWatch gli eventi di Explorer configurazione AWS Config e Amazon vengano creati automaticamente in OpsItems base a regole ed eventi di uso comune. Se non scegli questa opzione, OpsCenter rimane disattivato.

#### Note

Amazon EventBridge (precedentemente Amazon CloudWatch Events) fornisce tutte le funzionalità di CloudWatch Events e alcune nuove funzionalità, come bus di eventi personalizzati, fonti di eventi di terze parti e registro degli schemi.

5. Scegli Abilita OpsCenter.

Dopo l'abilitazione di OpsCenter, puoi eseguire le operazioni seguenti da Impostazioni:

- Crea CloudWatch allarmi utilizzando il pulsante Apri CloudWatch console. Per ulteriori informazioni, consulta [Configura CloudWatch gli allarmi per creare OpsItems](#).

- Attiva gli approfondimenti operativi. Per ulteriori informazioni, consulta [Analisi delle informazioni operative per ridurre OpsItems](#).
- Abilita gli AWS Security Hub CSPM allarmi relativi ai risultati. Per ulteriori informazioni, consulta [Comprensione OpsCenter integrazione con AWS Security Hub CSPM](#).

## Indice

- [\(Facoltativo\) Configurazione OpsCenter per gestire centralmente OpsItems tra gli account](#)
- [\(Facoltativo\) Configura Amazon SNS per ricevere notifiche su OpsItems](#)

### (Facoltativo) Configurazione OpsCenter per gestire centralmente OpsItems tra gli account

È possibile utilizzare Systems Manager OpsCenter per la gestione OpsItems centralizzata di più Account AWS utenti in uno selezionato Regione AWS. Questa funzionalità è disponibile dopo aver configurato l'organizzazione in AWS Organizations. AWS Organizations è un servizio di gestione degli account che consente di consolidare più AWS account in un'organizzazione creata e gestita centralmente. AWS Organizations include funzionalità di gestione degli account e fatturazione consolidata che consentono di soddisfare meglio le esigenze di budget, sicurezza e conformità della tua azienda. Per ulteriori informazioni, vedi [Che cos'è? AWS Organizations](#) nella Guida per l'AWS Organizations utente

Gli utenti che appartengono all'account di AWS Organizations gestione possono configurare un account amministratore delegato per Systems Manager. Nel contesto di OpsCenter, gli amministratori delegati possono creare, modificare e visualizzare OpsItems negli account dei membri. L'amministratore delegato può anche utilizzare i runbook di Systems Manager Automation per risolvere OpsItems o rimediare in blocco ai problemi relativi alle AWS risorse in fase di generazione. OpsItems

#### Note

È possibile assegnare un solo account come amministratore delegato per Systems Manager. Per ulteriori informazioni, consulta [Creare un AWS Organizations amministratore delegato per Systems Manager](#).

Systems Manager offre i seguenti metodi di configurazione di OpsCenter per la gestione centralizzata di OpsItems su più Account AWS.

- Configurazione rapida: configurazione rapida, uno strumento di Systems Manager, semplifica le attività di installazione e configurazione per gli strumenti di Systems Manager. Per ulteriori informazioni, consulta [AWS Systems Manager Configurazione rapida](#).

Configurazione rapida per OpsCenter consente di completare le seguenti attività per la gestione di OpsItems su più account:

- Registrazione di un account come amministratore delegato (se l'amministratore delegato non è già stato designato)
- Creazione di policy e ruoli obbligatori AWS Identity and Access Management (IAM)
- Specificare un' AWS Organizations organizzazione o unità organizzative (OU) in cui un amministratore delegato può gestire OpsItems più account

Per ulteriori informazioni, consulta [\(Facoltativo\) Configura OpsCenter da gestire OpsItems tra gli account utilizzando Configurazione rapida](#).

#### Note

La configurazione rapida non è disponibile in tutte le aree in Regioni AWS cui Systems Manager è attualmente disponibile. Se Configurazione rapida non è disponibile in una regione in cui desideri utilizzarla per configurare OpsCenter per la gestione centralizzata su più account di OpsItems, devi utilizzare il metodo manuale. Per visualizzare un elenco di Regioni AWS dove è disponibile Quick Setup, vedere [Disponibilità di Configurazione rapida in Regioni AWS](#).

- Configurazione manuale: se Configurazione rapida non è disponibile nella Regione in cui desideri configurare OpsCenter per la gestione centralizzata di OpsItems su più account, puoi utilizzare la procedura manuale a tale scopo. Per ulteriori informazioni, consulta [\(Facoltativo\) Configurazione manuale OpsCenter per gestire centralmente OpsItems tra gli account](#).

(Facoltativo) Configura OpsCenter da gestire OpsItems tra gli account utilizzando Configurazione rapida

Quick Setup semplifica le attività di installazione e configurazione per gli strumenti di Systems Manager. Quick Setup for OpsCenter consente di completare le seguenti attività per la gestione di OpsItems più account:

- Definizione dell'account di amministratore delegato

- Creazione delle policy e dei ruoli obbligatori AWS Identity and Access Management (IAM)
- Specificare un' AWS Organizations organizzazione o un sottoinsieme di account membri, in cui un amministratore delegato può gestire tutti gli account OpsItems

Quando configuri OpsCenter per gestire OpsItems su più account utilizzando Configurazione rapida, Quick Setup crea le seguenti risorse negli account specificati. Queste risorse consentono agli account specificati di utilizzare OpsItems e utilizzare i runbook di Automation per risolvere i problemi relativi alla generazione delle risorse. AWS OpsItems

| Resources                                                                                                                                                                                                                                                                              | Account                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| <p>AWSServiceRoleForAmazonSSM_AccountDiscovery Ruolo collegato al servizio (IAM) AWS Identity and Access Management</p> <p>Per ulteriori informazioni su questo ruolo, consulta <a href="#">Usare i ruoli per raccogliere Account AWS informazioni per OpsCenter and Explorer.</a></p> | <p>AWS Organizations account di gestione e account amministratore delegato</p> |
| <p>Ruolo IAM OpsItem-CrossAccountManagementRole</p> <p>AWS-SystemsManager-AutomationAdministrationRole Ruolo IAM</p>                                                                                                                                                                   | <p>Account amministratore delegato</p>                                         |
| <p>OpsItem-CrossAccountExecutionRole Ruolo IAM</p> <p>AWS-SystemsManager-AutomationExecutionRole Ruolo IAM</p> <p>AWS::SSM::ResourcePolicy Policy delle risorse di Systems Manager per il gruppo OpsItem predefinito (OpsItemGroup )</p>                                               | <p>Tutti gli account AWS Organizations dei membri</p>                          |

 Note

Se in precedenza hai configurato OpsCenter la gestione OpsItems di più account utilizzando il metodo [manuale](#), devi eliminare gli AWS CloudFormation stack o gli stack set creati durante i passaggi 4 e 5 di tale processo. Se tali risorse sono presenti nel tuo account quando completi la seguente procedura, Quick Setup non riesce a configurare correttamente la gestione multi-account di OpsItem.

Per configurare OpsCenter da gestire OpsItems tra gli account utilizzando Quick Setup

1. Accedi a Console di gestione AWS utilizzando l'account AWS Organizations di gestione.
2. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
3. Nel pannello di navigazione, scegli Quick Setup.
4. Scegli la scheda Libreria.
5. Scorri verso il basso e individua il riquadro di configurazione OpsCenter. Scegli Create (Crea).
6. Nella pagina Quick Setup OpsCenter, nella sezione Amministratore delegato, inserisci un ID account. Se non è possibile modificare questo campo, è già stato specificato un account amministratore delegato per Systems Manager.
7. Nella sezione Targets (Destinazioni), scegliere un'opzione. Se scegli Personalizzato, seleziona le unità organizzative (UO) dove desideri gestire OpsItems su più account.
8. Scegli Create (Crea).

Quick Setup crea la configurazione OpsCenter e distribuisce le risorse AWS richieste nelle unità organizzative designate.

 Note

Se non desideri gestire OpsItems su più account, puoi eliminare la configurazione da Quick Setup. Quando elimini la configurazione, Quick Setup elimina le seguenti policy e ruoli IAM creati quando la configurazione è stata originariamente distribuita:

- OpsItem-CrossAccountManagementRole dall'account di amministratore delegato
- OpsItem-CrossAccountExecutionRole e SSM::ResourcePolicy da tutti gli account dei membri di Organizations



Quick Setup rimuove la configurazione da tutte le unità organizzative e dalle Regioni AWS su cui è stata originariamente distribuita.

## Risoluzione dei problemi relativi a Configurazione rapida configurazione per OpsCenter

Questa sezione include informazioni per aiutarti a risolvere i problemi relativi alla configurazione della gestione multi-account di OpsItem tramite Quick Setup.

### Argomenti

- [La distribuzione su questi StackSets non è riuscita: DelegatedAdmin](#)
- [Configurazione rapida lo stato di configurazione indica Non riuscito](#)

### La distribuzione su questi StackSets non è riuscita: DelegatedAdmin

Quando si crea una configurazione OpsCenter, Quick Setup distribuisce due set di stack AWS CloudFormation nell'account di gestione di Organizations. I set di stack utilizzano il seguente prefisso: `AWS-QuickSetup-SSMOpsCenter`. Se Quick Setup visualizza il seguente errore: `Deployment to these StackSets failed: delegatedAdmin` utilizza la seguente procedura per risolvere questo problema.

### Per risolvere un errore fallito: DelegatedAdmin StackSets

1. Se hai ricevuto l'`Deployment to these StackSets failed: delegatedAdmin` errore in un banner rosso nella Quick Setup console, accedi all'account amministratore delegato e all'area designata come area geografica principale. Regione AWS Quick Setup
2. Apri la CloudFormation console all'indirizzo. <https://console.aws.amazon.com/cloudformation>
3. Scegli lo stack creato dalla configurazione di Quick Setup. Il nome dello stack include quanto segue: `AWS-QuickSetup-SSMOpsCenter`.

#### Note

A volte CloudFormation elimina le distribuzioni di stack non riuscite. Se lo stack non è disponibile nella tabella Stacks (Stack), scegli Deleted (Eliminato) dall'elenco dei filtri.

4. Controlla Status (Stato) e Status reason (Motivo dello stato). Per ulteriori informazioni sugli stati dello stack, consulta [Codici di stato dello stack](#) nella Guida per l'utente di AWS CloudFormation .
5. Per individuare il passaggio esatto non riuscito, controlla la scheda Events (Eventi) e rivedi lo Status (Stato) di ciascun evento. Per ulteriori informazioni, consulta la sezione [Risoluzione dei problemi](#) nella Guida per l'utente di AWS CloudFormation .

 Note

Se non riesci a risolvere l'errore di distribuzione utilizzando la procedura di CloudFormation risoluzione dei problemi, elimina la configurazione e riprova.

Configurazione rapida lo stato di configurazione indica Non riuscito

Se la tabella dei dettagli di configurazione nella pagina dei dettagli di configurazione mostra lo stato della configurazione Failed, accedi alla Account AWS regione in cui non è riuscito.

Per risolvere un problema Configurazione rapida mancata creazione di un OpsCenter configurazione

1. Accedere al sito Account AWS in Regione AWS cui si è verificato l'errore.
2. Apri la CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
3. Scegli lo stack creato dalla configurazione di Quick Setup. Il nome dello stack include quanto segue: AWS-QuickSetup-SSMOpsCenter.

 Note

A volte CloudFormation elimina le distribuzioni di stack non riuscite. Se lo stack non è disponibile nella tabella Stacks (Stack), scegli Deleted (Eliminato) dall'elenco dei filtri.

4. Controlla Status (Stato) e Status reason (Motivo dello stato). Per ulteriori informazioni sugli stati dello stack, consulta [Codici di stato dello stack](#) nella Guida per l'utente di AWS CloudFormation .
5. Per individuare il passaggio esatto non riuscito, controlla la scheda Events (Eventi) e rivedi lo Status (Stato) di ciascun evento. Per ulteriori informazioni, consulta la sezione [Risoluzione dei problemi](#) nella Guida per l'utente di AWS CloudFormation .

La configurazione dell'account membro mostra ResourcePolicyLimitExceededException

Se lo stato dello stack mostra ResourcePolicyLimitExceededException, l'account è già passato alla gestione multi-account di OpsCenter utilizzando il [metodo manuale](#). Per risolvere questo problema, è necessario eliminare gli AWS CloudFormation stack o gli stack set creati durante i passaggi 4 e 5 del processo di onboarding manuale. Per ulteriori informazioni, consulta [Eliminare uno stack set](#) ed [Eliminare uno stack sulla CloudFormation console](#) nella Guida per l'utente. AWS CloudFormation

(Facoltativo) Configurazione manuale OpsCenter per gestire centralmente OpsItems tra gli account

Questa sezione descrive come configurare manualmente OpsCenter per la gestione multi-account di OpsItem. Sebbene questo processo sia ancora supportato, è stato sostituito da un processo più recente che utilizza Quick Setup di Systems Manager. Per ulteriori informazioni, consulta [\(Facoltativo\) Configura OpsCenter da gestire OpsItems tra gli account utilizzando Configurazione rapida](#).

Puoi configurare un account centrale per creare manualmente OpsItems per gli account membri e per gestire e correggere tali OpsItems. L'account centrale può essere l'account di AWS Organizations gestione o sia l'account di AWS Organizations gestione che l'account amministratore delegato di Systems Manager. Si consiglia di utilizzare l'account amministratore delegato di Systems Manager come account centrale. È possibile utilizzare questa funzionalità solo dopo la configurazione di AWS Organizations.

Con AWS Organizations, puoi consolidarne più Account AWS in un'organizzazione che crei e gestisci centralmente. L'utente dell'account centrale può creare contemporaneamente OpsItems per tutti gli account dei membri selezionati e gestire questi OpsItems.

Utilizza la procedura descritta in questa sezione per abilitare l'entità del servizio Systems Manager in Organizations e configurare le autorizzazioni AWS Identity and Access Management (IAM) per l'utilizzo con OpsItems più account.

## Argomenti

- [Prima di iniziare](#)
- [Passaggio 1: Creazione di una sincronizzazione dati dei dati delle risorse](#)
- [Fase 2: Abilitazione del responsabile del servizio Systems Manager in AWS Organizations](#)
- [Fase 3: creazione del ruolo AWSServiceRoleForAmazonSSM \\_ AccountDiscovery service-linked](#)
- [Fase 4: Configurazione delle autorizzazioni con cui lavorare OpsItems tra gli account](#)

- [Passaggio 5: Configurazione delle autorizzazioni per lavorare con le risorse correlate su più account](#)

#### Note

Il supporto è fornito solo a OpsItems di tipo `/aws/issue` durante l'utilizzo di OpsCenter su più account.

## Prima di iniziare

Prima di OpsCenter configurare l'utilizzo con OpsItems più account, assicurati di aver impostato quanto segue:

- Un account di amministratore delegato per Systems Manager. Per ulteriori informazioni, consulta [Configurazione di un amministratore delegato per Explorer](#).
- Un'organizzazione impostata e configurata in Organizations. Per ulteriori informazioni, consulta [Creazione e gestione di un'organizzazione](#) nella Guida per l'utente di AWS Organizations .
- Hai configurato Systems Manager Automation per eseguire runbook di automazione su più Regioni AWS AWS account. Per ulteriori informazioni, consulta [Esecuzione di automazioni in più Regioni AWS e account](#).

## Passaggio 1: Creazione di una sincronizzazione dati dei dati delle risorse

Dopo aver impostato e configurato AWS Organizations, puoi aggregare OpsItems i dati OpsCenter per un'intera organizzazione creando una sincronizzazione dei dati delle risorse. Per ulteriori informazioni, consulta [Creazione di una sincronizzazione dati dei dati delle risorse](#). Quando crei la sincronizzazione, nella sezione Aggiungi account, assicurati di scegliere l'opzione Includi tutti gli account dalla mia configurazione AWS Organizations .

## Fase 2: Abilitazione del responsabile del servizio Systems Manager in AWS Organizations

Per consentire a un utente di lavorare con OpsItems più account, è necessario abilitare l'entità del servizio Systems Manager AWS Organizations. Se in precedenza hai configurato Systems Manager per scenari con multi-account utilizzando altri strumenti, il principale del servizio Systems Manager potrebbe essere già configurato in Organizations. Per verificarlo, esegui i comandi seguenti nella AWS Command Line Interface (AWS CLI). Se non hai configurato Systems Manager per altri scenari

multi-account, passa alla procedura successiva, Abilitazione del principale del servizio Systems Manager in AWS Organizations.

Per verificare che il responsabile del servizio Systems Manager sia abilitato in AWS Organizations

1. [Scarica](#) la versione più recente AWS CLI di sul tuo computer locale.
2. Apri ed AWS CLI esegui il seguente comando per specificare le tue credenziali e un Regione AWS.

```
aws configure
```

Il sistema richiede di specificare quanto segue. Nel seguente esempio, sostituisci ciascuno *user input placeholder* con le tue informazioni.

```
AWS Access Key ID [None]: key_name
AWS Secret Access Key [None]: key_name
Default region name [None]: region
Default output format [None]: ENTER
```

3. Esegui il seguente comando per verificare che il principale del servizio Systems Manager sia abilitato in AWS Organizations.

```
aws organizations list-aws-service-access-for-organization
```

Il comando restituisce informazioni simili a quelle mostrate nell'esempio seguente.

```
{
 "EnabledServicePrincipals": [
 {
 "ServicePrincipal":
"member.org.stacksets.cloudformation.amazonaws.com",
 "DateEnabled": "2020-12-11T16:32:27.732000-08:00"
 },
 {
 "ServicePrincipal": "opsdatasync.ssm.amazonaws.com",
 "DateEnabled": "2022-01-19T12:30:48.352000-08:00"
 },
 {
 "ServicePrincipal": "ssm.amazonaws.com",
 "DateEnabled": "2020-12-11T16:32:26.599000-08:00"
 }
]
}
```

```
}
]
}
```

Per abilitare il responsabile del servizio Systems Manager in AWS Organizations

Se in precedenza non hai configurato il principale del servizio Systems Manager per Organizations, utilizza la procedura seguente. Per ulteriori informazioni su questo comando, consulta [enable-aws-service-access](#) nel Riferimento ai comandi AWS CLI .

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto. Per informazioni, consulta le pagine [Installazione della CLI](#) e [Configurazione della CLI](#).
2. [Scarica](#) la versione più recente AWS CLI di sul tuo computer locale.
3. Apri ed AWS CLI esegui il seguente comando per specificare le tue credenziali e un Regione AWS.

```
aws configure
```

Il sistema richiede di specificare quanto segue. Nel seguente esempio, sostituisci ciascuno *user input placeholder* con le tue informazioni.

```
AWS Access Key ID [None]: key_name
AWS Secret Access Key [None]: key_name
Default region name [None]: region
Default output format [None]: ENTER
```

4. Esegui il seguente comando per abilitare il principale del servizio Systems Manager per AWS Organizations.

```
aws organizations enable-aws-service-access --service-principal "ssm.amazonaws.com"
```

Fase 3: creazione del ruolo **AWSServiceRoleForAmazonSSM \_ AccountDiscovery** service-linked

Un ruolo collegato al servizio come il **AWSServiceRoleForAmazonSSM\_AccountDiscovery** ruolo è un tipo unico di ruolo IAM collegato direttamente a un Servizio AWS, ad esempio Systems Manager. Service-linked i ruoli sono predefiniti dal servizio e includono tutte le autorizzazioni richieste

dal servizio per chiamare altri Servizi AWS per conto dell'utente. Per ulteriori informazioni sul ruolo collegato al servizio `AWSServiceRoleForAmazonSSM_AccountDiscovery`, consulta [Service-linked autorizzazioni di ruolo per Systems Manager individuazione dell'account](#).

Utilizza la procedura seguente per creare il ruolo collegato al servizio `AWSServiceRoleForAmazonSSM_AccountDiscovery` utilizzando la AWS CLI. Per ulteriori informazioni sul comando utilizzato in questa procedura, consulta [create-service-linked-role](#) nel Riferimento ai comandi AWS CLI .

### Per creare il ruolo **AWSServiceRoleForAmazonSSM \_ collegato al servizio AccountDiscovery**

1. Accedi all'account di AWS Organizations gestione.
2. Dopo aver effettuato l'accesso all'account di gestione di Organizations, esegui il comando seguente.

```
aws iam create-service-linked-role \
 --aws-service-name accountdiscovery.ssm.amazonaws.com \
 --description "Systems Manager account discovery for AWS Organizations service-linked role"
```

### Fase 4: Configurazione delle autorizzazioni con cui lavorare OpsItems tra gli account

Usa AWS CloudFormation gli stackset per creare una policy sulle `OpsItemGroup` risorse e un ruolo di esecuzione IAM che consentano agli utenti di lavorare con OpsItems più account. Per iniziare, scarica e decomprimi il file [OpsCenterCrossAccountMembers.zip](#). Questo file contiene il file `OpsCenterCrossAccountMembers.yaml` CloudFormation modello. Quando si crea uno stack set utilizzando questo modello, CloudFormation vengono creati automaticamente la politica `OpsItemCrossAccountResourcePolicy` delle risorse e il ruolo di `OpsItemCrossAccountExecutionRole` esecuzione nell'account. Per ulteriori informazioni sulla creazione di un set di stack, consulta [Creazione di un set di stack](#) nella Guida per l'utente di AWS CloudFormation .

#### Important

Prendi nota delle seguenti informazioni importanti per questa attività:

- Il set di stack deve essere implementato dopo aver effettuato l'accesso all'account di gestione di AWS Organizations .

- Devi ripetere questa procedura dopo aver effettuato l'accesso a tutti gli account scelti come destinazione per utilizzare OpsItems su più account, incluso l'account di amministratore delegato.
- Se desideri abilitare l'OpsItemsamministrazione tra account diversi Regioni AWS, scegli Aggiungi tutte le regioni nella sezione Specifica le regioni del modello. Cross-accountOpsIteml'amministrazione non è supportata per le regioni con opt-in.

## Passaggio 5: Configurazione delle autorizzazioni per lavorare con le risorse correlate su più account

Un OpsItem può includere informazioni dettagliate sulle risorse interessate, ad esempio istanze Amazon Elastic Compute Cloud (Amazon EC2) o bucket Amazon Simple Storage Service (Amazon S3). Il ruolo di esecuzione `OpsItemCrossAccountExecutionRole`, creato nel precedente Passaggio 4, fornisce a OpsCenter le autorizzazioni di sola lettura che gli account membri possono utilizzare per visualizzare le risorse correlate. È inoltre necessario creare un ruolo IAM per fornire agli account di gestione il permesso di visualizzare e interagire con le risorse correlate, che si completano in questa attività.

Per iniziare, scarica e decomprimi il file [OpsCenterCrossAccountManagementRole.zip](#). Questo file contiene il file `OpsCenterCrossAccountManagementRole.yaml` CloudFormation modello. Quando crei uno stack utilizzando questo modello, crea CloudFormation automaticamente il ruolo `OpsCenterCrossAccountManagementRole` IAM nell'account. Per ulteriori informazioni sulla creazione di uno stack, consulta [Creazione di uno stack sulla AWS CloudFormation console](#) nella Guida per l'AWS CloudFormation utente.

### Important

Prendi nota delle seguenti informazioni importanti per questa attività:

- Se prevedi di specificare un account come amministratore delegato perOpsCenter, assicurati di specificarlo Account AWS quando crei lo stack.
- Devi eseguire questa procedura dopo aver effettuato l'accesso all'account di gestione di AWS Organizations e ancora una volta dopo aver effettuato l'accesso all'account di amministratore delegato.



## (Facoltativo) Configura Amazon SNS per ricevere notifiche su OpsItems

È possibile configurare OpsCenter per l'invio di notifiche a un argomento Amazon Simple Notification Service (Amazon SNS), quando il sistema crea un nuovo OpsItem o aggiorna un OpsItem esistente.

Completa i passaggi seguenti per ricevere notifiche sugli OpsItems.

- [Passaggio 1: Creazione e abbonamento a un argomento Amazon SNS](#)
- [Passaggio 2: Aggiornamento della policy di accesso Amazon SNS](#)
- [Fase 3: Aggiornamento di AWS KMS policy d'accesso](#)

### Note

Se attivi la crittografia lato server AWS Key Management Service (AWS KMS) nel passaggio 2, devi completare il passaggio 3. In caso contrario, puoi andare al passaggio 3.

- [Fase 4: Attivazione dell'impostazione predefinita OpsItems regole per inviare notifiche per nuovi utenti OpsItems](#)

### Passaggio 1: Creazione e abbonamento a un argomento Amazon SNS

Per ricevere notifiche, è necessario creare ed effettuare la sottoscrizione a un argomento Amazon SNS. Per ulteriori informazioni, consulta [Creazione di un argomento Amazon SNS](#) e [Iscrizione a un argomento Amazon SNS](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service.

### Note

Se utilizzi OpsCenter più Regioni AWS account, devi creare e sottoscrivere un argomento Amazon SNS in ogni regione o account in cui desideri ricevere notifiche. OpsItem

### Passaggio 2: Aggiornamento della policy di accesso Amazon SNS

È necessario associare un argomento di Amazon SNS a OpsItems. Utilizza la procedura seguente per configurare la policy di accesso Amazon SNS in modo che Systems Manager possa pubblicare notifiche OpsItems nell'argomento Amazon SNS creato nella Fase 1.

1. Accedi Console di gestione AWS e apri la console Amazon SNS all'indirizzo. <https://console.aws.amazon.com/sns/v3/home>

2. Nel pannello di navigazione, scegli Argomenti.
3. Scegli l'argomento creato nel Passaggio 1, quindi scegli Modifica.
4. Espandi Policy di accesso.
5. Aggiungi il seguente blocco Sid alla policy esistente. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
{
 "Sid": "Allow OpsCenter to publish to this topic",
 "Effect": "Allow",
 "Principal": {
 "Service": "ssm.amazonaws.com"
 },
 "Action": "SNS:Publish",
 "Resource": "arn:aws:sns:region:account ID:topic name", // Account ID of the
 SNS topic owner
 "Condition": {
 "StringEquals": {
 "AWS:SourceAccount": "account ID" // Account ID of the OpsItem owner
 }
 }
}
```

#### Note

La chiave di condizione globale `aws:SourceAccount` protegge dallo scenario “confused deputy”. Per utilizzare questa chiave di condizione, imposta il valore sull'ID account del proprietario di OpsItem. Per ulteriori informazioni, consulta [Confused Deputy](#) nella Guida per l'utente IAM.

6. Scegli Salva modifiche.

Il sistema invia ora notifiche all'argomento Amazon SNS quando OpsItems vengono creati o aggiornati.

 Important

Se configuri l'argomento Amazon SNS con una chiave di crittografia lato server AWS Key Management Service (AWS KMS) nella Fase 2, completa la Fase 3. In caso contrario, puoi andare al passaggio 3.

## Fase 3: Aggiornamento di AWS KMS policy d'accesso

Se hai attivato la AWS KMS crittografia lato server per il tuo argomento Amazon SNS, devi anche aggiornare la politica di accesso dell'argomento AWS KMS key che hai scelto al momento della configurazione dell'argomento. Utilizza la procedura seguente per aggiornare la policy di accesso in modo che Systems Manager possa pubblicare notifiche OpsItem nell'argomento Amazon SNS creato nel Passaggio 1.

 Note

OpsCenter non supporta la pubblicazione di OpsItems in un argomento Amazon SNS configurato con una Chiave gestita da AWS.

1. Apri la console all' AWS KMS indirizzo. <https://console.aws.amazon.com/kms>
2. Per modificare il Regione AWS, usa il selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Scegli l'ID della chiave KMS selezionata al momento della creazione dell'argomento.
5. Nella sezione Policy della chiave, scegli Passa alla visualizzazione della policy.
6. Scegli Modifica.
7. Aggiungi il seguente blocco Sid alla policy esistente. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
{
 "Sid": "Allow OpsItems to decrypt the key",
 "Effect": "Allow",
 "Principal": {
 "Service": "ssm.amazonaws.com"
 },
}
```

```

 "Action": ["kms:Decrypt", "kms:GenerateDataKey*"],
 "Resource": "arn:aws:kms:region:account ID:key/key ID"
 }

```

Nell'esempio seguente, il nuovo blocco viene immesso alla riga 14.



8. Scegli Save changes (Salva modifiche).

Fase 4: Attivazione dell'impostazione predefinita OpsItems regole per inviare notifiche per nuovi utenti OpsItems

OpsItemsLe regole predefinite in Amazon EventBridge non sono configurate con un Amazon Resource Name (ARN) per le notifiche Amazon SNS. Utilizza la procedura seguente per modificare una regola in EventBridge e immettere un blocco notifications.

Per aggiungere un blocco di notifiche a un blocco predefinito OpsItem regola

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli OpsCenter.
3. Scegli la scheda OpsItems, quindi seleziona Configura origini.
4. Scegli il nome della regola di origine che desideri configurare con un blocco notifications, come illustrato nell'esempio seguente.

| OpsItem rules                                        |              |          |         | Edit |
|------------------------------------------------------|--------------|----------|---------|------|
| Rule                                                 | Category     | Severity | State   |      |
| SSMOpsItems-Autoscaling-instance-launch-failure      | Availability | 2-High   | enabled |      |
| SSMOpsItems-Autoscaling-instance-termination-failure | Availability | 2-High   | enabled |      |
| SSMOpsItems-EBS-snapshot-copy-failed                 | Availability | 2-High   | enabled |      |
| SSMOpsItems-EBS-snapshot-creation-failed             | Availability | 2-High   | enabled |      |
| SSMOpsItems-EBS-volume-performance-issue             | Performance  | 3-Medium | enabled |      |
| SSMOpsItems-EC2-issue                                | Availability | 2-High   | enabled |      |

La regola si apre in Amazon EventBridge.

5. Nella pagina dei dettagli della regola, nella scheda Destinazioni, scegli Modifica.
6. Nella sezione Impostazioni aggiuntive, scegli Configura il trasformatore di input.
7. Nella casella Modello, aggiungi un blocco notifications nel seguente formato.

```
"notifications": [{"arn": "arn:aws:sns:region:account ID:topic name"}],
```

Ecco un esempio:

```
"notifications": [{"arn": "arn:aws:sns:us-west-2:1234567890:MySNSTopic"}],
```

Inserisci il blocco delle notifiche prima del blocco resources, come mostrato nel seguente esempio per la Regione Stati Uniti occidentali (Oregon) (us-west-2).

```
{
 "title": "EBS snapshot copy failed",
 "description": "CloudWatch Event Rule SSM0psItems-EBS-snapshot-copy-failed was triggered. Your EBS snapshot copy has failed. See below for more details.",
 "category": "Availability",
 "severity": "2",
 "source": "EC2",
 "notifications": [{
 "arn": "arn:aws:sns:us-west-2:1234567890:MySNSTopic"
 }],
 "resources": <resources>,
 "operationalData": {
 "/aws/dedup": {
 "type": "SearchableString",
 "value": "{\\"dedupString\\":\\"SSM0psItems-EBS-snapshot-copy-failed\\"}"
 },
 "/aws/automations": {
 "value": "[{ \\"automationType\\": \\"AWS:SSM:Automation\\",
 \\"automationId\\": \\"AWS-CopySnapshot\\" }]"
 },
 "failure-cause": {
 "value": <failure - cause>
 },
 "source": {
 "value": <source>
 },
 },
}
```

```
 "start-time": {
 "value": <start - time>
 },
 "end-time": {
 "value": <end - time>
 }
 }
}
```

8. Scegli Conferma.
9. Scegli Successivo.
10. Scegli Next (Successivo).
11. Scegli Aggiorna regola.

La prossima volta che il sistema crea un OpsItem per la regola predefinita, pubblica una notifica nell'argomento Amazon SNS.

## Integra OpsCenter con altri Servizi AWS

OpsCenter si integra con più sistemi Servizi AWS per diagnosticare e risolvere i problemi con AWS le risorse. È necessario configurarlo Servizio AWS prima di integrarlo con. OpsCenter

Per impostazione predefinita, i seguenti elementi Servizi AWS sono integrati OpsCenter e possono essere creati OpsItems automaticamente:

- [Amazon CloudWatch](#)
- [Amazon CloudWatch Application Insights](#)
- [Amazon EventBridge](#)
- [AWS Config](#)
- [Strumento di gestione degli incidenti AWS Systems Manager](#)

I seguenti servizi devono essere integrati con OpsCenter per creare automaticamente OpsItems:

- [DevOpsGuru di Amazon](#)
- [AWS Security Hub CSPM](#)

Quando uno di questi servizi crea un OpsItem, puoi gestire e correggere l'OpsItem da OpsCenter. Per ulteriori informazioni, consultare [Manage \(Gestione\) OpsItems](#) e [Rimediare OpsItem problemi](#).

Per ulteriori informazioni su ciascuno di essi Servizio AWS e su come si integraOpsCenter, consulta i seguenti argomenti.

## Argomenti

- [Comprensione OpsCenter integrazione con Amazon CloudWatch](#)
- [Comprensione OpsCenter integrazione con Amazon CloudWatch Application Insights](#)
- [Comprensione OpsCenter integrazione con Amazon DevOps Guru](#)
- [Comprensione OpsCenter integrazione con Amazon EventBridge](#)
- [Comprensione OpsCenter integrazione con AWS Config](#)
- [Comprensione OpsCenter integrazione con AWS Security Hub CSPM](#)
- [Comprensione OpsCenter integrazione con Incident Manager](#)

## Comprensione OpsCenter integrazione con Amazon CloudWatch

Amazon CloudWatch monitora AWS le tue risorse e i tuoi servizi e visualizza le metriche su ogni cosa Servizio AWS che utilizzi. CloudWatch crea un avviso OpsItem quando un allarme entra in stato di allarme. Ad esempio, puoi configurare un allarme per creare in automatico un OpsItem se c'è un picco di errori HTTP generati da Application Load Balancer.

Alcuni allarmi che è possibile configurare CloudWatch per la creazione OpsItems sono riportati nell'elenco seguente:

- Amazon DynamoDB: le operazioni di lettura e scrittura del database raggiungono una soglia
- Amazon EC2: l'utilizzo della CPU raggiunge una soglia
- AWS fatturazione: gli addebiti stimati raggiungono una soglia
- Amazon EC2: un'istanza ha esito negativo su un controllo dello stato
- Amazon Elastic Block Store (EBS): l'utilizzo dello spazio su disco raggiunge una soglia

Puoi creare un avviso o modificare un avviso esistente per creare un OpsItem. Per ulteriori informazioni, consulta [Configura CloudWatch gli allarmi per creare OpsItems](#).

Quando si abilita OpsCenter l'utilizzo di Integrated Setup, si integra con. CloudWatch OpsCenter

## Comprensione OpsCenter integrazione con Amazon CloudWatch Application Insights

Utilizzando Amazon CloudWatch Application Insights, puoi configurare i monitor più appropriati per le risorse delle tue applicazioni per analizzare continuamente i dati per individuare eventuali segni di problemi con le tue applicazioni. Quando configuri le risorse delle CloudWatch applicazioni in Application Insights, puoi scegliere di far creare OpsItems il sistemaOpsCenter. Un OpsItem viene creato sulla console OpsCenter per ogni problema rilevato con l'applicazione. Per informazioni, consulta [Configurare, configurare e gestire l'applicazione per il monitoraggio](#) nella Amazon CloudWatch User Guide.

### Note

A partire dal 16 ottobre 2023, il titolo e la descrizione CloudWatch dell'applicazione OpsItems creata da Application Insights ora utilizzano il seguente formato migliorato:

```
OpsItem title: [<APPLICATION NAME>: <RESOURCE ID>] <PROBLEM SUMMARY>
```

```
OpsItem description:
```

```
CloudWatch Application Insights has detected a problem in application <APPLICATION NAME>.
```

```
Problem summary: <PROBLEM SUMMARY>
```

```
Problem ID: <PROBLEM ID> (hyperlinks to the Application Insights problem summary page)
```

```
Problem Status: <PROBLEM STATUS>
```

```
Insight: <INSIGHT>
```

Ecco un esempio:



AWS Systems Manager > OpsCenter > [exampleApplication: exampleCluster] ECS: Network received bytes

[exampleApplication: exampleCluster] ECS: Network received bytes

Open

Set status ▼

Overview

Related resource details

▼ OpsItem details: oi-aa11bb22cc33dd44

Edit

Description

CloudWatch Application Insights has detected a problem in application *exampleApplication*.

**Problem Summary:** ECS: Network received bytes

**Problem ID:** [p-aa11bb22-ccdd-eeff-33gg-aa11bb22cc33dd44](#)

**Problem Status:** RESOLVED

**Insight:** Unusual network received bytes can indicate misconfigured networks.

|                                                                  |                                 |
|------------------------------------------------------------------|---------------------------------|
| OpsItem ID                                                       | Status                          |
| oi-aa11bb22cc33dd44                                              | 🕒 Open                          |
| Title                                                            | Source                          |
| [exampleApplication: exampleCluster] ECS: Network received bytes | Cloudwatch Application Insights |
| Created                                                          | Last updated                    |
| 2023-09-26T17:39:31Z                                             | 2023-09-29T08:25:26Z            |
| Created by                                                       | Account ID                      |
| arn:aws:sts::112233445566::application-insights                  | 112233445566                    |
| Priority                                                         | Notifications                   |
| 2                                                                | -                               |
| Deduplication string                                             | Severity                        |
| p-aa11bb22-ccdd-eeff-33gg-aa11bb22cc33dd44                       | 3 - Medium                      |

Related resources (1)

AddEditRemoveRun automation ▼

🔍

< 1 >

| Resource ARN                                                               | Type |
|----------------------------------------------------------------------------|------|
| <a href="#">arn:aws:ecs:us-east-1: 112233445566:cluster/exampleCluster</a> | -    |

Comprensione OpsCenter integrazione con Amazon DevOps Guru

Amazon DevOps Guru applica l'apprendimento automatico per analizzare i dati operativi, le metriche delle applicazioni e gli eventi delle applicazioni per identificare comportamenti che si discostano dai

normali schemi operativi. Se consenti a DevOps Guru di generare un OpsItem inputOpsCenter, ogni insight ne genera uno nuovo. OpsItem Puoi utilizzare OpsCenter per gestire gli OpsItems.

DevOpsGuru crea automaticamente. OpsItems Puoi abilitare Amazon DevOps Guru a creare OpsItems utilizzando Quick Setup, che è uno strumento in Systems Manager. Il sistema crea OpsItems utilizzando il ruolo collegato al servizio [AWSServiceRoleForDevOpsGuru](#) AWS Identity and Access Management (IAM).

Per integrare OpsCenter con DevOps Guru

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Quick Setup.
3. Nella pagina delle opzioni di configurazione di Customize DevOps Guru, scegli la scheda Libreria.
4. Nel pannello DevOps Guru, scegli Crea.
5. Per le opzioni di configurazione, seleziona Abilita. AWS Systems Manager OpsItems
6. Dopo aver completato la configurazione, seleziona Crea.

Comprensione OpsCenter integrazione con Amazon EventBridge

Amazon EventBridge offre un flusso di eventi che descrivono i cambiamenti nelle AWS risorse. Quando abiliti OpsCenter l'utilizzo di Integrated Setup, si integra EventBridge e abilita EventBridge le regole predefinite. OpsCenter In base a queste regole, EventBridge creaOpsItems. Utilizzando le regole, puoi filtrare e indirizzare gli eventi a OpsCenter fini di analisi e correzione.

#### Note

Amazon EventBridge (in precedenza Amazon CloudWatch Events) fornisce tutte le funzionalità di CloudWatch Events e alcune nuove funzionalità, come bus di eventi personalizzati, sorgenti di eventi di terze parti e registro degli schemi.

Di seguito sono riportate alcune regole che puoi configurare EventBridge per creare un: OpsItem

- Security Hub CSPM: avviso di sicurezza emesso
- Amazon DynamoDB: un evento di limitazione (della larghezza di banda della rete)

- Dimensionamento automatico di Amazon Elastic Compute Cloud: impossibile avviare un'istanza
- Systems Manager: mancata esecuzione di un'automazione
- AWS Health: un avviso per la manutenzione programmata
- Amazon EC2: lo stato dell'istanza è stato modificato da in esecuzione ad arresto

In base alle tue esigenze, puoi creare una regola o modificare una regola esistente per creare un OpsItems. Per avere istruzioni su come modificare una regola per creare un OpsItem, consulta la pagina [Configura EventBridge le regole per creare OpsItems](#).

### Comprensione OpsCenter integrazione con AWS Config

AWS Config fornisce una visione dettagliata della configurazione delle AWS risorse nel tuo Account AWS.

AWS Config non si integra direttamente con OpsCenter. Invece, crei una AWS Config regola che invia un evento ad Amazon EventBridge, ad esempio quando AWS Config rileva un'istanza non conforme. Quindi EventBridge valuta quell'evento rispetto a una EventBridge regola che hai creato. Se la regola corrisponde, EventBridge trasforma l'evento in un OpsItem e lo trasmette OpsCenter come destinazione.

Utilizzando questo OpsItem, è possibile tenere traccia dei dettagli della risorsa non conforme, registrare le operazioni investigative e fornire l'accesso a operazioni correttive coerenti.

Informazioni correlate

[Configura EventBridge le regole per creare OpsItems](#)

[Utilizzo AWS Systems Manager OpsCenter e AWS Config per il monitoraggio della conformità](#)

### Comprensione OpsCenter integrazione con AWS Security Hub CSPM

AWS Security Hub CSPM raccoglie dati di sicurezza, denominati risultati, provenienti da tutti Account AWS i servizi. Utilizzando una serie di regole per rilevare e generare risultati, Security Hub CSPM ti aiuta a identificare, assegnare priorità e risolvere i problemi di sicurezza per le risorse che gestisci. Dopo aver configurato l'integrazione, come descritto in questo argomento, Systems Manager crea OpsItems per Security Hub i risultati CSPM in. OpsCenter

 Note

OpsCenter ha un'integrazione bidirezionale con Security Hub CSPM. Ciò significa che se si aggiorna il campo Stato o Severità OpsItem relativo a un risultato di sicurezza, il sistema sincronizza le modifiche con Security Hub CSPM. Allo stesso modo, qualsiasi modifica a un esito viene aggiornata automaticamente negli OpsItems corrispondenti in OpsCenter. Quando OpsItem viene creato un risultato CSPM di Security Hub, i metadati CSPM di Security Hub vengono aggiunti automaticamente al campo dei dati operativi del. OpsItem. Se questi metadati vengono eliminati, gli aggiornamenti bidirezionali non funzionano più.

Per impostazione predefinita, Systems Manager crea OpsItems per esiti critici e di elevata gravità. Puoi configurare OpsCenter manualmente per la creazione di OpsItems per risultati di media e bassa gravità. OpsCenter non crea OpsItems per gli esiti informativi, perché questi non richiedono interventi correttivi. Per ulteriori informazioni sui livelli di gravità del CSPM di Security Hub, consulta Severity in the API Reference. [https://docs.aws.amazon.com/securityhub/1.0/APIReference/API\\_Severity.html](https://docs.aws.amazon.com/securityhub/1.0/APIReference/API_Severity.html)

AWS Security Hub

Prima di iniziare

Prima di configurare la creazione OpsCenter in OpsItems base ai risultati del CSPM di Security Hub, verifica di aver completato le attività di configurazione di Security Hub CSPM. Per ulteriori informazioni, vedere [Configurazione di Security Hub](#) CSPM nella Guida per l'utente. AWS Security Hub

Quando si integra Security Hub CSPM con OpsCenter, il sistema crea OpsItems utilizzando il ruolo collegato al `AWSServiceRoleForSystemsManagerOpsDataSync` servizio IAM. Per ulteriori informazioni su questo ruolo, consulta [Usare i ruoli per creare OpsData e OpsItems per Explorer](#).

 Warning

Tieni presente le seguenti importanti informazioni sui prezzi per l'OpsCenter integrazione con Security Hub CSPM:

- Se hai effettuato l'accesso all'account amministratore di Security Hub CSPM durante la configurazione OpsCenter e l'integrazione di Security Hub CSPM, il sistema crea i risultati nell'amministratore e in tutti OpsItems gli account dei membri. Gli OpsItems sono tutti creati nell'account amministratore. A seconda di una serie di fattori, ciò può comportare una fattura inaspettatamente elevata da AWS.

Se hai effettuato l'accesso a un account membro quando configuri l'integrazione, il sistema crea OpsItems solo per gli esiti di quel singolo account. Per ulteriori informazioni sull'account amministratore CSPM di Security Hub, sugli account dei membri e sulla loro relazione con il feed degli EventBridge eventi per i risultati, consulta [Tipi di integrazione con Security Hub CSPM nella Guida per l'utente. EventBridge](#) AWS Security Hub

- Per ogni esito che crea un OpsItem, ti viene addebitato il prezzo normale per la creazione dell'OpsItem. Ti verrà inoltre addebitato un costo se modifichi OpsItem o se il risultato corrispondente viene aggiornato in Security Hub CSPM (che attiva un aggiornamento). OpsItem
- OpsItems creati da un'integrazione con non AWS Security Hub CSPM sono attualmente limitati dalla quota massima di 500.000 OpsItems per account in una regione. È quindi possibile che gli avvisi CSPM di Security Hub creino più di 500.000 addebitabili OpsItems in ciascuna regione in un account.

Per gli ambienti ad alta produzione, consigliamo pertanto di limitare l'ambito dei risultati del CSPM di Security Hub ai soli problemi di elevata gravità.

Per configurare OpsCenter da creare OpsItems per i risultati del Security Hub CSPM

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli OpsCenter.
3. Seleziona Impostazioni.
4. Nella sezione dei risultati del Security Hub CSPM, scegli Modifica.
5. Scegli il cursore per passare da Disabilitato ad Abilitato.
6. Se desideri che il sistema crei OpsItems per esiti di media o bassa gravità, attiva queste opzioni.
7. Seleziona Salva per salvare la configurazione.

Utilizza la procedura seguente se non desideri più che il sistema crei i risultati CSPM OpsItems di Security Hub.

Per interrompere la ricezione OpsItems per i risultati del Security Hub CSPM

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli OpsCenter.
3. Seleziona Impostazioni.
4. Nella sezione dei risultati del Security Hub CSPM, scegli Modifica.
5. Scegli il cursore per passare da Abilitato a Disabilitato. Se non riesci ad attivare il cursore, Security Hub CSPM non è stato abilitato per il tuo Account AWS
6. Scegli Salva per salvare la configurazione. OpsCenter non crea più in OpsItems base ai risultati del CSPM di Security Hub.

 Important

Un amministratore delegato di Systems Manager o l'account di AWS Organizations gestione può abilitare i risultati CSPM di Security Hub OpsCenter per più account e Regioni AWS creare una sincronizzazione dei dati delle risorse. Explorer Se la fonte CSPM di Security Hub è abilitata Explorer ed esiste una sincronizzazione dei dati delle risorse indirizzata all'account membro in cui è stata disattivata l'integrazione CSPM di Security Hub, le impostazioni selezionate dall'amministratore hanno la precedenza. OpsCenter continua a creare per Security Hub i risultati OpsItems CSPM. Per interrompere OpsItems la creazione di risultati CSPM per Security Hub in un account membro oggetto della sincronizzazione dei dati delle risorse, contatta l'amministratore e chiedigli di rimuovere il tuo account dalla sincronizzazione dei dati delle risorse o di disattivare il codice sorgente CSPM di Security Hub. Explorer Per informazioni su come modificare questa impostazione in Explorer, consultare [Modifica delle origini dei dati in Systems Manager Explorer](#).

## Comprensione OpsCenter integrazione con Incident Manager

Incident Manager fornisce una console di gestione degli incidenti che consente di mitigare e ripristinare gli incidenti che interessano le applicazioni AWS ospitate. Un incidente è una qualsiasi interruzione o riduzione non pianificata della qualità dei servizi. Dopo aver impostato e configurato [Strumento di gestione degli incidenti](#), il sistema crea automaticamente OpsItems in OpsCenter.

Quando il sistema crea un incidente nello Strumento di gestione degli incidenti, crea anche un OpsItem in OpsCenter e visualizza l'incidente come voce correlata. Se l'OpsItem esiste già, lo

Strumento di gestione degli incidenti non crea un OpsItem. Questo primo OpsItem è noto come OpsItem padre. Se un incidente cresce in termini di scala e ambito, è possibile aggiungere incidenti a un OpsItem esistente. Se necessario, è possibile creare manualmente un incidente per un OpsItem. Dopo la chiusura di un incidente, è possibile creare un'analisi nello Strumento di gestione degli incidenti per migliorare la procedura di risoluzione di problemi analoghi.

Per impostazione predefinita, OpsCenter si integra con lo Strumento di gestione degli incidenti. Se Incident Manager non è impostato, nella OpsCenter pagina viene visualizzato un messaggio per configurare Incident Manager. Quando lo Strumento di gestione degli incidenti crea un OpsItem, è possibile gestire e correggere l'OpsItem da OpsCenter. Per istruzioni sulla creazione di un incidente per un OpsItem, consulta la pagina [Creazione di un incidente per un OpsItem](#).

## Crea OpsItems

Dopo averlo configurato e integrato con il tuo OpsCenter Servizi AWS, puoi crearlo Servizi AWS automaticamente in OpsItems base a regole, eventi o allarmi predefiniti.

Puoi visualizzare gli stati e i livelli di gravità delle regole Amazon EventBridge predefinite. Se necessario, puoi creare o modificare queste regole da Amazon EventBridge. Puoi anche visualizzare gli allarmi da Amazon CloudWatch e creare o modificare allarmi. Utilizzando regole e allarmi, puoi configurare gli eventi per i quali desideri generare automaticamente OpsItems.

Quando il sistema crea un OpsItem, è nello stato Aperto. È possibile modificare lo stato a In corso quando avvii l'indagine sull'OpsItem e in Risolto dopo aver risolto l'OpsItem. Per ulteriori informazioni su come configurare allarmi e regole in Servizi AWS to create OpsItems e su come creare OpsItems manualmente, consulta i seguenti argomenti.

### Argomenti

- [Configura EventBridge le regole per creare OpsItems](#)
- [Configura CloudWatch gli allarmi per creare OpsItems](#)
- [Crea OpsItems manualmente](#)

### Configura EventBridge le regole per creare OpsItems

Quando Amazon EventBridge riceve un evento, ne crea uno nuovo OpsItem basato su regole predefinite. Puoi creare una regola o modificare una regola esistente da impostare OpsCenter come destinazione di un EventBridge evento. Per informazioni su come creare una regola di evento, consulta [Creating a rule for an Servizio AWS](#) nella Amazon EventBridge User Guide.

Per configurare una EventBridge regola da creare OpsItems in OpsCenter

1. Apri la EventBridge console Amazon all'indirizzo <https://console.aws.amazon.com/events/>.
2. Nel riquadro di navigazione, scegli Regole.
3. Alla pagina Regole, per Router di eventi, scegli predefinito.
4. Per Regole, scegli una regola selezionando la casella di controllo accanto al rispettivo nome.
5. Seleziona il nome della regola per aprire la relativa pagina dei dettagli. Nella sezione Dettagli regola, verifica che Stato sia impostato su Abilitato.

 Note

Se necessario, puoi aggiornare lo stato utilizzando il selettore Modifica nell'angolo in alto a destra della pagina.

6. Scegliere la scheda Destinazioni.
7. Nella scheda Destinazioni scegliere Modifica.
8. Per i tipi di destinazione, selezionare Servizio AWS.
9. Per Select a target (Seleziona una destinazione), scegli Systems Manager OpsItem.
10. Per molti tipi di target, è EventBridge necessaria l'autorizzazione per inviare eventi alla destinazione. In questi casi, EventBridge può creare il ruolo AWS Identity and Access Management (IAM) necessario per l'esecuzione della regola:
  - Per creare un ruolo IAM automaticamente, seleziona Crea un nuovo ruolo per questa risorsa specifica.
  - Per utilizzare un ruolo IAM che hai creato per EventBridge autorizzare la creazione OpsItemsOpsCenter, scegli Usa il ruolo esistente.
11. Nella sezione Impostazioni aggiuntive, per Configura input target, scegli Trasformatore di input.

È possibile utilizzare l'opzione Trasformatore di input per specificare una stringa di deduplicazione e altre informazioni importanti per OpsItems, come un titolo e una gravità.
12. Seleziona Configura il trasformatore di input.
13. Nella sezione Trasformatore di input target, per Percorso di input, specifica i valori da analizzare dell'evento di attivazione. Ad esempio, per analizzare l'ora di inizio, l'ora di fine e altri dettagli dell'evento che attiva la regola, utilizza il seguente JSON.

```
{
```



```

 "end-time": "$.detail.EndTime",
 "failure-cause": "$.detail.cause",
 "resources": "$.resources[0]",
 "source": "$.detail.source",
 "start-time": "$.detail.StartTime"
 }

```

14. Per Template, specifica le informazioni da inviare alla destinazione. Ad esempio, utilizza il seguente codice JSON per trasmettere informazioni aOpsCenter. Le informazioni vengono utilizzate per creare un OpsItem.

#### Note

Se il modello di input è in formato JSON, il valore dell'oggetto nel modello non può includere virgolette. Ad esempio, i valori per le risorse, la causa dell'errore, l'origine, l'ora di inizio e l'ora di fine non possono essere racchiusi tra virgolette.

```

{
 "title": "EBS snapshot copy failed",
 "description": "CloudWatch Event Rule SSM0psItems-EBS-snapshot-copy-failed was triggered. Your EBS snapshot copy has failed. See below for more details.",
 "category": "Availability",
 "severity": "2",
 "source": "EC2",
 "operationalData": {
 "/aws/dedup": {
 "type": "SearchableString",
 "value": "{\"dedupString\":\"SSM0psItems-EBS-snapshot-copy-failed\"}"
 },
 "/aws/automations": {
 "value": "[{ \"automationType\": \"AWS:SSM:Automation\",
 \"automationId\": \"AWS-CopySnapshot\" }]"
 },
 "failure-cause": {
 "value": <failure-cause>
 },
 "source": {
 "value": <source>
 },
 "start-time": {
 "value": <start-time>
 }
 }
}

```

```
 },
 "end-time": {
 "value": <end-time>
 },
 },
 "resources": {
 "value": <resources>
 }
}
```

Per ulteriori informazioni su questi campi, consulta [Transforming target input](#) nella Amazon EventBridge User Guide.

15. Scegli Conferma.
16. Scegli Successivo.
17. Scegli Next (Successivo).
18. Scegli Aggiorna regola.

Dopo che un OpsItem viene creato da un evento, è possibile visualizzare i dettagli dell'evento aprendo OpsItem e scorrendo alla sezione Dati operativi privati. Per ulteriori informazioni su come configurare le opzioni in un OpsItem, consulta [Manage \(Gestione\) OpsItems](#).

### Configura CloudWatch gli allarmi per creare OpsItems

Durante la configurazione integrata di OpsCenter, consenti CloudWatch ad Amazon di creare automaticamente OpsItems in base agli allarmi comuni. Puoi creare un allarme o modificare un allarme esistente per la creazione di OpsItems in OpsCenter.

CloudWatch crea un nuovo ruolo collegato ai servizi in AWS Identity and Access Management (IAM) quando configuri un allarme da creare. OpsItems Il nuovo ruolo è denominato `AWSServiceRoleForCloudWatchAlarms_ActionSSM`. Per ulteriori informazioni sui ruoli collegati ai servizi, consulta [Using CloudWatch service-linked roles for CloudWatch](#) nella Amazon User Guide. CloudWatch

Quando un CloudWatch allarme ne genera uno OpsItem, il OpsItem display CloudWatch alarm - ***alarm\_name*** 'è in stato ALARM.

Per visualizzare i dettagli relativi a uno specifico OpsItem, scegli l'OpsItem, quindi scegli la scheda Dettagli della risorsa correlata. È possibile modificare manualmente OpsItems per cambiare dettagli

quali la gravità o la categoria. Tuttavia, quando si modifica la gravità o la categoria di un allarme, Systems Manager non può aggiornare la gravità o la categoria degli OpsItems che sono già stati creati dall'allarme. Se un allarme ha creato una stringa OpsItem e se è stata specificata una stringa di deduplicazione, l'avviso non ne creerà un'altra OpsItems anche se si modifica l'avviso in CloudWatch. Se OpsItem viene risolto in OpsCenter, CloudWatch ne creerà uno nuovo. OpsItem

Per ulteriori informazioni sulla configurazione degli CloudWatch allarmi, consulta i seguenti argomenti.

## Argomenti

- [Configurazione di un CloudWatch allarme da creare OpsItems \(console\)](#)
- [Configurazione di un CloudWatch allarme esistente da creare OpsItems \(a livello di codice\)](#)

## Configurazione di un CloudWatch allarme da creare OpsItems (console)

Puoi creare manualmente un allarme o aggiornare un allarme esistente OpsItems da creare da Amazon CloudWatch.

Per creare un CloudWatch allarme e configurare Systems Manager come bersaglio di tale allarme

1. Completa i passaggi da 1 a 9 come specificato in [Creare un CloudWatch allarme basato su una soglia statica](#) nella Amazon CloudWatch User Guide.
2. Nella sezione Azione Systems Manager, scegli Aggiungi OpsCenter azione Systems Manager.
3. Scegli OpsItems.
4. Per Gravità, scegli un valore da 1 a 4.
5. (Facoltativo) Per Categoria, scegli una categoria per l'OpsItem.
6. Completa i passaggi da 11 a 13 come specificato in [Creare un CloudWatch allarme basato su una soglia statica](#) nella Amazon CloudWatch User Guide.
7. Scegli Next (Successivo) e completa la procedura guidata.

Per modificare un allarme esistente e configurare Systems Manager come destinazione di quell'allarme

1. Apri la CloudWatch console all'indirizzo. <https://console.aws.amazon.com/cloudwatch/>
2. Nel pannello di navigazione, seleziona Alarms (Allarmi).
3. Seleziona l'allarme, quindi scegli Actions (Operazioni), Edit (Modifica).

4. (Facoltativo) Modifica le impostazioni nelle sezioni Metrics (Parametri) e Conditions (Condizioni), quindi scegli Next (Successivo).
5. Nella sezione Systems Manager, scegli l'operazione Add Systems Manager OpsCenter (Aggiungi Systems Manager ).
6. Per Severity (Gravità) scegli un numero.

 Note

La gravità è un valore definito dall'utente. L'utente o la propria organizzazione determinano il significato di ogni valore di gravità e qualsiasi accordo sui livelli di servizio associato a ogni gravità.

7. (Facoltativo) Per Category (Categoria), scegliere un'opzione.
8. Scegli Next (Successivo) e completa la procedura guidata.

Configurazione di un CloudWatch allarme esistente da creare OpsItems (a livello di codice)

Puoi configurare gli CloudWatch allarmi Amazon per crearli a OpsItems livello di codice utilizzando AWS Command Line Interface (AWS CLI), AWS CloudFormation modelli o Java frammenti di codice.

### Argomenti

- [Prima di iniziare](#)
- [Configurazione degli CloudWatch allarmi da creare OpsItems \(\)AWS CLI](#)
- [Configurazione degli CloudWatch allarmi per creare o aggiornare OpsItems \(\) CloudFormation](#)
- [Configurazione degli CloudWatch allarmi per creare o aggiornare OpsItems \(\) Java](#)

### Prima di iniziare

Se modifichi a livello di programmazione un allarme esistente o crei un allarme che crea OpsItems, devi specificare un nome della risorsa Amazon (ARN). Questo ARN identificherà Systems Manager OpsCenter come obiettivo per la creazione di OpsItems dall'allarme. È possibile personalizzare l'ARN in modo che OpsItems creati dall'allarme includano informazioni specifiche quali la gravità o la categoria. Ogni ARN include le informazioni descritte nella tabella seguente.

| Parametro              | Informazioni                                                                                                                                                                                                                    |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Region(richiesto)      | La posizione Regione AWS in cui si trova l'allarme. Ad esempio: <code>us-west-2</code> . Per informazioni su Regioni AWS dove è possibile utilizzare OpsCenter, consulta <a href="#">Endpoint e quote AWS Systems Manager</a> . |
| account_ID (richiesto) | Lo stesso Account AWS ID usato per creare l'allarme. Ad esempio: <code>123456789012</code> . L'ID account deve essere seguito da due punti (:) e dal parametro <code>opsitem</code> come mostrato negli esempi seguenti.        |
| severity(richiesto)    | Un livello di gravità definito dall'utente per la creazione di OpsItems dall'allarme. Valori validi: 1, 2, 3, 4                                                                                                                 |
| Category (facoltativo) | categoria per la creazione di OpsItems dall'allarme. Valori validi: <code>Availability</code> , <code>Cost</code> , <code>Performance</code> , <code>Recovery</code> e <code>Security</code> .                                  |

Creare l'ARN utilizzando la seguente sintassi. Questo ARN non include l'opzione di parametro `Category`.

```
arn:aws:ssm:Region:account_ID:opsitem:severity
```

Di seguito è riportato un esempio.

```
arn:aws:ssm:us-west-2:123456789012:opsitem:3
```

Per creare un ARN che utilizza l'opzione `Category` utilizzare la seguente sintassi.

```
arn:aws:ssm:Region:account_ID:opsitem:severity#CATEGORY=category_name
```

Di seguito è riportato un esempio.

```
arn:aws:ssm:us-west-2:123456789012:opsitem:3#CATEGORY=Security
```

## Configurazione degli CloudWatch allarmi da creare OpsItems (AWS CLI)

Questo comando richiede di specificare un ARN per il parametro `alarm-actions`. Per informazioni su come creare l'ARN, consulta [Prima di iniziare](#).

### Per configurare un CloudWatch allarme da creare OpsItems (AWS CLI)

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Eseguire il seguente comando per raccogliere informazioni sull'allarme da configurare.

```
aws cloudwatch describe-alarms --alarm-names "alarm name"
```

3. Esegui il seguente comando per aggiornare un allarme. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
aws cloudwatch put-metric-alarm --alarm-name name \
--alarm-description "description" \
--metric-name name --namespace namespace \
--statistic statistic --period value --threshold value \
--comparison-operator value \
--dimensions "dimensions" --evaluation-periods value \
--alarm-actions
arn:aws:ssm:Region:account_ID:opsitem:severity#CATEGORY=category_name \
--unit unit
```

Ecco un esempio:

### Linux & macOS

```
aws cloudwatch put-metric-alarm --alarm-name cpu-mon \
--alarm-description "Alarm when CPU exceeds 70 percent" \
--metric-name CPUUtilization --namespace AWS/EC2 \
--statistic Average --period 300 --threshold 70 \
--comparison-operator GreaterThanThreshold \
--dimensions "Name=InstanceId,Value=i-12345678" --evaluation-periods 2 \

```

```
--alarm-actions arn:aws:ssm:us-east-1:123456789012:opsitem:3#CATEGORY=Security \
--unit Percent
```

## Windows

```
aws cloudwatch put-metric-alarm --alarm-name cpu-mon ^
--alarm-description "Alarm when CPU exceeds 70 percent" ^
--metric-name CPUUtilization --namespace AWS/EC2 ^
--statistic Average --period 300 --threshold 70 ^
--comparison-operator GreaterThanThreshold ^
--dimensions "Name=InstanceId,Value=i-12345678" --evaluation-periods 2 ^
--alarm-actions arn:aws:ssm:us-east-1:123456789012:opsitem:3#CATEGORY=Security ^
--unit Percent
```

## Configurazione degli CloudWatch allarmi per creare o aggiornare OpsItems () CloudFormation

Questa sezione include AWS CloudFormation modelli che è possibile utilizzare per configurare gli CloudWatch allarmi da creare o aggiornare automaticamente. OpsItems Ogni modello richiede di specificare un ARN per il parametro AlarmActions. Per informazioni su come creare l'ARN, consulta [Prima di iniziare](#).

Allarme metrico: utilizza il seguente CloudFormation modello per creare o aggiornare un allarme CloudWatch metrico. L'allarme specificato in questo modello monitora i controlli dello stato delle istanze Amazon Elastic Compute Cloud (Amazon EC2). Se l'allarme entra nel ALARM, crea un OpsItem in OpsCenter.

```
{
 "AWSTemplateFormatVersion": "2010-09-09",
 "Parameters" : {
 "RecoveryInstance" : {
 "Description" : "The EC2 instance ID to associate this alarm with.",
 "Type" : "AWS::EC2::Instance::Id"
 }
 },
 "Resources": {
 "RecoveryTestAlarm": {
 "Type": "AWS::CloudWatch::Alarm",
 "Properties": {
```

```

 "AlarmDescription": "Run a recovery action when instance status check fails
for 15 consecutive minutes.",
 "Namespace": "AWS/EC2" ,
 "MetricName": "StatusCheckFailed_System",
 "Statistic": "Minimum",
 "Period": "60",
 "EvaluationPeriods": "15",
 "ComparisonOperator": "GreaterThanThreshold",
 "Threshold": "0",
 "AlarmActions": [{"Fn::Join" : ["",
["arn:arn:aws:ssm:Region:account_ID:opsitem:severity#CATEGORY=category_name",
{ "Ref" : "AWS::Partition" }, ":ssm:", { "Ref" : "AWS::Region" }, { "Ref" : "AWS::
AccountId" }, ":opsitem:3"]]]],
 "Dimensions": [{"Name": "InstanceId","Value": {"Ref": "RecoveryInstance"}}]
 }
}
}
}

```

Allarme composito: utilizza il seguente CloudFormation modello per creare o aggiornare un allarme composito. Un allarme composito è costituito da più allarmi dei parametri. Se l'allarme entra nel ALARM, crea un OpsItem in OpsCenter.

```

"Resources":{
 "HighResourceUsage":{
 "Type":"AWS::CloudWatch::CompositeAlarm",
 "Properties":{
 "AlarmName":"HighResourceUsage",
 "AlarmRule":"(ALARM(HighCPUUsage) OR ALARM(HighMemoryUsage)) AND NOT
ALARM(DeploymentInProgress)",
 "AlarmActions":"arn:aws:ssm:Region:account_ID:opsitem:severity#CATEGORY=category_name",
 "AlarmDescription":"Indicates that the system resource usage is high while
no known deployment is in progress"
 },
 "DependsOn":[
 "DeploymentInProgress",
 "HighCPUUsage",
 "HighMemoryUsage"
]
 },
 "DeploymentInProgress":{
 "Type":"AWS::CloudWatch::CompositeAlarm",

```



```

 "Properties":{
 "AlarmName":"DeploymentInProgress",
 "AlarmRule":"FALSE",
 "AlarmDescription":"Manually updated to TRUE/FALSE to disable other
alarms"
 }
 },
 "HighCPUUsage":{
 "Type":"AWS::CloudWatch::Alarm",
 "Properties":{
 "AlarmDescription":"CPUUsageishigh",
 "AlarmName":"HighCPUUsage",
 "ComparisonOperator":"GreaterThanThreshold",
 "EvaluationPeriods":1,
 "MetricName":"CPUUsage",
 "Namespace":"CustomNamespace",
 "Period":60,
 "Statistic":"Average",
 "Threshold":70,
 "TreatMissingData":"notBreaching"
 }
 },
 "HighMemoryUsage":{
 "Type":"AWS::CloudWatch::Alarm",
 "Properties":{
 "AlarmDescription":"Memoryusageishigh",
 "AlarmName":"HighMemoryUsage",
 "ComparisonOperator":"GreaterThanThreshold",
 "EvaluationPeriods":1,
 "MetricName":"MemoryUsage",
 "Namespace":"CustomNamespace",
 "Period":60,
 "Statistic":"Average",
 "Threshold":65,
 "TreatMissingData":"breaching"
 }
 }
}

```

## Configurazione degli CloudWatch allarmi per creare o aggiornare OpsItems () Java

Questa sezione include frammenti di Java codice che è possibile utilizzare per configurare gli CloudWatch allarmi da creare o aggiornare automaticamente. OpsItems Ogni frammento richiede di

specificare un ARN per il parametro `validSsmActionStr`. Per informazioni su come creare l'ARN, consulta [Prima di iniziare](#).

Un allarme specifico: utilizza il seguente frammento di Java codice per creare o aggiornare un avviso. CloudWatch L'allarme specificato in questo modello monitora i controlli dello stato delle istanze Amazon EC2. Se l'allarme entra nel ALARM, crea un OpsItem in OpsCenter.

```
import com.amazonaws.services.cloudwatch.AmazonCloudWatch;
import com.amazonaws.services.cloudwatch.AmazonCloudWatchClientBuilder;
import com.amazonaws.services.cloudwatch.model.ComparisonOperator;
import com.amazonaws.services.cloudwatch.model.Dimension;
import com.amazonaws.services.cloudwatch.model.PutMetricAlarmRequest;
import com.amazonaws.services.cloudwatch.model.PutMetricAlarmResult;
import com.amazonaws.services.cloudwatch.model.StandardUnit;
import com.amazonaws.services.cloudwatch.model.Statistic;

private void putMetricAlarmWithSsmAction() {
 final AmazonCloudWatch cw =
 AmazonCloudWatchClientBuilder.defaultClient();

 Dimension dimension = new Dimension()
 .withName("InstanceId")
 .withValue(instanceId);

 String validSsmActionStr =
 "arn:aws:ssm:Region:account_ID:opsitem:severity#CATEGORY=category_name";

 PutMetricAlarmRequest request = new PutMetricAlarmRequest()
 .withAlarmName(alarmName)
 .withComparisonOperator(
 ComparisonOperator.GreaterThanThreshold)
 .withEvaluationPeriods(1)
 .withMetricName("CPUUtilization")
 .withNamespace("AWS/EC2")
 .withPeriod(60)
 .withStatistic(Statistic.Average)
 .withThreshold(70.0)
 .withActionsEnabled(false)
 .withAlarmDescription(
 "Alarm when server CPU utilization exceeds 70%")
 .withUnit(StandardUnit.Seconds)
 .withDimensions(dimension)
 .withAlarmActions(validSsmActionStr);
}
```

```
PutMetricAlarmResult response = cw.putMetricAlarm(request);
}
```

Aggiorna tutti gli allarmi: utilizza il seguente frammento di Java codice per aggiornare tutti gli CloudWatch allarmi presenti nel tuo sistema e Account AWS creare OpsItems quando un allarme entra in uno stato. ALARM

```
import com.amazonaws.services.cloudwatch.AmazonCloudWatch;
import com.amazonaws.services.cloudwatch.AmazonCloudWatchClientBuilder;
import com.amazonaws.services.cloudwatch.model.DescribeAlarmsRequest;
import com.amazonaws.services.cloudwatch.model.DescribeAlarmsResult;
import com.amazonaws.services.cloudwatch.model.MetricAlarm;

private void listMetricAlarmsAndAddSsmAction() {
 final AmazonCloudWatch cw = AmazonCloudWatchClientBuilder.defaultClient();

 boolean done = false;
 DescribeAlarmsRequest request = new DescribeAlarmsRequest();

 String validSsmActionStr =
 "arn:aws:ssm:Region:account_ID:opsitem:severity#CATEGORY=category_name";

 while(!done) {

 DescribeAlarmsResult response = cw.describeAlarms(request);

 for(MetricAlarm alarm : response.getMetricAlarms()) {
 // assuming there are no alarm actions added for the metric alarm
 alarm.setAlarmActions(ImmutableList.of(validSsmActionStr));
 }

 request.setNextToken(response.getNextToken());

 if(response.getNextToken() == null) {
 done = true;
 }
 }
}
```

## Crea OpsItems manualmente

Quando trovi un problema operativo, puoi creare manualmente un modulo OpsItem OpsCenter per gestirlo e risolverlo.

Se si configura OpsCenter l'amministrazione tra più account, è possibile creare un amministratore delegato o un account di AWS Organizations gestione di Systems Manager OpsItems per gli account dei membri. Per ulteriori informazioni, consulta [\(Facoltativo\) Configurazione manuale OpsCenter per gestire centralmente OpsItems tra gli account](#).

È possibile creare OpsItems utilizzando la AWS Systems Manager console, AWS Command Line Interface (AWS CLI) o. AWS Tools for Windows PowerShell

### Argomenti

- [Creazione manuale di OpsItems \(console\)](#)
- [Creazione in corso OpsItems manualmente \(AWS CLI\)](#)
- [Creazione manuale di OpsItems \(PowerShell\)](#)

### Creazione manuale di OpsItems (console)

Puoi creare manualmente OpsItems utilizzando la AWS Systems Manager console. Quando crei un OpsItem, viene visualizzato nell'account OpsCenter. Se imposti OpsCenter per l'amministrazione multi-account, OpsCenter fornisce all'amministratore delegato o a un account di gestione la possibilità di creare OpsItems per gli account membri selezionati. Per ulteriori informazioni, consulta [\(Facoltativo\) Configurazione manuale OpsCenter per gestire centralmente OpsItems tra gli account](#).

Per creare un file OpsItem utilizzando la AWS Systems Manager console

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli OpsCenter.
3. Scegli Crea OpsItem. Se non visualizzi questo pulsante, seleziona la scheda OpsItems, quindi scegli Crea OpsItem.
4. (Facoltativo) Scegli Altro account, quindi scegli l'account in cui desideri creare l'OpsItem.

 Note

Questo passaggio è obbligatorio se stai creando OpsItems per un account membro.

5. Per Titolo, immetti un nome dettagliato per aiutare a comprendere lo scopo di OpsItem.
6. Per Origine, inserisci il tipo di risorsa AWS coinvolta o altre informazioni sull'origine per aiutare gli utenti a comprendere l'origine di OpsItem.

 Note

Non è possibile modificare il campo Origine dopo aver creato OpsItem.

7. Per Priorità, scegli il livello di priorità.
8. (Facoltativo) Per Gravità, scegli il livello di gravità.
9. (Facoltativo) Per Categoria, scegli una categoria.
10. Per Descrizione, immetti le informazioni su questo OpsItem tra le quali (se applicabile) la procedura per riprodurre il problema.

 Note

La console supporta la maggior parte della formattazione dei markdown nel campo della OpsItem descrizione. Per ulteriori informazioni, consulta [Uso di Markdown nella console](#) nella Guida introduttiva alla Console di gestione AWS .

11. Per Stringa di deduplicazione, inserisci le parole che il sistema deve utilizzare per verificare la presenza di OpsItems duplicati. Per ulteriori informazioni sulle stringhe di deduplicazione, consulta [Gestione dei OpsItems duplicati](#).
12. (Facoltativo) Per Notifiche, specifica il nome della risorsa Amazon (ARN) dell'argomento Amazon SNS al quale desideri che vengano inviate le notifiche quando questo OpsItem viene aggiornato. È necessario specificare un ARN Amazon SNS che sia uguale a. Regione AWS OpsItem
13. (Facoltativo) In Risorse correlate, scegli Aggiungi per specificare l'ID o l'ARN della risorsa coinvolta e di qualsiasi risorsa correlata.
14. Scegli Crea OpsItem.

Se l'esito è positivo, la pagina visualizza l'OpsItem. Quando un amministratore delegato o un account di gestione crea un OpsItem per gli account membri selezionati, i nuovi OpsItems vengono visualizzati nell'OpsCenter dell'account amministratore e degli account membri. Per ulteriori informazioni su come configurare le opzioni in un OpsItem, consulta [Manage \(Gestione\) OpsItems](#).

### Creazione in corso OpsItems manualmente (AWS CLI)

Nella procedura riportata di seguito viene descritto come creare un OpsItem tramite AWS Command Line Interface (AWS CLI).

Per creare un OpsItem utilizzando il AWS CLI

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Apri AWS CLI ed esegui il seguente comando per creare unOpsItem. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
aws ssm create-ops-item \
 --title "Descriptive_title" \
 --description "Information_about_the_issue" \
 --priority Number_between_1_and_5 \
 --source Source_of_the_issue \
 --operational-data Up_to_20_KB_of_data_or_path_to_JSON_file \
 --notifications Arn="SNS_ARN_in_same_Region" \
 --tags "Key=key_name,Value=a_value"
```

### Specificare i dati operativi da un file

Quando crei un OpsItem, è possibile specificare i dati operativi da un file. Il file deve essere un file JSON e i contenuti del file devono avere il formato seguente.

```
{
 "key_name": {
 "Type": "SearchableString",
 "Value": "Up to 20 KB of data"
 }
}
```

Ecco un esempio.

```
aws ssm create-ops-item ^
 --title "EC2 instance disk full" ^
 --description "Log clean up may have failed which caused the disk to be full" ^
 --priority 2 ^
 --source ec2 ^
 --operational-data file:///Users/TestUser1/Desktop/OpsItems/opsData.json ^
 --notifications Arn="arn:aws:sns:us-west-1:12345678:TestUser1" ^
 --tags "Key=EC2,Value=Production"
```

### Note

Per informazioni su come immettere JSON-formatted i parametri nella riga di comando su diversi sistemi operativi locali, vedere [Utilizzo delle virgolette con stringhe nella Guida per l'AWS Command Line Interface utente. AWS CLI](#)

Il sistema restituisce informazioni simili alle seguenti.

```
{
 "OpsItemId": "oi-1a2b3c4d5e6f"
}
```

3. Esegui questo comando per visualizzare i dettagli sull'OpsItem che hai creato.

```
aws ssm get-ops-item --ops-item-id ID
```

Il sistema restituisce informazioni simili alle seguenti.

```
{
 "OpsItem": {
 "CreatedBy": "arn:aws:iam::12345678:user/TestUser",
 "CreatedTime": 1558386334.995,
 "Description": "Log clean up may have failed which caused the disk to be
full",
 "LastModifiedBy": "arn:aws:iam::12345678:user/TestUser",
 "LastModifiedTime": 1558386334.995,
 "Notifications": [
 {
 "Arn": "arn:aws:sns:us-west-1:12345678:TestUser"
 }
]
 }
}
```

```

],
 "Priority": 2,
 "RelatedOpsItems": [],
 "Status": "Open",
 "OpsItemId": "oi-1a2b3c4d5e6f",
 "Title": "EC2 instance disk full",
 "Source": "ec2",
 "OperationalData": {
 "EC2": {
 "Value": "12345",
 "Type": "SearchableString"
 }
 }
 }
}

```

4. Eseguire il seguente comando per aggiornare OpsItem. Questo comando modifica lo stato da Open (predefinito) a InProgress.

```
aws ssm update-ops-item --ops-item-id ID --status InProgress
```

Il comando non ha output.

5. Esegui nuovamente il seguente comando per verificare che lo stato sia cambiato in InProgress.

```
aws ssm get-ops-item --ops-item-id ID
```

## Esempi di creazione di un OpsItem

Negli esempi seguenti viene illustrato come creare un OpsItem utilizzando il portale di gestione Linux, macOS oppure Windows Server.

### Portale di gestione Linux oppure macOS

Il comando seguente crea un OpsItem quando un disco istanza Amazon Elastic Compute Cloud (Amazon EC2) è pieno.

```

aws ssm create-ops-item \
 --title "EC2 instance disk full" \
 --description "Log clean up may have failed which caused the disk to be full" \

```



```
--priority 2 \
--source ec2 \
--operational-data '{"EC2":{"Value":"12345","Type":"SearchableString"}}' \
--notifications Arn="arn:aws:sns:us-west-1:12345678:TestUser1" \
--tags "Key=EC2,Value=ProductionServers"
```

Il comando seguente utilizza la chiave `/aws/resources` in `OperationalData` per creare un `OpsItem` con una risorsa correlata ad Amazon DynamoDB.

```
aws ssm create-ops-item \
 --title "EC2 instance disk full" \
 --description "Log clean up may have failed which caused the disk to be full" \
 --priority 2 \
 --source ec2 \
 --operational-data '{""/aws/resources":{"Value":["{"arn": "arn:aws:dynamodb:us-west-2:12345678:table/OpsItems"}'], "Type":"SearchableString"}}' \
 --notifications Arn="arn:aws:sns:us-west-2:12345678:TestUser"
```

Il comando seguente utilizza la chiave `/aws/automations` in `OperationalData` per creare un `OpsItem` che specifica il documento AWS-ASGEnterStandby come runbook Automation associato.

```
aws ssm create-ops-item \
 --title "EC2 instance disk full" \
 --description "Log clean up may have failed which caused the disk to be full" \
 --priority 2 \
 --source ec2 \
 --operational-data '{""/aws/automations":{"Value":["{"automationId": "AWS-ASGEnterStandby", "automationType": "AWS::SSM::Automation"}'], "Type":"SearchableString"}}' \
 --notifications Arn="arn:aws:sns:us-west-2:12345678:TestUser"
```

## Windows

Il comando seguente crea un `OpsItem` quando un'istanza Amazon Relational Database Service (Amazon RDS) non risponde.

```
aws ssm create-ops-item ^
 --title "RDS instance not responding" ^
 --description "RDS instance not responding to ping" ^
 --priority 1 ^
 --source RDS ^
```

```
--operational-data={\"RDS\":{\"Value\": \"abcd\", \"Type\": \"SearchableString\"}} ^
--notifications Arn=\"arn:aws:sns:us-west-1:12345678:TestUser1\" ^
--tags \"Key=RDS,Value=ProductionServers\"
```

Il comando seguente utilizza la chiave `/aws/resources` in `OperationalData` per creare un `OpsItem` con una risorsa correlata a un'istanza Amazon EC2.

```
aws ssm create-ops-item ^
 --title \"EC2 instance disk full\" ^
 --description \"Log clean up may have failed which caused the disk to be full\" ^
 --priority 2 ^
 --source ec2 ^
 --operational-data={\"/aws/resources\":{\"Value\": \"[{\\\"arn\\\":\\\"arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0\\\"}]\\\", \"Type\": \"SearchableString\"}}
```

Il comando seguente utilizza la chiave `/aws/automations` in `OperationalData` per creare un `OpsItem` che specifica il runbook `AWS-RestartEC2Instance` come runbook Automation associato.

```
aws ssm create-ops-item ^
 --title \"EC2 instance disk full\" ^
 --description \"Log clean up may have failed which caused the disk to be full\" ^
 --priority 2 ^
 --source ec2 ^
 --operational-data={\"/aws/automations\":{\"Value\": \"[{\\\"automationId\\\":\\\"AWS-RestartEC2Instance\\\", \\\"automationType\\\":\\\"AWS::SSM::Automation\\\"}]\\\", \"Type\": \"SearchableString\"}}
```

## Creazione manuale di OpsItems (PowerShell)

Nella procedura riportata di seguito viene descritto come creare un `OpsItem` utilizzando AWS Tools for Windows PowerShell.

Per creare un `OpsItem` utilizzo AWS Tools for Windows PowerShell

1. Apri AWS Tools for Windows PowerShell ed esegui il comando seguente per specificare le tue credenziali.

```
Set-AWSCredentials -AccessKey key-name -SecretKey key-name
```

2. Esegui il comando seguente Regione AWS per impostare la PowerShell sessione.

```
Set-DefaultAWSRegion -Region Region
```

3. Per creare un nuovo OpsItem, eseguire il comando seguente. Sostituisci ogni *example resource placeholder* con le tue informazioni. Questo comando specifica un runbook di automazione di Systems Manager per la correzione di questo OpsItem.

```
$opsItem = New-Object Amazon.SimpleSystemsManagement.Model.OpsItemDataValue
$opsItem.Type = [Amazon.SimpleSystemsManagement.OpsItemDataType]::SearchableString
$opsItem.Value = ' [{\"automationId\": \"runbook_name\", \"automationType\": \"AWS::SSM::Automation\"}] '
$newHash = @{" /aws/
automations"=[Amazon.SimpleSystemsManagement.Model.OpsItemDataValue]$opsItem}

New-SSMOpsItem `
 -Title "title" `
 -Description "description" `
 -Priority priority_number `
 -Source AWS_service `
 -OperationalData $newHash
```

In caso di esito positivo, il comando emette l'ID del nuovo OpsItem.

L'esempio seguente specifica il nome della risorsa Amazon (ARN) di un'istanza Amazon Elastic Compute Cloud (Amazon EC2) compromessa.

```
$opsItem = New-Object Amazon.SimpleSystemsManagement.Model.OpsItemDataValue
$opsItem.Type = [Amazon.SimpleSystemsManagement.OpsItemDataType]::SearchableString
$opsItem.Value = ' [{\"arn\": \"arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0\"}] '
$newHash = @{" /aws/
resources"=[Amazon.SimpleSystemsManagement.Model.OpsItemDataValue]$opsItem}
New-SSMOpsItem -Title "EC2 instance disk full still" -Description "Log clean up may
have failed which caused the disk to be full" -Priority 2 -Source ec2 -OperationalData
$newHash
```

## Manage (Gestione) OpsItems

OpsCenter traccia OpsItems dalla loro creazione alla risoluzione. Se imposti OpsCenter per l'amministrazione multi-account, un amministratore delegato o un account di gestione possono

gestire gli OpsItems dal proprio account. Per ulteriori informazioni, consulta [\(Facoltativo\) Configurazione manuale OpsCenter per gestire centralmente OpsItems tra gli account](#).

È possibile visualizzare e gestire gli OpsItems utilizzando le seguenti pagine nella console di Systems Manager:

- **Riepilogo:** mostra il numero degli OpsItems aperti e in corso, il numero di OpsItems per origine ed età, nonché gli approfondimenti operativi. Puoi filtrare gli OpsItems per origine e stato di OpsItems.
- **OpsItems:** visualizza un elenco di OpsItems con più campi di informazioni, come titolo, ID, priorità, descrizione, origine dell'OpsItem, nonché data e ora dell'ultimo aggiornamento. Utilizzando questa pagina, puoi creare manualmente OpsItems, configurare le origini, modificare lo stato di un OpsItem e filtrare gli OpsItems in base a nuovi incidenti. Puoi scegliere un OpsItem per visualizzare la rispettiva pagina dei Dettagli degli OpsItems.
- **Dettagli dell'OpsItem:** fornisce approfondimenti e strumenti che è possibile utilizzare per gestire un OpsItem. La pagina dei dettagli dell'OpsItems contiene le seguenti schede:
  - **Panoramica:** visualizza le risorse correlate, i runbook eseguiti negli ultimi 30 giorni e un elenco dei runbook disponibili che puoi eseguire. Puoi anche visualizzare OpsItems simili, aggiungere dati operativi e aggiungere OpsItems correlati.
  - **Dettagli sulle risorse correlate:** visualizza le informazioni sulla risorsa provenienti da diversi AWS servizi. Espandi la sezione Dettagli della risorsa per visualizzare le informazioni sulla risorsa fornite dal AWS servizio che la ospita. È anche possibile scorrere le altre risorse correlate associate a questo OpsItem utilizzando l'elenco Risorse correlate.

Per ulteriori informazioni sulla gestione di OpsItems, consulta gli argomenti indicati di seguito.

## Argomenti

- [Visualizzazione dei dettagli di un OpsItem](#)
- [Modifica di un OpsItem](#)
- [Aggiungere risorse correlate a un OpsItem](#)
- [Aggiungere elementi correlati OpsItems a un OpsItem](#)
- [Aggiungere dati operativi a un OpsItem](#)
- [Creazione di un incidente per un OpsItem](#)
- [Gestione dei OpsItems duplicati](#)

- [Analisi delle informazioni operative per ridurre OpsItems](#)
- [Visualizzazione di log e report di OpsCenter](#)

## Visualizzazione dei dettagli di un OpsItem

Per avere una visione completa di un OpsItem, utilizza la pagina dei Dettagli OpsItem nella console OpsCenter. La pagina Panoramica contiene le seguenti informazioni:

- **Dettagli OpsItems:** visualizza informazioni generali sull'OpsItem selezionato.
- **Risorse correlate:** una risorsa correlata è la risorsa coinvolta o quella che ha attivato l'evento che ha creato l'OpsItem.
- **Esecuzioni di Automazione negli ultimi 30 giorni:** un elenco di runbook eseguiti negli ultimi 30 giorni.
- **Runbook:** puoi scegliere un runbook da un elenco di runbook disponibili.
- **Simile OpsItems:** si tratta di un elenco generato dal sistema OpsItems che potrebbe essere correlato o di interesse per l'utente. Per generare l'elenco, il sistema analizza i titoli e le descrizioni di tutti gli OpsItems e restituisce OpsItems che utilizzano parole simili.
- **Dati operativi:** i dati operativi sono dati personalizzati che forniscono dettagli di riferimento utili riguardo all'OpsItem. Ad esempio, è possibile specificare i file di log, le stringhe di errore, le chiavi di licenza, i suggerimenti per la risoluzione dei problemi o altri dati.
- **Correlato OpsItems:** puoi specificare gli ID OpsItems che sono in qualche modo correlati a quello corrente. OpsItem
- **Dettagli sulle risorse correlate:** visualizza i fornitori di dati, tra cui CloudWatch metriche e allarmi di Amazon, AWS CloudTrail log e dettagli da AWS Config

## Per visualizzare i dettagli di un OpsItem

1. Apri la console all' AWS Systems Manager indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli OpsCenter.
3. Scegli un OpsItem per visualizzarne i dettagli.

## Modifica di un OpsItem

La sezione Dettagli dell'OpsItem include informazioni su un OpsItem, tra cui la descrizione, il titolo, l'origine, l'ID dell'OpsItem e lo stato.

È possibile modificare un OpsItem individualmente oppure selezionare più OpsItems e modificare i seguenti campi: Stato, Priorità, Gravità e Categoria.

Quando Amazon EventBridge crea unOpsItem, compila i campi Titolo , Fonte e Descrizione. È possibile modificare i campi Titolo e Descrizione, ma non è possibile modificare il campo Origine.

### Note

La console supporta la maggior parte della formattazione markdown nel campo della OpsItem descrizione. Per ulteriori informazioni, consulta [Usare Markdown nella console](#) nella Guida introduttiva alla guida introduttiva. Console di gestione AWS

In genere, è possibile modificare i seguenti dati configurabili per un OpsItem:

- Titolo: il nome dell'OpsItem. L'origine crea il titolo dell'OpsItem.
- Descrizione: le informazioni su questo OpsItem tra le quali (se applicabile) la procedura per riprodurre il problema.
- Stato: stato di un OpsItem. Per un elenco di valori di stato validi, consulta [Stato OpsItem](#) nella Documentazione di riferimento API di AWS Systems Manager .
- Priorità: la priorità di un OpsItem può essere compresa tra 1 e 5. Consigliamo che l'organizzazione determini ciò che ogni livello di priorità significa e un contratto sul livello di servizio corrispondente per ciascun livello.
- Gravità: la gravità di un OpsItem può essere compresa tra 1 e 4, dove 1 è critica, 2 è alta, 3 è media e 4 è bassa.
- Categoria: la categoria di un OpsItem può essere la disponibilità, il costo, le prestazioni, il ripristino o la sicurezza.
- Notifiche: quando modifichi un OpsItem, puoi specificare il nome della risorsa Amazon (ARN) di un argomento Servizio di notifica semplice Amazon nel campo Notifiche. Specificando un ARN, ti assicuri che tutte le parti interessate ricevano una notifica quando OpsItem viene modificato, incluso un cambio di stato. Per ulteriori informazioni, consulta la [Guida per gli sviluppatori di Amazon Simple Notification Service](#).

 Important

L'argomento Amazon SNS deve coincidere con. Regione AWS OpsItem Se l'argomento e l'OpsItem si trovano in Regioni diverse, il sistema restituisce un errore.

OpsCenter ha un'integrazione bidirezionale con. AWS Security Hub CSPM Quando aggiorni uno OpsItem stato e una gravità relativi a un risultato di sicurezza, tali modifiche vengono inviate automaticamente a Security Hub CSPM per assicurarti di visualizzare sempre le informazioni più recenti e corrette.

Quando OpsItem viene creato un risultato CSPM di Security Hub, i metadati CSPM di Security Hub vengono aggiunti automaticamente al campo dei dati operativi del. OpsItem Se questi metadati vengono eliminati, gli aggiornamenti bidirezionali non funzionano più.

Per modificare OpsItem details

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli OpsCenter.
3. Scegliere un ID di OpsItem per aprire la pagina e scegliere più OpsItems. Se scegli più OpsItems, è possibile modificare solo lo stato, la priorità, la gravità o la categoria. Se modifichi più OpsItems, OpsCenter aggiorna e salva le modifiche non appena scegli il nuovo stato, priorità, gravità o categoria.
4. Nella sezione dei OpsItem dettagli, scegli Modifica.
5. Modificare i dettagli di OpsItem in base ai requisiti e alle linee guida specificate dall'organizzazione.
6. Al termine, seleziona Salva.

Aggiungere risorse correlate a un OpsItem

Ogni OpsItem include la sezione Risorse correlate, che elenca il nome della risorsa Amazon (ARN) della risorsa correlata. Una risorsa correlata è la AWS risorsa interessata che deve essere esaminata.

Se Amazon EventBridge crea il OpsItem, il sistema lo compila automaticamente OpsItem con l'ARN della risorsa. Gli ARN delle risorse correlate possono essere specificati anche manualmente. Per

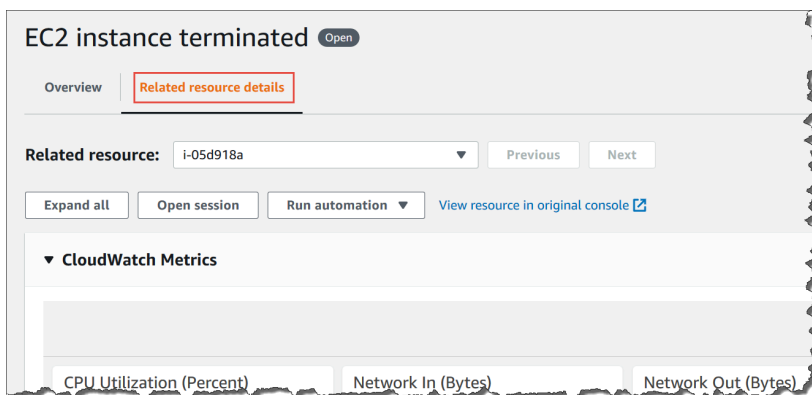
alcuni tipi di ARN, OpsCenter crea automaticamente un collegamento diretto che visualizza la risorsa direttamente nella console di OpsCenter. Ad esempio, se specifichi l'ARN di un'istanza Amazon Elastic Compute Cloud (Amazon EC2) come risorsa correlata, OpsCenter inserisce i dettagli di tale istanza EC2. Ciò ti consente di visualizzare informazioni dettagliate sulle AWS risorse interessate senza dover uscire. OpsCenter

Per visualizzare e aggiungere risorse correlate a un OpsItem

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli OpsCenter.
3. Scegli la scheda OpsItems.
4. Scegliere un ID OpsItem.

| ID                              | Title                   | Status | Source |
|---------------------------------|-------------------------|--------|--------|
| <a href="#">oi-a80f1dbb4464</a> | EC2 instance stopped    | Open   | EC2    |
| <a href="#">oi-0cdb512b47ed</a> | EC2 instance terminated | Open   | EC2    |
| <a href="#">oi-06f350858b55</a> | EC2 instance terminated | Open   | EC2    |

5. Per visualizzare informazioni sulla risorse coinvolte, scegliere la scheda Related resources details (Dettagli risorse correlate).



In questa scheda vengono visualizzate le informazioni sulla risorsa da più Servizi AWS. Espandi la sezione Dettagli della risorsa per visualizzare le informazioni su questa risorsa fornite da Servizio AWS che la ospita. È anche possibile scorrere le altre risorse correlate associate a questo OpsItem utilizzando l'elenco Risorse correlate.

6. Per aggiungere altre risorse correlate, scegliere la scheda Panoramica.
7. Nella sezione Risorse correlate, scegli Aggiungi.



8. Per Tipo di risorsa scegli una risorsa dall'elenco.
9. Per ID risorsa, inserisci l'ID o l'Amazon Resource Name (ARN). Il tipo di informazioni scelto dipende dalla risorsa scelta nel passaggio precedente.

#### Note

È possibile aggiungere manualmente i nomi ARN di altre risorse correlate. Ogni OpsItem può elencare un massimo di 100 ARN di risorse correlate.

La tabella seguente elenca i tipi di risorse che creano automaticamente collegamenti diretti alle risorse correlate.

#### Tipi di risorse supportati

| Nome risorsa                        | Formato ARN                                                                                                                                      |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| AWS Certificate Manager certificato | <code>arn:aws:acm: <i>region</i>:<i>account-id</i>:certificate/<i>certificate-id</i></code>                                                      |
| Gruppo con Amazon EC2 Auto Scaling  | <code>arn:aws:autoscaling: <i>region</i>:<i>account-id</i>:autoScalingGroup: <i>groupid</i>:autoScalingGroupName/<i>groupfriendlyname</i></code> |
| CloudFront Distribuzione Amazon     | <code>arn:aws:cloudfront:: <i>account-id</i> :*</code>                                                                                           |
| AWS CloudFormation pila             | <code>arn:aws:cloudformation: <i>region</i>:<i>account-id</i>:stack/<i>stackname</i> /<i>additionalidentifier</i></code>                         |
| CloudWatch Allarme Amazon           | <code>arn:aws:cloudwatch: <i>region</i>:<i>account-id</i>:alarm:<i>alarm-name</i></code>                                                         |

| Nome risorsa                                                  | Formato ARN                                                                                                                        |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| AWS CloudTrail pista                                          | <code>arn:aws:cloudtrail: <i>region</i>:<i>account-id</i> :trail/<i>trailname</i></code>                                           |
| AWS CodeBuild progetto                                        | <code>arn:aws:codebuild: <i>region</i>:<i>account-id</i> :<i>resourcetype</i> /<i>resource</i></code>                              |
| AWS CodePipeline                                              | <code>arn:aws:codepipeline: <i>region</i>:<i>account-id</i> :<i>resource-specifier</i></code>                                      |
| Informazioni su Amazon DevOps Guru                            | <code>arn:aws:devops-guru: <i>region</i>:<i>account-id</i> :insight/ <i>proactive</i> or <i>reactive</i>/<i>resource-id</i></code> |
| Tabella Amazon DynamoDB                                       | <code>arn:aws:dynamodb: <i>region</i>:<i>account-id</i> :table/<i>tablename</i></code>                                             |
| Gateway del cliente Amazon Elastic Compute Cloud (Amazon EC2) | <code>arn:aws:ec2: <i>region</i>:<i>account-id</i> :customer-gateway/ <i>cgw-id</i></code>                                         |
| IP elastico Amazon EC2                                        | <code>arn:aws:ec2: <i>region</i>:<i>account-id</i> :eip/<i>eipalloc-id</i></code>                                                  |
| Host dedicato di Amazon EC2                                   | <code>arn:aws:ec2: <i>region</i>:<i>account-id</i> :dedicated-host/ <i>host-id</i></code>                                          |
| Istanza Amazon EC2                                            | <code>arn:aws:ec2: <i>region</i>:<i>account-id</i> :instance/ <i>instance-id</i></code>                                            |
| Gateway internet Amazon EC2                                   | <code>arn:aws:ec2: <i>region</i>:<i>account-id</i> :internet-gateway/ <i>igw-id</i></code>                                         |

| Nome risorsa                                          | Formato ARN                                                                                                 |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Lista di controllo degli accessi alla rete Amazon EC2 | <code>arn:aws:ec2: <i>region</i>:<i>account-id</i> :network-acl/ <i>nacl-id</i></code>                      |
| Interfaccia di rete Amazon EC2                        | <code>arn:aws:ec2: <i>region</i>:<i>account-id</i> :network-interface/ <i>eni-id</i></code>                 |
| Tabella di routing Amazon EC2                         | <code>arn:aws:ec2: <i>region</i>:<i>account-id</i> :route-table/ <i>route-table-id</i></code>               |
| Gruppo di sicurezza Amazon EC2                        | <code>arn:aws:ec2: <i>region</i>:<i>account-id</i> :security-group/ <i>security-group-id</i></code>         |
| Sottorete Amazon EC2                                  | <code>arn:aws:ec2: <i>region</i>:<i>account-id</i> :subnet/ <i>subnet-id</i></code>                         |
| Volume Amazon EC2                                     | <code>arn:aws:ec2: <i>region</i>:<i>account-id</i> :volume/ <i>volume-id</i></code>                         |
| VPC Amazon EC2                                        | <code>arn:aws:ec2: <i>region</i>:<i>account-id</i> :vpc/ <i>vpc-id</i></code>                               |
| Connessione VPN di Amazon EC2                         | <code>arn:aws:ec2: <i>region</i>:<i>account-id</i> :vpn-connection/ <i>vpn-id</i></code>                    |
| Gateway VPN di Amazon EC2                             | <code>arn:aws:ec2: <i>region</i>:<i>account-id</i> :vpn-gateway/ <i>vgw-id</i></code>                       |
| AWS Elastic Beanstalk applicazione                    | <code>arn:aws:elasticbeanstalk: <i>region</i>:<i>account-id</i> :application/ <i>applicationname</i></code> |

| Nome risorsa                                            | Formato ARN                                                                                                                            |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Elastic Load Balancing (Classic Load Balancer)          | arn:aws:elasticloadbalancing: <i>region</i> : <i>account-id</i> :loadbalancer/ <i>name</i>                                             |
| Elastic Load Balancer (Application Load Balancer)       | arn:aws:elasticloadbalancing: <i>region</i> : <i>account-id</i> :loadbalancer/app/ <i>load-balancer-name</i> / <i>load-balancer-id</i> |
| Elastic Load Balancing (Network Load Balancer)          | arn:aws:elasticloadbalancing: <i>region</i> : <i>account-id</i> :loadbalancer/net/ <i>load-balancer-name</i> / <i>load-balancer-id</i> |
| AWS Identity and Access Management gruppo (IAM)         | arn:aws:iam:: <i>account-id</i> :group/ <i>group-name</i>                                                                              |
| Policy IAM                                              | arn:aws:iam:: <i>account-id</i> :policy/ <i>policy-name</i>                                                                            |
| Ruolo IAM                                               | arn:aws:iam:: <i>account-id</i> :role/ <i>role-name</i>                                                                                |
| Utente IAM                                              | arn:aws:iam:: <i>account-id</i> :user/ <i>user-name</i>                                                                                |
| AWS Lambda funzione                                     | arn:aws:lambda: <i>region</i> : <i>account-id</i> :function: <i>function-name</i>                                                      |
| Cluster Amazon Relational Database Service (Amazon RDS) | arn:aws:rds: <i>region</i> : <i>account-id</i> :cluster: <i>db-cluster-name</i>                                                        |

| Nome risorsa                            | Formato ARN                                                                                                         |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Istanza database Amazon RDS             | <code>arn:aws:rds: <i>region</i>:<i>account-id</i> :db:<i>db-instance-name</i></code>                               |
| Abbonamento Amazon RDS                  | <code>arn:aws:rds: <i>region</i>:<i>account-id</i> :es:<i>subscription-name</i></code>                              |
| Gruppo di sicurezza Amazon RDS          | <code>arn:aws:rds: <i>region</i>:<i>account-id</i> :secgrp:<i>security-group-name</i></code>                        |
| Snapshot del cluster Amazon RDS         | <code>arn:aws:rds: <i>region</i>:<i>account-id</i> :cluster-snapshot: <i>cluster-snapshot-name</i></code>           |
| Gruppo di sottoreti Amazon RDS          | <code>arn:aws:rds: <i>region</i>:<i>account-id</i> :subgrp:<i>subnet-group-name</i></code>                          |
| Cluster Amazon Redshift                 | <code>arn:aws:redshift: <i>region</i>:<i>account-id</i> :cluster: <i>cluster-name</i></code>                        |
| Gruppi parametro Amazon Redshift        | <code>arn:aws:redshift: <i>region</i>:<i>account-id</i> :parametergroup: <i>parameter-group-name</i></code>         |
| Gruppo di sicurezza di Amazon Redshift  | <code>arn:aws:redshift: <i>region</i>:<i>account-id</i> :securitygroup: <i>security-group-name</i></code>           |
| Snapshot del cluster di Amazon Redshift | <code>arn:aws:redshift: <i>region</i>:<i>account-id</i> :snapshot: <i>cluster-name</i> /<i>snapshot-name</i></code> |

| Nome risorsa                                                                  | Formato ARN                                                                                            |
|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Gruppi di sottoreti di Amazon Redshift                                        | <code>arn:aws:redshift: <i>region</i>:<i>account-id</i> :subnetgroup: <i>subnet-group-name</i></code>  |
| Bucket Amazon Simple Storage Service (Amazon S3)                              | <code>arn:aws:s3::: <i>bucket_name</i></code>                                                          |
| AWS Config registrazione dell'inventario dei nodi AWS Systems Manager gestiti | <code>arn:aws:ssm: <i>region</i>:<i>account-id</i> :managed-instance-inventory / <i>node_id</i></code> |
| Associazione State Manager di Systems Manager                                 | <code>arn:aws:ssm: <i>region</i>:<i>account-id</i> :association/ <i>association_ID</i></code>          |

## Aggiungere elementi correlati OpsItems a un OpsItem

Utilizzando Related OpsItems della pagina OpsItemsDettagli, è possibile esaminare i problemi operativi e fornire il contesto per un problema. OpsItem può essere correlato in diversi modi, tra cui una relazione padre-figlio OpsItems, una causa principale o un duplicato. È possibile associare un OpsItem con un altro per visualizzarlo nella sezione OpsItem correlati. È possibile specificare un massimo di 10 ID per altri OpsItems correlati all'OpsItem corrente.

| Related OpsItems (2)     |                                 |        |                         |        |
|--------------------------|---------------------------------|--------|-------------------------|--------|
| <input type="checkbox"/> | ID                              | Status | Title                   | Source |
| <input type="checkbox"/> | <a href="#">oi-0cdb512b47ed</a> | ⌚ Open | EC2 Instance terminated | EC2    |
| <input type="checkbox"/> | <a href="#">oi-06f350858b55</a> | ⌚ Open | EC2 Instance terminated | EC2    |

## Per aggiungere un elemento correlato OpsItem

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli OpsCenter.
3. Scegliere un ID di OpsItem per aprire la pagina dei dettagli.
4. Nella sezione Related (Correlato) OpsItem, scegli Add (Aggiungi).
5. Per ID OpsItem, specifica un ID.

## 6. Scegliere Aggiungi.

### Aggiungere dati operativi a un OpsItem

I dati operativi sono dati personalizzati che forniscono dettagli di riferimento utili riguardo a un OpsItem. È possibile inserire più coppie chiave-valore di dati operativi. Ad esempio, è possibile specificare i file di log, le stringhe di errore, le chiavi di licenza, i suggerimenti per la risoluzione dei problemi o altri dati. La lunghezza massima della chiave può essere di 128 caratteri e la dimensione massima del valore può essere di 20 KB.

| Key            | Value                                                                                                       | Searchable                          | Remove |
|----------------|-------------------------------------------------------------------------------------------------------------|-------------------------------------|--------|
| event-time     | 2019-06-04T00:33:35Z                                                                                        | <input type="checkbox"/>            | Remove |
| instance-state | stopped                                                                                                     | <input type="checkbox"/>            | Remove |
| Log data       | 6093] ata1: PATA max MWDMA2 cmd<br>0x1f0 ctl 0x3f6 bmdma 0xc100 irq 14<br>[ 1.981012] ata2: PATA max MWDMA2 | <input checked="" type="checkbox"/> | Remove |

Add item

È possibile rendere i dati disponibili per la ricerca da parte di altri utenti nell'account oppure limitare l'accesso alla ricerca. I dati sono definiti come "disponibili per la ricerca" quando tutti gli utenti con accesso alla pagina Panoramica dell'OpsItem (risultante dall'operazione API [DescribeOpsItems](#)) possono visualizzare ed effettuare ricerche sui dati specificati. I dati operativi che non sono ricercabili sono visualizzabili solo dagli utenti che hanno accesso a OpsItem (come fornito dal funzionamento dell'[GetOpsItemAPI](#)).

### Per aggiungere dati operativi a un OpsItem

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli OpsCenter.
3. Scegli un ID OpsItem per aprire la rispettiva pagina dei dettagli.
4. Espandi la sezione Dati operativi.
5. Se non esistono dati operativi per l'OpsItem, scegli Aggiungi. Se i dati operativi esistono già per OpsItem, scegliere Manage (Gestisci).

Dopo aver creato i dati operativi, è possibile modificare la chiave e il valore, rimuovere i dati operativi o aggiungere ulteriori coppie chiave-valore scegliendo Manage (Gestisci).

6. Per Key (Chiave), specificare una o più parole per aiutare gli utenti a comprendere lo scopo dei dati.

 Important

Chiavi di dati operativi non può iniziare con il seguente: amazon, aws, amzn, ssm, /amazon, /aws, /amzn, /ssm.

7. Per Value (Valore), specificare i dati.
8. Scegli Save (Salva).

 Note

È possibile filtrare l'OpsItems utilizzando l'operatore Operational data (Dati operativi) nella pagina OpsItems. Nella casella Ricerca, scegli Dati operativi, quindi inserisci una coppia chiave-valore in formato JSON. È necessario immettere la coppia chiave-valore utilizzando il formato seguente: {"key": "*key\_name*", "value": "*a\_value*"}

## Creazione di un incidente per un OpsItem

Utilizzare la procedura seguente per creare manualmente un incidente in cui OpsItem tenerne traccia e gestirlo Strumento di gestione degli incidenti AWS Systems Manager, ovvero uno strumento in AWS Systems Manager. Un incidente è una qualsiasi interruzione o riduzione non pianificata della qualità dei servizi. Per ulteriori informazioni sullo Strumento di gestione degli incidenti, consulta la pagina [the section called “Integra OpsCenter con altri Servizi AWS”](#).

### Come creare manualmente un incidente per un OpsItem

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli OpsCenter.



3. Se lo Strumento di gestione degli incidenti ha creato un OpsItem, scegliilo e vai al passaggio 5. In caso contrario, scegli Crea OpsItem e completa il modulo. Se non visualizzi questo pulsante, seleziona la scheda OpsItems, quindi scegli Crea OpsItem.
4. Se hai creato un nuovo OpsItem, aprilo.
5. Scegli Avvio incidente.
6. Per Piano di risposta, scegli il piano di risposta dello Strumento di gestione degli incidenti che desideri assegnare a questo incidente.
7. (Facoltativo) Per Titolo inserisci un nome descrittivo che aiuti gli altri membri del team a comprendere la natura dell'incidente. Se non inserisci un nuovo titolo, OpsCenter crea il OpsItem e l'incidente corrispondente nello Strumento di gestione degli incidenti utilizzando il titolo nel piano di risposta.
8. (Facoltativo) Per Incident impact (Impatto degli incidenti), scegli un livello di impatto per questo incidente. Se non inserisci un nuovo livello di impatto, OpsCenter crea il OpsItem e l'incidente corrispondente nello Strumento di gestione degli incidenti utilizzando il livello di impatto nel piano di risposta.
9. Scegli Avvia.

## Gestione dei OpsItems duplicati

OpsCenter può ricevere più OpsItems duplicati per una singola origine da più Servizi AWS.

OpsCenter utilizza una combinazione di logica integrata e stringhe di deduplicazione configurabili per evitare la creazione di OpsItems duplicati. AWS Systems Manager applica tale logica integrata di deduplicazione quando viene richiamata l'operazione [Crea OpsItem](#) dell'API.

AWS Systems Manager utilizza la seguente logica di deduplicazione:

1. Quando si crea l'OpsItem, Systems Manager crea e archivia un hash in base alla stringa di deduplicazione e alla risorsa che ha attivato l'OpsItem.
2. Quando viene effettuata un'altra richiesta di creazione di un OpsItem, il sistema controlla la stringa di deduplicazione della nuova richiesta.
3. Se per tale stringa di deduplicazione esiste un hash corrispondente, Systems Manager verifica lo stato dell'OpsItem esistente. Se lo stato di un OpsItem esistente è aperto o in corso, l'OpsItem non viene creato. Se l'OpsItem esistente viene risolto, Systems Manager crea un nuovo OpsItem.

Dopo aver creato un OpsItem, non è possibile modificare o cambiare le stringhe di deduplicazione in tale OpsItem.

Per gestire gli OpsItems duplicati, procedi nel modo seguente:

- Modifica la stringa di deduplicazione per una EventBridge regola Amazon destinata. OpsCenter Per ulteriori informazioni, consulta [Modifica di una stringa di deduplicazione in una regola predefinita EventBridge](#).
- Specifica una stringa di deduplicazione quando crei manualmente un nuovo OpsItem. Per ulteriori informazioni, consulta [Specificare una stringa di deduplicazione utilizzando AWS CLI](#).
- Esamina e risolvi gli OpsItems duplicati utilizzando Approfondimenti operativi. Per risolvere gli OpsItems duplicati, puoi utilizzare i runbook.

Per risolvere gli OpsItems duplicati e ridurre il numero di OpsItems creati da un'origine, Systems Manager fornisce dei runbook Automation. Per informazioni, consulta [Risolvere i duplicati OpsItems basato su approfondimenti](#).

## Modifica di una stringa di deduplicazione in una regola predefinita EventBridge

Utilizzare la procedura seguente per specificare una stringa di deduplicazione per una EventBridge regola mirata. OpsCenter

Per modificare una stringa di deduplicazione per una regola EventBridge

1. Accedi a Console di gestione AWS e apri la EventBridge console Amazon all'indirizzo <https://console.aws.amazon.com/events/>.
2. Nel riquadro di navigazione, scegli Regole.
3. Scegli la regola, quindi seleziona Edit (Modifica).
4. Vai alla pagina Select target(s) (Seleziona destinazioni).
5. Nella sezione Additional settings (Impostazioni aggiuntive), scegli Configure input transformer (Configura il trasformatore di input).
6. Nella casella Template in basso, individua la voce JSON "operationalData": { "/aws/dedup" e le stringhe di deduplicazione da modificare.

L'immissione della stringa di deduplicazione nelle EventBridge regole utilizza il seguente formato JSON.

```
"operationalData": { "/aws/dedup": {"type": "SearchableString","value":
 "{\\"dedupString\\":\\"Words the system should use to check for duplicate
 OpsItems\\"}"}}
```

Ecco un esempio.

```
"operationalData": { "/aws/dedup": {"type": "SearchableString","value":
 "{\\"dedupString\\":\\"SSMOpsCenter-EBS-volume-performance-issue\\"}"}}
```

7. Modifica le stringhe di deduplicazione, quindi scegli Conferma.
8. Scegli Next (Successivo).
9. Scegli Next (Successivo).
10. Scegli Aggiorna regola.

Specificare una stringa di deduplicazione utilizzando AWS CLI

È possibile specificare una stringa di deduplicazione quando si crea manualmente una nuova stringa OpsItem utilizzando la console o il AWS Systems Manager AWS CLI Per informazioni sull'immissione delle stringhe di deduplicazione quando si crea manualmente un OpsItem nella console, consulta [Crea OpsItems manualmente](#). Se utilizzi la AWS CLI, puoi immettere la stringa di deduplicazione per il parametro OperationalData. La sintassi del parametro utilizza JSON, come illustrato nell'esempio seguente.

```
--operational-data '{"/aws/dedup":{"Value":{"\\"dedupString\\": \\"Words the system should
use to check for duplicate OpsItems\\"},"Type":"SearchableString"}}'
```

Ecco un esempio di comando che specifica disk full come stringa di deduplicazione.

Linux & macOS

```
aws ssm create-ops-item \
 --title "EC2 instance disk full" \
 --description "Log clean up may have failed which caused the disk to be full" \
 --priority 1 \
 --source ec2 \
 --operational-data '{"/aws/dedup":{"Value":{"\\"dedupString\\": \\"disk full
\\"},"Type":"SearchableString"}}' \
 --tags "Key=EC2,Value=ProductionServers" \
```

```
--notifications Arn="arn:aws:sns:us-west-1:12345678:TestUser"
```

## Windows

```
aws ssm create-ops-item ^
 --title "EC2 instance disk full" ^
 --description "Log clean up may have failed which caused the disk to be full" ^
 --priority 1 ^
 --source EC2 ^
 --operational-data="{\"/aws/dedup\":{\"Value\": \"{\\\"dedupString\\\":\\\"disk full\\\"}\"},\"Type\": \"SearchableString\"}" ^
 --tags "Key=EC2,Value=ProductionServers" --notifications Arn="arn:aws:sns:us-west-1:12345678:TestUser"
```

## Analisi delle informazioni operative per ridurre OpsItems

OpsCenter gli approfondimenti operativi visualizzano informazioni sui duplicati OpsItems.

OpsCenter analizza automaticamente OpsItems nel tuo account e genera tre tipi di approfondimenti. Puoi visualizzare queste informazioni nella sezione Approfondimenti operativi della scheda Riepilogo di OpsCenter.

- **OpsItems duplicati:** un approfondimento viene generato quando otto o più OpsItems hanno lo stesso titolo per la medesima risorsa.
- **Titoli più comuni:** un approfondimento viene generato quando più di 50 OpsItems hanno lo stesso titolo.
- **Le risorse che generano il maggior numero di risorse OpsItems:** viene generata un'analisi quando una AWS risorsa ne ha più di 10 aperte OpsItems. Questi approfondimenti e le risorse corrispondenti vengono visualizzati nella OpsItems tabella Risorse che generano il maggior numero di risorse della scheda OpsCenter Riepilogo. Le risorse sono elencate in ordine decrescente di numero di OpsItem.

### Note

OpsCenter crea approfondimenti Risorse che generano il maggior numero di OpsItems per i seguenti tipi di risorse:

- Istanze Amazon Elastic Compute Cloud (Amazon EC2)
- Gruppi di sicurezza Amazon EC2

- Gruppo Amazon EC2 Auto Scaling
- Database Amazon Relational Database Service (Amazon RDS)
- Cluster Amazon RDS
- AWS Lambda funzione
- Tabella Amazon DynamoDB
- Bilanciatore del carico Elastic Load Balancing
- Cluster Amazon Redshift
- AWS Certificate Manager certificato
- Volume Amazon Elastic Block Store

OpsCenter impone un limite di 15 approfondimenti per tipo. Se un tipo raggiunge questo limite, OpsCenter interrompe la visualizzazione di ulteriori approfondimenti per quel tipo. Per visualizzare informazioni aggiuntive, è necessario risolvere tutti i problemi OpsItems associati a un OpsInsight documento di quel tipo. Se si impedisce la visualizzazione di un approfondimento in sospeso nella console a causa del limite di 15 approfondimenti, tale approfondimento diventa visibile dopo la chiusura di un altro approfondimento.

Se scegli un approfondimento, OpsCenter visualizza informazioni sulle risorse e sugli OpsItems interessati. Nella screenshot seguente viene presentato un esempio con i dettagli di un'informazione dettagliata OpsItem duplicata.

The screenshot displays the 'Duplicate OpsItems: 1122334455' insight page in the AWS OpsCenter console. The page is divided into two main sections: 'Insight details' and 'Recommended runbooks (1)'.

**Insight details**

|                                                                                                                                                       |                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| <b>Insight type</b><br>Duplicate OpsItems                                                                                                             | <b>Status</b><br>🕒 Open                         |
| <b>Affected OpsItems</b><br>100 🔗                                                                                                                     | <b>Date created</b><br>14 Aug 2020 20:00:00 GMT |
| <b>Affected resources</b><br>i-06bd38270                                                                                                              | <b>Last updated</b><br>5 Sep 2020 20:00:00 GMT  |
| <b>Description</b><br>Multiple unresolved OpsItems have the same title 'EC2 Instance Launch Unsuccessful' and involve the same resource 'i-06bd38270' |                                                 |

**Recommended runbooks (1)**

| Document name                                                             | Description | Execution ID | Start time |
|---------------------------------------------------------------------------|-------------|--------------|------------|
| Bulk resolve all unresolved OpsItems with the title 'EC2 Instance Launch' |             |              |            |

Gli approfondimenti operativi sono disattivati per impostazione predefinita. Per ulteriori informazioni sull'utilizzo degli approfondimenti operativi, consulta gli argomenti riportati di seguito.

## Argomenti

- [Abilitazione degli approfondimenti operativi](#)
- [Risolvere i duplicati OpsItems basato su approfondimenti](#)
- [Disabilitazione di informazioni dettagliate operative](#)

## Abilitazione degli approfondimenti operativi

Puoi abilitare gli approfondimenti operativi nella pagina OpsCenter della console di Systems Manager. Se abiliti gli approfondimenti operativi, Systems Manager crea un ruolo collegato ai servizi AWS Identity and Access Management (IAM) chiamato `AWSServiceRoleForAmazonSSM_OpsInsights`. Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a Systems Manager. Service-linked ruoli sono predefiniti e includono tutte le autorizzazioni richieste dal servizio per chiamare altri Servizi AWS utenti per conto dell'utente. Per ulteriori informazioni sul ruolo collegato al servizio `AWSServiceRoleForAmazonSSM_OpsInsights`, consulta [Utilizzo dei ruoli per creare informazioni operative OpsItems in Systems Manager OpsCenter](#).

### Note

Prendi nota delle seguenti informazioni importanti.

- Le informazioni operative Account AWS sono a carico del tuo. Per ulteriori informazioni, consultare [AWS Systems Manager Prezzi](#).
- OpsCenter aggiorna periodicamente le informazioni dettagliate utilizzando un processo batch. Ciò significa che l'elenco degli approfondimenti visualizzati in OpsCenter può non essere sincronizzato.

Utilizza la seguente procedura per abilitare e visualizzare gli approfondimenti operativi in OpsCenter.

## Abilitazione e visualizzazione degli approfondimenti operativi

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli OpsCenter.

3. Nella casella di messaggio Un approfondimento operativo è disponibile, scegli Abilita. Se non vedi questo messaggio, scorri verso il basso fino alla sezione Approfondimenti operativi e scegli Abilita.
4. Dopo aver abilitato questa funzionalità, nella scheda Riepilogo scorri verso il basso fino alla sezione Approfondimenti operativi.
5. Per visualizzare un elenco filtrato di approfondimenti, scegli il collegamento accanto a Duplica OpsItems, Titoli più comuni o Risorse che generano il maggior numero di OpsItems. Per visualizzare tutte le informazioni dettagliate, scegli View all operational insights (Visualizza tutte le informazioni dettagliate operative).
6. Scegli un ID di informazioni dettagliate per visualizzare ulteriori informazioni.

### Risolvere i duplicati OpsItems basato su approfondimenti

Per la risoluzione delle informazioni dettagliate, è necessario innanzitutto risolvere tutte le OpsItems associate a ognuna di queste. Puoi utilizzare il runbook AWS-BulkResolveOpsItemsForInsight per la risoluzione di OpsItems associato a un'informazione dettagliata.

Per risolvere gli OpsItems duplicati e ridurre il numero di OpsItems creati da un'origine, Systems Manager fornisce i seguenti runbook Automation:

- Il runbook AWS-BulkResolveOpsItems risolve OpsItems che corrispondono a un filtro specificato.
- Il AWS-AddOpsItemDedupStringToEventBridgeRule runbook aggiunge una stringa di deduplicazione per tutte le OpsItem destinazioni associate a una regola Amazon specifica. EventBridge Questo runbook non aggiunge una stringa di deduplicazione se una regola ne ha già una.
- AWS-DisableEventBridgeRuleDisattiva una regola EventBridge se la regola ne genera dozzine o centinaia. OpsItems

### Per risolvere un approfondimento operativo

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli OpsCenter.
3. Nella scheda Overview (Panoramica), scorri verso il basso fino a Operational insights (Informazioni dettagliate operative).

4. Scegli Visualizza tutti gli approfondimenti operativi.
5. Scegli un ID di informazioni dettagliate per visualizzare ulteriori informazioni.
6. Scegli un runbook e scegli Esegui.

## Disabilitazione di informazioni dettagliate operative

Quando disattivi questa funzionalità, il sistema interrompe la creazione di nuovi approfondimenti e ne interrompe la visualizzazione nella console. Sebbene non vengano visualizzati nella console, gli approfondimenti attivi rimangono invariati nel sistema. Se attivi nuovamente questa funzionalità, il sistema visualizza tutti gli approfondimenti non risolti in precedenza e inizia a crearne di nuovi. La seguente procedura consente di disattivare gli approfondimenti operativi.

### Disattivazione degli approfondimenti operativi

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli OpsCenter.
3. Seleziona Impostazioni.
4. Nella sezione Operational insights (Informazioni dettagliate operative), scegli Edit (Modifica), quindi attiva o disattiva l'opzione Disable (Disabilita).
5. Seleziona Save (Salva).

## Visualizzazione di log e report di OpsCenter

AWS CloudTrail registra le chiamate AWS Systems Manager OpsCenter API sulla console, su AWS Command Line Interface (AWS CLI) e sull'SDK. Puoi visualizzare le informazioni nella CloudTrail console o in un bucket Amazon Simple Storage Service (Amazon S3). Amazon S3 utilizza un bucket per archiviare tutti i CloudTrail log del tuo account.

I log delle operazioni OpsCenter mostrano attività di creazione, aggiornamento, ottenimento e descrizione di OpsItem. Per ulteriori informazioni sulla visualizzazione e l'utilizzo dei CloudTrail registri delle attività di Systems Manager, vedere [Registrazione dei log AWS Systems Manager Chiamate API con AWS CloudTrail](#).

AWS Systems Manager OpsCenter fornisce le seguenti informazioni su OpsItems:



- Riepilogo dello stato dell'OpsItem: un riepilogo dell'OpsItems in base allo stato (Aperto e in corso, Aperto o In corso).
- Fonti con la maggior parte delle fonti aperte OpsItems: fornisce una suddivisione della parte superiore Servizi AWS con openOpsItems.
- OpsItems per origine ed età: fornisce un conteggio di OpsItems raggruppati per origine e giorni dalla creazione.

### Visualizzazione del report di riepilogo di OpsCenter

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli OpsCenter.
3. Nella pagina Panoramica di OpsItems, scegli Riepilogo.
4. In OpsItems per origine ed età, scegli la barra di ricerca per filtrare OpsItems in base alla voce Origine. Utilizza l'elenco per filtrare in base alla voce Stato.

### Elimina OpsItems

Puoi eliminare una persona OpsItem chiamando l'operazione [Delete OpsItem](#) API utilizzando AWS Command Line Interface o l' AWS SDK. Non è possibile eliminare un OpsItem nella Console di gestione AWS. Per eliminare unOpsItem, l'utente, il gruppo o il ruolo AWS Identity and Access Management (IAM) deve disporre dell'autorizzazione o dell'autorizzazione di amministratore per chiamare l'operazione `DeleteOpsItem` API.

#### Important

Presta attenzione alle seguenti informazioni importanti su questa operazione.

- L'eliminazione di un OpsItem è irreversibile. Non è possibile recuperare un OpsItem eliminato.
- Questa operazione utilizza un modello di consistenza finale, il che significa che il sistema può impiegare alcuni minuti per completare l'operazione. Se elimini un OpsItem e chiami immediatamente, ad esempio, [GetOpsItem](#), l'OpsItem eliminato potrebbe comunque apparire nella risposta.
- Questa operazione è idempotente. Il sistema non genera un'eccezione se chiami ripetutamente questa operazione per lo stesso OpsItem. Se la prima chiamata ha esito

positivo, tutte le chiamate aggiuntive restituiscono la stessa risposta positiva della prima chiamata.

- Questa operazione non supporta le chiamate multi-account. Un amministratore delegato o un account di gestione non può eliminare OpsItems in altri account, anche se OpsCenter è stato impostato per l'amministrazione multi-account. Per ulteriori informazioni sull'accesso multi-account, consulta [\(Facoltativo\) Configurazione OpsCenter per gestire centralmente OpsItems tra gli account](#).
- Se ricevi `OpsItemLimitExceededException`, puoi eliminare uno o più OpsItems per ridurre il numero totale di OpsItems sotto i limiti di quota. Per ulteriori informazioni su questa eccezione, consulta [Risoluzione dei problemi con OpsCenter](#).

## Eliminazione di un OpsItem

Per eliminare un OpsItem, utilizza la procedura seguente.

Per eliminare un OpsItem

1. Installa e configura AWS CLI se non l'hai già fatto. Per ulteriori informazioni, consulta [Installare o aggiornare la versione più recente della AWS CLI](#).
2. Eseguire il seguente comando seguente. Sostituisci **ID** con l'ID della OpsItem persona che desideri eliminare.

```
aws ssm delete-ops-item --ops-item-id ID
```

In caso di esito positivo, il comando non restituisce alcun dato.

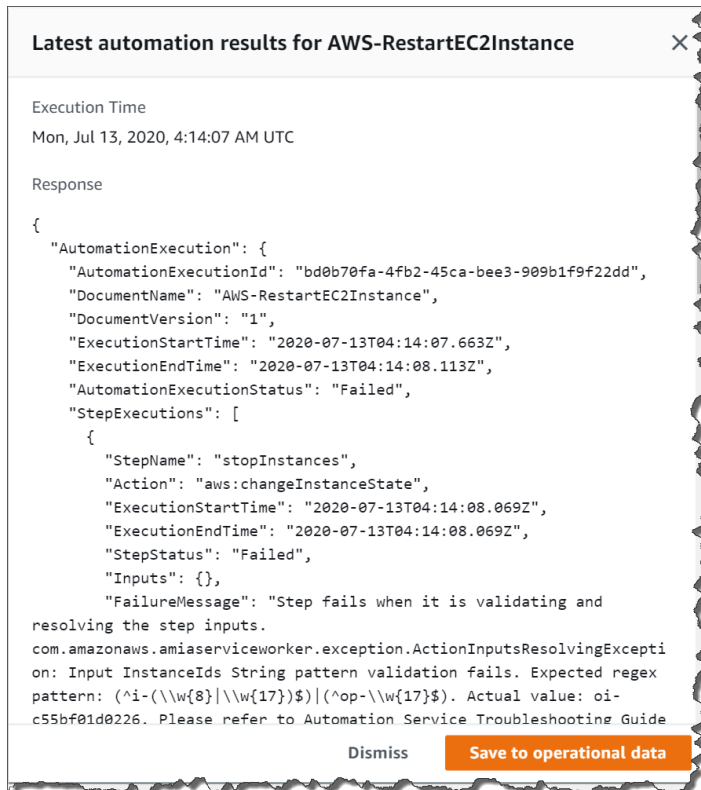
## Rimediare OpsItem problemi

Utilizzando i runbook di AWS Systems Manager automazione, è possibile risolvere i problemi relativi alle AWS risorse identificate in un. OpsItem L'automazione utilizza runbook predefiniti per risolvere problemi comuni relativi alle risorse. AWS

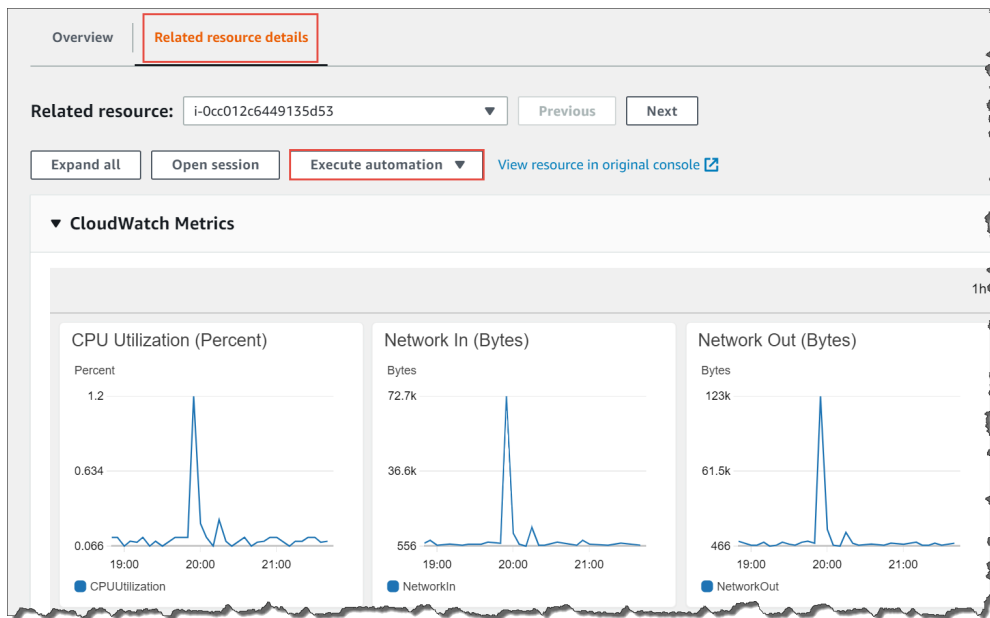
Ogni OpsItem include la sezione Runbook, che fornisce un elenco di runbook che è possibile utilizzare per la correzione. Quando scegli un runbook Automation dall'elenco, OpsCenter visualizza automaticamente alcuni dei campi obbligatori per l'esecuzione del documento. Quando esegui un runbook Automation, il sistema associa il runbook alla risorsa correlata all'OpsItem. Se Amazon

EventBridge crea un fileOpsItem, associa un runbook a. OpsItem OpsCenterconserva un registro di 30 giorni di runbook di automazione per un. OpsItem

Puoi scegliere uno stato per visualizzare dettagli importanti sul runbook, ad esempio il motivo per cui un'automazione non è riuscita e il passaggio del runbook Automation che era in esecuzione al verificarsi dell'errore, come illustrato nell'esempio seguente.



La pagina Dettagli relativi alle risorse per un OpsItem selezionato include l'elenco Esegui automazione. Puoi scegliere runbook Automation recenti o specifici per una risorsa ed eseguirli per risolvere i problemi. Questa pagina include anche i fornitori di dati, tra cui CloudWatch metriche e allarmi di Amazon, AWS CloudTrail log e dettagli di. AWS Config



È possibile visualizzare informazioni su un runbook Automation scegliendo il nome nella console o utilizzando [Riferimento al runbook dell'Automazione Systems Manager](#).

## Riparazione di un OpsItem utilizzando un runbook

Prima di eseguire un runbook di Automazione per correggere un problema di OpsItem, esegui queste operazioni:

- Verifica di disporre dell'autorizzazione per eseguire i runbook Automation di Systems Manager. Per ulteriori informazioni, consulta [Configurazione del servizio di automazione](#).
- Raccogli informazioni di ID specifiche delle risorse per l'automazione che desideri eseguire. Ad esempio, per eseguire un'automazione che riavvia un'istanza EC2, è necessario specificare l'ID dell'istanza EC2 da riavviare.

## Eseguire un runbook di automazione per correggere un OpsItem issue

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli OpsCenter.
3. Scegliere l'ID OpsItem per aprire la pagina dei dettagli.

| ID                              | Title                   | Status | Source |
|---------------------------------|-------------------------|--------|--------|
| <a href="#">oi-a80f1dbb4464</a> | EC2 instance stopped    | Open   | EC2    |
| <a href="#">oi-0cdb512b47ed</a> | EC2 instance terminated | Open   | EC2    |
| <a href="#">oi-06f350858b55</a> | EC2 instance terminated | Open   | EC2    |

4. Scorri alla sezione Runbook.
5. Utilizza il riquadro di ricerca o i numeri nell'angolo in alto a destra per trovare il runbook Automation che desideri eseguire.
6. Scegli un runbook ed Esegui.
7. Inserisci le informazioni necessarie per il runbook e scegli Invia.

Una volta avviato il runbook, il sistema torna alla schermata precedente e ne visualizza lo stato.

8. Nella sezione Esecuzioni di automazione negli ultimi 30 giorni, scegli il link ID esecuzione per visualizzare i passaggi e lo stato dell'esecuzione.

### Riparazione di un OpsItem utilizzando un runbook associato

Dopo aver eseguito un runbook Automation da un OpsItem, OpsCenter associa il runbook all'OpsItem. Un runbook associato ha una posizione più alta in classifica rispetto ad altri runbook nell'elenco Runbook.

Utilizza la procedura seguente per eseguire un runbook Automation già associato a una delle risorse correlate in un OpsItem. Per informazioni sull'aggiunta di risorse correlate, consulta [Manage \(Gestione\) OpsItems](#).

### Eseguire un runbook associato a una risorsa per correggere un OpsItem issue

1. Apri AWS Systems Manager la console <https://console.aws.amazon.com/systems-manager/> all'indirizzo.
2. Nel pannello di navigazione, scegli OpsCenter.
3. Apri la OpsItem.
4. Nella sezione Risorse correlate, scegli la risorsa sulla quale si desidera eseguire un runbook di automazione.
5. Scegli Esegui automazione, quindi scegli il runbook di automazione associato che si desidera eseguire.
6. Inserisci le informazioni necessarie per il runbook e scegli Esegui.

Una volta avviato il runbook, il sistema torna alla schermata precedente e ne visualizza lo stato.

7. Nella sezione Esecuzioni di automazione negli ultimi 30 giorni, scegli il link ID esecuzione per visualizzare i passaggi e lo stato dell'esecuzione.

## Visualizzazione dei report di riepilogo OpsCenter

AWS Systems Manager OpsCenter include una pagina di riepilogo che visualizza automaticamente le informazioni riportate di seguito.

- Riepilogo dello stato di OpsItem: un riepilogo di OpsItems per stato, ad esempio Open e In progress.
- Fonti con la maggior parte delle fonti aperte OpsItems: una suddivisione delle parti superiori Servizi AWS che sono aperteOpsItems.
- OpsItems per origine ed età: un conteggio di OpsItems raggruppati per origine e giorni dalla creazione.

Per visualizzare i report di riepilogo di OpsCenter

1. Apri la AWS Systems Manager console su <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli OpsCenter, quindi scegli la scheda Riepilogo.
3. Nella sezione OpsItems per origine ed età, esegui le seguenti operazioni:
  1. (Facoltativo) Nel campo del filtro, scegli Origine, seleziona Equal, Begin With o Not Equal, quindi inserisci un parametro di ricerca.
  2. Nell'elenco adiacente, seleziona uno dei seguenti valori di stato:
    - Open
    - In progress
    - Resolved
    - Open and in progress
    - All

## Risoluzione dei problemi con OpsCenter

In questo argomento vengono fornite informazioni utili per risolvere problemi e errori comuni relativi a OpsCenter.

Riceverai il `OpsItemLimitExceededException`

Se hai Account AWS raggiunto il numero massimo di utenti `OpsItems` consentiti quando chiami l'operazione `CreateOpsItem` API, ricevi un `OpsItemLimitExceededException`. OpsCenter restituisce l'eccezione se la chiamata supera il numero massimo di `OpsItems` per una delle seguenti quote:

- Numero totale di chiamate `OpsItems` Account AWS per regione (incluso `Open` e `Resolved` `OpsItems`): 500.000
- Numero massimo di `OpsItems` persone al Account AWS mese: 10.000

Queste quote si applicano a `OpsItems` creati da qualsiasi origine ad eccezione delle seguenti:

- `OpsItems` creati dai AWS Security Hub CSPM risultati
- `OpsItems` generati in automatico all'apertura di un incidente dello Strumento di gestione degli incidenti

Gli `OpsItems` creati da tali origini non vengono conteggiati nelle tue quote `OpsItem`, ma ti verranno addebitati i costi per ogni `OpsItem`.

Se ne ricevi un `OpsItemLimitExceededException`, puoi eliminare manualmente `OpsItems` finché non scendi al di sotto della quota che ti impedisce di creare un nuovo `OpsItem`. Anche in questo caso, l'eliminazione dei risultati `OpsItems` creati per gli incidenti di Security Hub CSPM o di Incident Manager non ridurrà il numero totale di elementi `OpsItems` applicati dalle quote. È necessario procedere all'eliminazione di `OpsItems` da altre origini. Per informazioni sull'eliminazione di un `OpsItem`, consulta [Elimina OpsItems](#).

Riceverai una fattura ingente da AWS per un gran numero di generati automaticamente `OpsItems`

Se hai configurato l'integrazione con AWS Security Hub CSPM, OpsCenter crea `OpsItems` per Security Hub i risultati CSPM. A seconda del numero di risultati generati da Security Hub CSPM e dell'account a cui hai effettuato l'accesso al momento della configurazione dell'integrazione, OpsCenter può generarne un numero elevato, a un costo `OpsItems`. Ecco dettagli più specifici relativi ai risultati `OpsItems` generati da Security Hub CSPM:

- Se hai effettuato l'accesso all'account amministratore CSPM di Security Hub durante la configurazione OpsCenter e l'integrazione di Security Hub CSPM, il sistema crea i risultati nell'amministratore e in tutti OpsItems gli account dei membri. Gli OpsItems sono tutti creati nell'account amministratore. A seconda di una serie di fattori, ciò può portare a una fattura inaspettatamente elevata da parte di AWS.

Se hai effettuato l'accesso a un account membro quando configuri l'integrazione, il sistema crea OpsItems solo per gli esiti di quel singolo account. Per ulteriori informazioni sull'account amministratore CSPM di Security Hub, sugli account dei membri e sulla loro relazione con il feed degli EventBridge eventi per i risultati, consulta [Tipi di integrazione con Security Hub CSPM nella Guida per l'utente. EventBridge](#) AWS Security Hub

- Per ogni esito che crea un OpsItem, ti viene addebitato il prezzo normale per la creazione dell'OpsItem. Ti verrà inoltre addebitato un costo se modifichi OpsItem o se il risultato corrispondente viene aggiornato in Security Hub CSPM (che attiva un aggiornamento). OpsItem
- OpsItems creati da un'integrazione con non AWS Security Hub CSPM sono attualmente limitati dalla quota massima di 500.000 OpsItems per account in una regione. È quindi possibile che gli avvisi CSPM di Security Hub creino più di 500.000 addebitabili OpsItems in ciascuna regione in un account.

Per gli ambienti ad alta produzione, consigliamo pertanto di limitare l'ambito dei risultati del CSPM di Security Hub ai soli problemi di elevata gravità.

#### Important

Se ritieni che un numero elevato di dati sia OpsItems stato creato per errore e che la tua AWS fattura sia ingiustificata, contattaci. Supporto

Utilizza la seguente procedura se non desideri più che il sistema crei i risultati CSPM OpsItems di Security Hub.

Per interrompere la ricezione OpsItems per i risultati del Security Hub CSPM

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli OpsCenter.
3. Seleziona Impostazioni.



4. Nella sezione dei risultati del Security Hub CSPM, scegli Modifica.
5. Scegli il cursore per passare da Abilitato a Disabilitato. Se non riesci ad attivare il cursore, Security Hub CSPM non è stato abilitato per il tuo Account AWS.
6. Scegli Salva per salvare la configurazione. OpsCenter non crea più in OpsItems base ai risultati del CSPM di Security Hub.

 Important

Se riporta l'impostazione OpsCenter su Abilitato e continua a creare OpsItems in base ai risultati, accedi all'account amministratore delegato di Systems Manager o all'account di AWS Organizations gestione e ripeti questa procedura. Se non disponi dell'autorizzazione per accedere a nessuno di tali account, contatta l'amministratore e chiedigli di ripetere questa procedura per disabilitare l'integrazione per il tuo account.

## Utilizzo delle CloudWatch dashboard Amazon ospitate da Systems Manager

CloudWatch Le dashboard di Amazon sono home page personalizzabili nella console. CloudWatch Puoi utilizzarli per monitorare le tue risorse in un'unica visualizzazione, anche le risorse distribuite su più aree. Regioni AWS Puoi utilizzare CloudWatch le dashboard per creare visualizzazioni personalizzate delle metriche e degli allarmi per le tue risorse. AWS Con i pannelli di controllo è possibile creare quanto segue:

- Una visualizzare singola per i parametri e gli allarmi selezionati che consentono di valutare l'integrità delle risorse e applicazioni su una o più Regioni AWS. È possibile selezionare il colore utilizzato per ogni parametro su ogni grafico, in modo da monitorare facilmente lo stesso parametro su più grafici.
- Un playbook operativo che fornisce ai membri del team linee guida su come reagire a incidenti specifici durante gli eventi operativi.
- Una vista comune delle misure delle risorse e delle applicazioni critiche che possono essere condivise con i membri del team per velocizzare il flusso di comunicazione durante gli eventi operativi.

Puoi creare dashboard utilizzando la console, AWS Command Line Interface (AWS CLI) o utilizzando l'API. CloudWatch PutDashboard Per ulteriori informazioni, consulta [Usare le CloudWatch dashboard di Amazon](#) nella Amazon CloudWatch User Guide.

# Lavorare con Agente SSM

AWS Systems Manager Agent (SSM Agent) è un software Amazon che viene eseguito su istanze Amazon Elastic Compute Cloud (Amazon EC2), dispositivi edge, server locali e macchine virtuali (VM). SSM Agent consente a Systems Manager di aggiornare, gestire e configurare queste risorse. L'agente elabora le richieste dal servizio Systems Manager in Cloud AWS, quindi le esegue come specificato nella richiesta. SSM Agent invia quindi le informazioni sullo stato e sull'esecuzione al servizio Systems Manager utilizzando [Amazon Message Gateway Service](#) (ssmmessages). (Se Regioni AWS lanciato prima del 2024, le informazioni sullo stato e sull'esecuzione potrebbero essere restituite anche dal [Amazon Message Delivery Service](#) (prefisso del servizio:ec2messages).)

Se monitorate il traffico, noterete che i nodi gestiti comunicano con gli endpoint e possibilmente con gli ssmmessages.\* endpoint. ec2messages.\* Per ulteriori informazioni, consulta [Referenza: ec2messages, ssmmessages e altre operazioni API](#). Per informazioni sulla portabilità dei SSM Agent log su Amazon CloudWatch Logs, consulta. [Registrazione e monitoraggio AWS Systems Manager](#)

## Indice

- [Scopri i dettagli tecnici sul Agente SSM](#)
- [Trova AMI con il Agente SSM preinstallato](#)
- [Utilizzo di SSM Agent sulle istanze EC2 per Linux](#)
- [Utilizzo di SSM Agent sulle istanze EC2 per macOS](#)
- [Lavorare con Agente SSM su istanze EC2 per Windows Server](#)
- [Verifica Agente SSM stato e avvio dell'agente](#)
- [Verifica del Agente SSM numero di versione](#)
- [Visualizzazione Agente SSM log](#)
- [Limitare l'accesso ai comandi a livello di root tramite SSM Agent](#)
- [Automatizzazione degli aggiornamenti a Agente SSM](#)
- [Abbonarsi a Agente SSM notifiche](#)
- [Risoluzione dei problemi Agente SSM](#)

## Scopri i dettagli tecnici sul Agente SSM

Utilizzate le informazioni contenute in questo argomento per implementare AWS Systems Manager Agent (SSM Agent) e capire come funziona l'agente.

## Argomenti

- [Agente SSM comportamento delle credenziali della versione 3.2.x.x](#)
- [Agente SSM precedenza delle credenziali](#)
- [Configurazione Agente SSM da utilizzare con il Federal Information Processing Standard \(FIPS\)](#)
- [Informazioni sull'account ssm-user locale](#)
- [Agente SSM e Servizio di metadati dell'istanza \(IMDS\)](#)
- [Mantenendo Agente SSM aggiornato](#)
- [Garantire che il Agente SSM la directory di installazione non venga modificata, spostata o eliminata](#)
- [Agente SSM aggiornamenti continui di Regioni AWS](#)
- [Agente SSM comunicazioni con AWS bucket S3 gestiti](#)
- [Agente SSM on GitHub](#)
- [Comprensione Agente SSM ibernazione](#)

## Agente SSM comportamento delle credenziali della versione 3.2.x.x

SSM Agent memorizza un set di credenziali temporanee in `/var/lib/amazon/ssm/credentials` (per Linux e macOS) o `%PROGRAMFILES%\Amazon\SSM\credentials` (per Windows Server) quando si esegue l'onboarding di un'istanza utilizzando la funzionalità Configurazione di gestione host predefinita in Quick Setup. Le credenziali temporanee dispongono delle autorizzazioni specificate per il ruolo IAM scelto per la funzionalità Configurazione gestione host predefinita. Su Linux, solo l'account root può accedere a queste credenziali. Su Windows Server, solo l'account SYSTEM e gli amministratori locali possono accedere a queste credenziali.

## Agente SSM precedenza delle credenziali

In questa sezione sono riportate informazioni importanti su come SSM Agent ha l'autorizzazione per eseguire operazioni sulle risorse dell'utente.

### Note

Il supporto per i dispositivi edge è leggermente diverso. È necessario configurare i dispositivi edge per utilizzare il software AWS IoT Greengrass Core, configurare un ruolo di servizio AWS Identity and Access Management (IAM) e SSM Agent distribuirli sui dispositivi

utilizzando. AWS IoT Greengrass Per ulteriori informazioni, consulta [Gestione dei dispositivi edge con Systems Manager](#).

Quando l'SSM Agent è installato su una macchina, richiede le autorizzazioni per comunicare con il servizio Systems Manager. Nelle istanze di Amazon Elastic Compute Cloud (Amazon EC2), queste autorizzazioni vengono fornite in un profilo collegato con l'istanza. Su una macchina non EC2, SSM Agent normalmente ottiene le autorizzazioni necessarie dal file delle credenziali condivise, che si trova in `/root/.aws/credentials` (Linux e macOS) o `%USERPROFILE%\aws\credentials` (Windows Server). Le autorizzazioni necessarie vengono aggiunte a questo file durante il processo di [attivazione ibrida](#). Se un nodo attivato da un sistema ibrido viene annullato, l'agente può entrare in modalità di ibernazione. Per ulteriori informazioni, consulta [Comprensione Agente SSM ibernazione](#).

In rari casi, tuttavia, una macchina potrebbe ritrovarsi autorizzazioni aggiunte a più di una delle posizioni in cui SSM Agent controlla le autorizzazioni per eseguire le sue attività.

Ad esempio, immaginiamo che tu abbia configurato un'istanza EC2 perché fosse gestita da Systems Manager. Questa configurazione include il collegamento di un profilo dell'istanza. Tuttavia, si può decidere di utilizzare tale istanza anche per le attività di sviluppatore o utente finale e di installarvi il AWS Command Line Interface (AWS CLI). Questa installazione comporta l'aggiunta di ulteriori autorizzazioni a un file di credenziali nell'istanza.

Quando si esegue un comando di Systems Manager sull'istanza, SSM Agent potrebbe provare a utilizzare credenziali diverse da quelle previste, ad esempio da un file di credenziali anziché da un profilo dell'istanza. Questo perché SSM Agent cerca le credenziali nell'ordine prescritto per la catena di provider di credenziali predefinita.

#### Note

Su Linux e macOS, SSM Agent funziona come utente root. Di conseguenza, le variabili di ambiente e i file delle credenziali che SSM Agent cerca in questo processo sono solo quelli dell'utente root (`/root/.aws/credentials`). Durante la ricerca delle credenziali, SSM Agent non esamina le variabili di ambiente o il file delle credenziali di altri utenti sull'istanza.

La catena di provider predefinita cerca le credenziali nel seguente ordine:

1. Variabili di ambiente, se configurate (`AWS_ACCESS_KEY_ID` e `AWS_SECRET_ACCESS_KEY`).

2. File delle credenziali condiviso (\$HOME/.aws/credentials per Linux e macOS o %USERPROFILE%\.aws\credentials per Windows Server) con autorizzazioni fornite, ad esempio, da un'attivazione ibrida o da un'installazione di AWS CLI .
3. Un ruolo AWS Identity and Access Management (IAM) per le attività se è presente un'applicazione che utilizza una definizione di attività o un'operazione API di Amazon Elastic Container Service (Amazon ECS). RunTask
4. Collegare un profilo dell'istanza a un'istanza Amazon EC2
5. Il ruolo IAM scelto per la funzionalità Configurazione di gestione host predefinita.

Per le relative informazioni, consultare i seguenti argomenti:

- Profili dell'istanza per istanze EC2: [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#)
- Attivazioni ibride: [crea un'attivazione ibrida per registrare i nodi con Systems Manager](#)
- AWS CLI credenziali: [configurazione e impostazioni dei file delle credenziali](#) nella Guida per l'utente AWS Command Line Interface
- Catena di provider di credenziali predefinita: [Specificare le credenziali](#) nella Guida per gli sviluppatori di AWS SDK per Go

#### Note

Questo argomento nella Guida per gli sviluppatori di AWS SDK per Go descrive la catena di provider predefinita dal punto di vista di SDK for Go; tuttavia, gli stessi principi si applicano alla valutazione delle credenziali per SSM Agent.

## Configurazione Agente SSM da utilizzare con il Federal Information Processing Standard (FIPS)

Se è necessario utilizzare Systems Manager con moduli crittografici convalidati dal Federal Information Processing Standard (FIPS) 140-3, è possibile configurare AWS Systems Manager Agent (SSM Agent) per utilizzare gli endpoint FIPS nelle regioni supportate.

Per configurare Agente SSM per connettersi agli endpoint FIPS 140-3

1. Connessione al nodo gestito.

2. Passa alla directory che contiene il file `amazon-ssm-agent.json`:
  - Linux: `/etc/amazon/ssm/`
  - macOS: `/opt/aws/ssm/`
  - Windows Server: `C:\Program Files\Amazon\SSM\`
3. Aprire il file denominato `amazon-ssm-agent.json` per la modifica.

 Tip

Se non esiste ancora alcun file `amazon-ssm-agent.json`, copia il contenuto di `amazon-ssm-agent.json.template` in un nuovo file denominato `amazon-ssm-agent.json`. Save (Salva) `amazon-ssm-agent.json` nella stessa directory dove `amazon-ssm-agent.json.template` si trova.

4. Aggiungi i seguenti contenuti al file. Sostituisci i valori *region* segnato con il codice regionale appropriato per la tua partizione:

```
{
 ---Existing file content, if any---
 "Mds": {
 "Endpoint": "ec2messages-fips.region.amazonaws.com",
 },
 "Ssm": {
 "Endpoint": "ssm-fips.region.amazonaws.com",
 },
 "Mgs": {
 "Endpoint": "ssmmessages-fips.region.amazonaws.com",
 "Region": "region"
 },
 "S3": {
 "Endpoint": "s3-fips.dualstack.region.amazonaws.com",
 "Region": region
 },
 "Kms": {
 "Endpoint": "kms-fips.region.amazonaws.com"
 }
}
```

Le regioni supportate includono quanto segue:

- `us-east-1` per la Regione Stati Uniti orientali (Virginia settentrionale)
- `us-east-2` per la Regione Stati Uniti orientali (Ohio)
- `us-west-1` per Regione Stati Uniti occidentali (California settentrionale)
- `us-west-2` per la Regione Stati Uniti occidentali (Oregon)
- `ca-west-1` per la Regione Canada occidentale (Calgary)

5. Salvare il file e riavviare l'SSM Agent.

Ogni volta che si modifica la configurazione, riavviare SSM Agent.

È possibile personalizzare altre funzionalità di SSM Agent utilizzando la stessa procedura. Per un elenco aggiornato delle proprietà di configurazione disponibili e dei relativi valori predefiniti, consulta [Config Property Definitions](#) nel repository in. `amazon-ssm-agent` GitHub

Per ulteriori informazioni sul AWS supporto per FIPS, vedere [Federal Information Processing Standard \(FIPS\) 140-3](#).

## Informazioni sull'account `ssm-user` locale

A partire dalla versione 2.3.50.0 di SSM Agent, l'agente crea un account utente locale denominato `ssm-user` e lo aggiunge alla directory di `/etc/sudoers.d` (Linux e macOS) o al gruppo Administrators (Windows Server). Nelle versioni dell'agente precedenti alla 2.3.612.0, l'account viene creato la prima volta che SSM Agent viene avviato o riavviato dopo l'installazione. Nella versione 2.3.612.0 e successive, l'account `ssm-user` viene creato la prima volta che una sessione viene avviata su un'istanza. Questo `ssm-user` è l'utente predefinito del sistema operativo all'avvio di una sessione. Session Manager È possibile modificare le autorizzazioni spostando `ssm-user` in un gruppo con meno privilegi o cambiando il file `sudoers`. Quando si disinstalla SSM Agent, l'account `ssm-user` non viene rimosso dal sistema.

Windows ServerAttivato, SSM Agent gestisce l'impostazione di una nuova password per l'`ssm-user` account all'avvio dell'agente SSM e all'avvio di ogni sessione. Nessuna password viene impostata per `ssm-user` su istanze gestite Linux.

A partire dalla versione di SSM Agent 2.3.612.0, l'account `ssm-user` non viene creato automaticamente sui computer Windows Server utilizzati come controller di dominio. Per utilizzare Session Manager su un controller di dominio Windows Server, creare l'account `ssm-user` manualmente, se non è già presente, e assegnare le autorizzazioni di amministratore di dominio all'utente.



 Important

Per creare l'`ssm-useraccount`, il profilo dell'istanza collegato all'istanza deve fornire le autorizzazioni necessarie. Per informazioni, consulta [Fase 2: Verifica o aggiungi le autorizzazioni dell'istanza per Session Manager](#).

## Agente SSM e Servizio di metadati dell'istanza (IMDS)

Per funzionare correttamente Systems Manager si basa sui metadati dell'istanza EC2. Systems Manager può accedere ai metadati dell'istanza utilizzando la versione 1 o la versione 2 di Instance Metadata Service (IMDSv1 e IMDSv2). L'istanza deve essere in grado di accedere all'indirizzo IPv4 del servizio di metadati dell'istanza: 169.254.169.254. Per ulteriori informazioni, consulta [Metadati e dati dell'utente delle istanze](#) nella Guida per l'utente di Amazon EC2.

## Mantenendo Agente SSM aggiornato

Una versione aggiornata di SSM Agent viene distribuita ogni volta che vengono aggiunti nuovi strumenti a Systems Manager o eseguiti aggiornamenti degli strumenti esistenti. Il mancato utilizzo della versione più recente dell'agente può impedire al nodo gestito di utilizzare vari strumenti e funzionalità di Systems Manager. Per questo motivo, ti consigliamo di automatizzare il processo di aggiornamento di SSM Agent sulle macchine. Per informazioni, consulta [Automatizzazione degli aggiornamenti a Agente SSM](#). Iscriviti alla pagina [Note di rilascio di SSM Agent](#) su GitHub per ricevere notifiche sugli aggiornamenti di SSM Agent.

 Note

Una versione aggiornata di SSM Agent viene distribuita ogni volta che vengono aggiunti nuovi strumenti a Systems Manager o eseguiti aggiornamenti degli strumenti esistenti. Il mancato utilizzo della versione più recente dell'agente può impedire al nodo gestito di utilizzare vari strumenti e funzionalità di Systems Manager. Per questo motivo, ti consigliamo di automatizzare il processo di aggiornamento di SSM Agent sulle macchine. Per informazioni, consulta [Automatizzazione degli aggiornamenti a Agente SSM](#). Iscriviti alla pagina [Note di rilascio di SSM Agent](#) su GitHub per ricevere notifiche sugli aggiornamenti di SSM Agent. Le Amazon Machine Images (AMIs) che includono SSM Agent per impostazione predefinita possono impiegare fino a due settimane per essere aggiornate con la versione più recente di

SSM Agent. Consigliamo di configurare aggiornamenti automatici di SSM Agent ancora più frequenti.

## Garantire che il Agente SSM la directory di installazione non venga modificata, spostata o eliminata

SSM Agent sia installato in `/var/lib/amazon/ssm/` (Linux e macOS) e `%PROGRAMFILES%\Amazon\SSM\` (Windows Server). Queste directory di installazione contengono file e cartelle critici utilizzati da SSM Agent, ad esempio un file di credenziali, risorse per la comunicazione tra processi (IPC) e cartelle di orchestrazione. Nulla all'interno della directory di installazione deve essere modificato, spostato o eliminato. In caso contrario, SSM Agent potrebbe smettere di funzionare correttamente.

## Agente SSM aggiornamenti continui di Regioni AWS

Una volta reso disponibile un SSM Agent aggiornamento nel relativo GitHub archivio, possono essere necessarie fino a due settimane prima che la versione aggiornata venga distribuita a tutti Regioni AWS in momenti diversi. Per questo motivo, è possibile che venga visualizzato l'errore “Non supportato sulla piattaforma corrente” o “aggiornamento di amazon-ssm-agent a una versione precedente, abilitare il downgrade per procedere” quando si tenta di distribuire una nuova versione di SSM Agent in una regione.

Per determinare la versione di SSM Agent disposizione per l'utente, è possibile eseguire un comando `curl`.

Per visualizzare la versione dell'agente disponibile nel bucket di download globale, eseguire il comando seguente.

```
curl https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/VERSION
```

Per visualizzare la versione dell'agente disponibile in una regione specifica, esegui il comando seguente, sostituendolo *region* con la regione in cui stai lavorando, ad esempio la regione Stati Uniti orientali (Ohio). `us-east-2`

```
curl https://s3.region.amazonaws.com/amazon-ssm-region/latest/VERSION
```

È possibile anche aprire il file `VERSION` direttamente nel browser senza un comando `curl`.

## Agente SSM comunicazioni con AWS bucket S3 gestiti

Nel corso dell'esecuzione di varie operazioni di Systems Manager, AWS Systems Manager Agent (SSM Agent) accede a diversi bucket Amazon Simple Storage Service (Amazon S3). Questi bucket S3 sono accessibili pubblicamente e, per impostazione predefinita, l'SSM Agent si connette con essi usando chiamate HTTP.

Tuttavia, se utilizzi un endpoint cloud privato virtuale (VPC) nelle operazioni di Systems Manager, devi fornire un'autorizzazione esplicita in un profilo dell'istanza Amazon Elastic Compute Cloud (Amazon EC2) per Systems Manager o in un ruolo di servizio per le macchine non EC2 in un ambiente [ibrido e multicloud](#). In caso contrario, le risorse non accedono a questi bucket pubblici.

Per concedere l'accesso dei nodi gestiti a questi bucket quando utilizzi un endpoint VPC, devi creare una policy di autorizzazioni Amazon S3 personalizzata e collegarla al profilo dell'istanza (per le istanze EC2) o al ruolo del servizio (per i nodi gestiti non EC2).

Per informazioni sull'utilizzo dell'endpoint di un cloud privato virtuale (VPC) nelle operazioni di Systems Manager, consulta [Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager](#).

### Note

Queste autorizzazioni forniscono solo l'accesso ai bucket AWS gestiti richiesti da SSM Agent. Non forniscono le autorizzazioni necessarie per altre operazioni Amazon S3. Inoltre, non offrono l'autorizzazione per i propri bucket S3.

Per ulteriori informazioni, consulta i seguenti argomenti:

- [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#)
- [Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud](#)
- [Riferimento: bucket Amazon S3 per operazioni di applicazione di patch](#)

### Indice

- [Autorizzazioni dei bucket necessarie](#)
- [Esempio](#)
- [Convalida di macchine attivate da sistemi tramite un'impronta digitale hardware](#)

## Autorizzazioni dei bucket necessarie

La tabella seguente descrive ciascuno dei bucket S3 di cui SSM Agent potrebbe aver bisogno per accedere alle operazioni di Systems Manager.

### Note

*region* rappresenta l'identificatore di una regione AWS supportata da AWS Systems Manager, ad esempio `us-east-2` per la regione Stati Uniti orientali (Ohio). Per un elenco dei *region* valori supportati, vedere la colonna Regione negli endpoint [del servizio](#) Systems Manager in. Riferimenti generali di Amazon Web Services

### Autorizzazioni di Amazon S3 richieste da SSM Agent

| ARN di bucket S3                                                | Description                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>arn:aws:s3:::aws-windows-downloads-<i>region</i>/*</code> | Richiesto per alcuni documenti SSM che supportano solo i sistemi operativi Windows Server, oltre ad alcuni per il supporto multipiattaforma, come <code>AWSEC2-ConfigureSTIG</code> .                                                                                                                                                                   |
| <code>arn:aws:s3:::amazon-ssm-<i>region</i>/*</code>            | Necessario per l'aggiornamento di installazioni SSM Agent. Questi bucket contengono i pacchetti di installazione dell'SSM Agent e i file manifest a cui fanno riferimento il documento <code>AWS-UpdateSSMAgent</code> e il plugin. Se queste autorizzazioni non vengono fornite, l'SSM Agent effettua una chiamata HTTP per scaricare l'aggiornamento. |
| <code>arn:aws:s3:::aws-ssm-<i>region</i>/*</code>               | Fornisce l'accesso al bucket S3 contenente i moduli necessari da utilizzare con documenti di Systems Manager (documenti SSM Command), tra cui operazioni con applicazione delle patch e meno. Ad esempio: <code>arn:aws:s3:::aws-ssm-us-east-2/*</code> .                                                                                               |

| ARN di bucket S3 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <p>Di seguito sono riportati alcuni documenti SSM comunemente utilizzati che si servono di moduli provenienti da questi bucket.</p> <ul style="list-style-type: none"><li>• AWS-RunPatchBaseline</li><li>• AWS-RunPatchBaselineAssociation</li><li>• AWS-RunPatchBaselineWithHooks</li><li>• AWS-ApplyPatchBaseline (un documento SSM legacy)</li><li>• AWS-ConfigureWindowsUpdate</li><li>• AWS-FindWindowsUpdates</li><li>• AWS-UpdateSSMAgent</li></ul> |

| ARN di bucket S3                                                                                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>arn:aws:s3:::patch-baseline-snapshot- <i>region</i>/*</p> <p>oppure</p> <p>arn:aws:s3:::patch-baseline-snapshot- <i>region-unique-suffix</i> /*</p> | <p>Fornisce l'accesso al bucket S3 contenent e snapshot della baseline delle patch. È necessario se si utilizza uno dei seguenti documenti SSM Command:</p> <ul style="list-style-type: none"><li>• AWS-RunPatchBaseline</li><li>• AWS-RunPatchBaselineAssocia tion</li><li>• AWS-RunPatchBaselineWithHooks</li><li>• AWS-ApplyPatchBaseline (un documento SSM legacy)</li></ul> <p>I bucket più supportati Regioni AWS utilizzano il seguente formato:</p> <p>arn:aws:s3:::patch-baseline-snapshot- <i>region</i></p> <p>Per alcune regioni, nel nome del bucket è incluso un suffisso univoco aggiuntivo. Ad esempio, il nome del bucket per la regione Medio Oriente (Bahrein) (me-south-1) è il seguente:</p> <ul style="list-style-type: none"><li>• patch-baseline-snapshot-me-south-1-uduv17q8</li></ul> <p>Per un elenco completo dei nomi dei bucket di snapshot della baseline delle patch, consulta <a href="#">Secchi contenenti AWS istantanee della baseline delle patch gestite</a>.</p> |

| ARN di bucket S3 | Description                                                                                                                                                                                                                                                                                      |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <div><div> Note</div><div>Se si usa un firewall on-premises e si intende utilizzare Patch Manager, il firewall deve consentire anche l'accesso all'endpoint della baseline delle patch appropriato.</div></div> |

| ARN di bucket S3                                                                                                                                                                                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Per nodi gestiti dal Linux e Windows Server:<br/> arn:aws:s3:::aws-patch-manager- <i>region-unique-suffix</i> /*</p> <p>Per le istanze Amazon EC2 per macOS:<br/> arn:aws:s3:::aws-patchmanager-macos- <i>region-unique-suffix</i> /*</p> | <p>Fornisce l'accesso al bucket S3 contenente i documenti di SSM Command utilizzati per le operazioni di applicazione delle patch in Patch Manager. Ogni nome del bucket include un suffisso univoco, ad esempio 552881074 per i bucket nella Regione Stati Uniti orientali (Ohio) (us-east-2):</p> <ul style="list-style-type: none"> <li>arn:aws:s3:::aws-patch-manager-us-east-2-552881074/*</li> <li>arn:aws:s3:::aws-patchmanager-macos-us-east-2-552881074/*</li> </ul> <p>Documenti SSM</p> <p>Di seguito sono riportati alcuni documenti SSM comunemente utilizzati che si servono di moduli provenienti da questi bucket.</p> <ul style="list-style-type: none"> <li>AWS-RunPatchBaseline</li> <li>AWS-RunPatchBaselineAssociation</li> <li>AWS-RunPatchBaselineWithHooks</li> <li>AWS-InstanceRebootWithHooks</li> <li>AWS-PatchAsgInstance</li> <li>AWS-PatchInstanceWithRollback</li> </ul> <p>Per un elenco completo dei bucket S3 AWS gestiti per le operazioni di patching, consulta i seguenti argomenti:</p> <ul style="list-style-type: none"> <li><a href="#">Bucket contenenti documenti SSM Command per le operazioni di patching (Linux e Windows Server)</a></li> </ul> |



| ARN di bucket S3                                | Description                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                 | <ul style="list-style-type: none"> <li><a href="#">Bucket contenenti documenti SSM Command per le operazioni di patching (macOS)</a></li> </ul>                                                                                                                                                                                                                                                                   |
| arn:aws:s3::: <i>region</i> -birdwatcher-prod/* | <p>Necessario per le operazioni. Distributor</p> <p>Questo bucket contiene i manifesti dei pacchetti utilizzati dal <code>aws:configurePackage</code> plug-in durante l'installazione o l'aggiornamento dei pacchetti Distributor utilizzando documenti come <code>AWS-ConfigureAWSPackage</code>. Se utilizzi un endpoint VPC, la tua policy sugli endpoint VPC S3 deve includere l'accesso a questo bucket.</p> |

## Esempio

L'esempio seguente mostra come fornire l'accesso al bucket S3 richiesto per le operazioni di Systems Manager nella Regione Stati Uniti orientali (Ohio) (us-east-2). Nella maggior parte dei casi, è necessario fornire queste autorizzazioni esplicitamente in un profilo dell'istanza o in un ruolo di servizio solo quando si utilizza un endpoint VPC.

### Important

Consigliamo di evitare l'uso di caratteri jolly (\*) al posto delle Regioni specifiche in questa policy. Ad esempio, è preferibile usare `arn:aws:s3:::aws-ssm-us-east-2/*` anziché `arn:aws:s3:::aws-ssm-*/*`. L'utilizzo di caratteri jolly potrebbe fornire l'accesso ai bucket S3 a cui non si intende concedere l'accesso. Se si desidera utilizzare il profilo dell'istanza per più di una regione, si consiglia di ripetere il primo elemento Statement per ogni regione.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
```

```
{
 "Effect": "Allow",
 "Action": "s3:GetObject",
 "Resource": [
 "arn:aws:s3:::aws-windows-downloads-us-east-2/*",
 "arn:aws:s3:::amazon-ssm-us-east-2/*",
 "arn:aws:s3:::aws-ssm-us-east-2/*",
 "arn:aws:s3:::us-east-2-birdwatcher-prod/*",
 "arn:aws:s3:::patch-baseline-snapshot-us-east-2/*",
 "arn:aws:s3:::aws-patch-manager-us-east-2-552881074/*",
 "arn:aws:s3:::aws-patchmanager-macos-us-east-2-552881074/*"
]
}
```

## Convalida di macchine attivate da sistemi tramite un'impronta digitale hardware

Quando si utilizzano macchine non EC2 in un ambiente [ibrido e multicloud](#), SSM Agent raccoglie una serie di attributi di sistema (denominati hash hardware) e utilizza questi attributi per calcolare un'impronta digitale. L'impronta digitale è una stringa opaca che l'agente passa a determinate API di Systems Manager. Questa impronta digitale univoca associa il chiamante a un particolare nodo gestito attivato da sistemi ibridi. L'agente memorizza l'impronta digitale e l'hash hardware sul disco locale in una posizione chiamata Vault.

L'agente calcola l'hash hardware e l'impronta digitale quando la macchina viene registrata per essere utilizzata con Systems Manager. Quindi, l'impronta digitale viene restituita al servizio Systems Manager quando l'agente invia un comando `RegisterManagedInstance`.

Più tardi, quando si invia un comando `RequestManagedInstanceRoleToken`, l'agente controlla l'impronta digitale e l'hash hardware nel vault per verificare che gli attributi correnti della macchina corrispondano all'hash hardware archiviato. Se gli attributi correnti della macchina corrispondono effettivamente all'hash hardware archiviato nel vault, l'agente passa l'impronta digitale dal vault a `RegisterManagedInstance`, dando come risultato una chiamata riuscita.

Se gli attributi correnti della macchina non corrispondono all'hash hardware memorizzato, SSM Agent calcola una nuova impronta digitale, memorizza il nuovo hash hardware e l'impronta digitale nel vault e passa la nuova impronta digitale a `RequestManagedInstanceRoleToken`. Questo causa un errore in `RequestManagedInstanceRoleToken` e l'agente non sarà in grado di ottenere un token di ruolo per connettersi al servizio Systems Manager.

Questo errore varia in base alla progettazione e viene utilizzato come fase di verifica per impedire che più nodi gestiti comunichino con il servizio Systems Manager come fossero lo stesso nodo gestito.

Quando si confrontano gli attributi correnti della macchina con l'hash hardware memorizzato nel vault, l'agente utilizza la logica seguente per stabilire se gli hash vecchi e nuovi corrispondono:

- Se il SID (system/machine ID) è diverso, non corrisponde.
- Altrimenti, se l'indirizzo IP è lo stesso, c'è corrispondenza.
- In caso contrario, la percentuale di attributi della macchina corrispondenti viene calcolata e confrontata con la soglia di similarità configurata dall'utente per determinare se esiste una corrispondenza.

La soglia di somiglianza viene memorizzata nel vault, insieme all'hash hardware.

La soglia di somiglianza può essere impostata dopo che un'istanza è stata registrata utilizzando un comando simile al seguente.

Su macchine Linux:

```
sudo amazon-ssm-agent -fingerprint -similarityThreshold 1
```

Su Windows Server macchine che utilizzano PowerShell:

```
cd "C:\Program Files\Amazon\SSM\" `
.\amazon-ssm-agent.exe -fingerprint -similarityThreshold 1
```

#### Important

Se uno dei componenti utilizzati per calcolare l'impronta digitale cambia, questo può causare l'ibernazione dell'agente. Per evitare questa ibernazione, impostare la soglia di somiglianza su un valore basso, ad esempio **1**. Per ulteriori informazioni sull'ibernazione, consulta [Comprensione Agente SSM ibernazione](#).

## Agente SSM on GitHub

Il codice sorgente per SSM Agent è disponibile su [GitHub](#) in modo da poter adattare l'agente per soddisfare le esigenze dell'utente. Ti consigliamo di inviare le [richieste pull](#) per le modifiche da includere. Tuttavia, Amazon Web Services attualmente non fornisce il supporto per eseguire copie modificate di questo software.

## Comprensione Agente SSM ibernazione

AWS Systems Manager L'ibernazione di Agent (SSM Agent) è una modalità operativa che si verifica quando l'agente non è in grado di mantenere una comunicazione corretta con il servizio Systems Manager. Durante l'ibernazione, l'agente riduce la frequenza di comunicazione ed entra in uno stato di stand-by.

Quando Agente SSM si verifica l'ibernazione

Questa può verificarsi nei seguenti scenari:

Nodi ibridi annullati

Quando si annulla la registrazione di un nodo [attivato in modalità ibrida](#) da Systems Manager, l'SSM Agent sul relativo nodo non può aggiornare il token di autorizzazione. Ciò fa sì che l'agente entri in modalità di ibernazione perché non può autenticarsi con il servizio.

Modifiche dell'impronta dell'hardware

SSM Agent utilizza un'impronta hardware per convalidare macchine funzionanti con sistema ibrido. Se uno dei componenti utilizzati per calcolare l'impronta cambia in modo significativo, l'agente potrebbe ricorrere all'ibernazione come misura di sicurezza. Questo meccanismo è concepito per impedire che più nodi gestiti comunichino con Systems Manager come se fossero lo stesso nodo gestito. Per ulteriori informazioni, consulta [Convalida di macchine attivate da sistemi tramite un'impronta digitale hardware](#).

Ibernazione dell'SSM Agent su istanze Amazon EC2

L'ibernazione può verificarsi anche sulle istanze Amazon EC2 in determinate condizioni, ad esempio in caso di problemi di connettività o problemi di autenticazione con il servizio Systems Manager.

Comportamento di comunicazione di ibernazione

Quando SSM Agent entra in modalità di ibernazione, il modello di comunicazione con il servizio Systems Manager cambia:

- Funzionamento normale: l'agente comunica regolarmente con Systems Manager (in genere ogni pochi minuti) per verificare la presenza di nuovi comandi e segnalare lo stato.
- Modalità di ibernazione: la frequenza di ping inizia a 5 minuti e aumenta gradualmente fino a una volta all'ora per impostazione predefinita (configurabile fino a 24 ore). Questa frequenza di comunicazione ridotta aiuta a ridurre al minimo il traffico di rete non necessario, pur consentendo all'agente di riprendersi se le condizioni cambiano.

Durante l'ibernazione, l'agente continua a riprovare l'autenticazione e i tentativi di connessione con una frequenza ridotta, ma non può elaborare nuovi comandi o riportare informazioni dettagliate sullo stato finché l'ibernazione non viene risolta.

Opzioni di configurazione per prevenire l'ibernazione nelle istanze ibride

L'opzione di configurazione principale per evitare l'ibernazione causata dalle modifiche delle impronte digitali dell'hardware consiste nella regolazione della soglia di somiglianza:

Su macchine Linux:

```
sudo amazon-ssm-agent -fingerprint -similarityThreshold 1
```

Sui computer Windows Server che utilizzano: PowerShell

```
cd "C:\Program Files\Amazon\SSM\" `
.\amazon-ssm-agent.exe -fingerprint -similarityThreshold 1
```

La soglia di somiglianza determina la precisione con cui l'agente confronta gli attributi correnti della macchina con l'hash hardware memorizzato:

- I valori più alti richiedono più attributi corrispondenti
- I valori più bassi (ad esempio **1**) sono più permissivi e possono aiutare a evitare l'ibernazione causata da piccole modifiche hardware

Registrazione e monitoraggio dell'ibernazione

Quando SSM Agent entra in modalità di ibernazione, crea voci di log che possono aiutarti a identificare e risolvere i problemi dello stato di ibernazione:

- File di log dell'agente: gli eventi di ibernazione vengono registrati nei file di log standard dell'SSM Agent. Per ulteriori informazioni sulle posizioni dei file, consulta [Risolvi i problemi utilizzando Agente SSM file di log](#).
- Registrazione della console Amazon EC2: per le istanze EC2, i messaggi di ibernazione vengono ora registrati nei log di sistema della console Amazon EC2, fornendo ulteriore visibilità sullo stato dell'agente. Per accedere ai log, seleziona l'istanza nella console EC2 e poi scegli Operazioni, Monitoraggio e risoluzione dei problemi, Ottieni il log di sistema.
- File di log specifici: all'avvio dell'ibernazione, vengono creati particolari file di log che contengono informazioni dettagliate sull'attivazione e sullo stato dell'ibernazione.

Monitora queste origini di log per rilevare tempestivamente gli eventi di ibernazione e intraprendere azioni correttive per ripristinare il normale funzionamento dell'agente.

## Recupero dall'ibernazione

Per ripristinare lo stato d'ibernazione, risolvi la causa sottostante:

- Per i nodi ibridi annullati: registra nuovamente il nodo con Systems Manager utilizzando un nuovo codice di attivazione e un ID, come descritto in [the section called “Annullamento della registrazione e nuova registrazione di un nodo gestito \(Linux\)”](#) e [the section called “Annullare la registrazione e ri-registrare un nodo gestito \(Windows Server\)”](#).
- Per problemi relativi alle impronte digitali hardware: regola la soglia di somiglianza come descritto sopra in Opzioni di configurazione per evitare l'ibernazione nelle istanze ibride, oppure registra nuovamente il nodo se le modifiche hardware sono significative.
- Per problemi di connettività: verifica la connettività di rete e assicurati che gli endpoint richiesti siano accessibili. Per ulteriori informazioni, consulta [Risoluzione dei problemi di disponibilità dei nodi gestiti tramite ssm-cli](#).

Dopo aver risolto il problema sottostante, l'agente dovrebbe uscire automaticamente dalla modalità di ibernazione e riprendere il normale funzionamento al successivo tentativo di comunicazione.

## Trova AMI con il Agente SSM preinstallato

AWS Systems Manager Agent (SSM Agent) è preinstallato su alcuni Amazon Machine Images (AMIs) forniti da terze parti affidabili AWS e affidabili.

Ad esempio, quando avvii un'istanza Amazon Elastic Compute Cloud (Amazon EC2) creata da un'AMI con uno dei seguenti sistemi operativi, probabilmente scoprirai che SSM Agent è già installato:

- AlmaLinux
- Amazon Linux 2
- Amazon Linux 2 ECS-Optimized Base AMIs
- Amazon Linux 2023 (AL2023)
- Amazon EKS-Optimized Amazon Linux AMIs
- macOS 13.x (Ventura), 14.x (Sonoma) e 15.x (Sequoia)
- SUSE Linux Enterprise Server (SLES) 15.3 e versioni successive
- Ubuntu Server 18.04, 20.04, 22.04 LTS, 24.04 LTS, 24.0 e 25.04
- Windows Server 2012 R2 AMIs pubblicate a novembre 2016 o successivamente
- Windows Server 2016, 2019 e 2022 (escluse le versioni Nano) e 2025

#### Note

La versione di SSM Agent preinstallata su un'AMI potrebbe non essere l'ultima versione disponibile. Come best practice, consigliamo di utilizzare sempre l'ultima versione disponibile di SSM Agent sui nodi gestiti. Per ulteriori informazioni sull'automazione degli aggiornamenti di SSM Agent, consulta [Automatizzazione degli aggiornamenti a Agente SSM](#).

SSM Agent potrebbe essere preinstallato su gestite che non sono presenti in questo elenco. AWS AMIs Ciò indica in genere che il sistema operativo (SO) non è completamente supportato da tutti gli strumenti di Systems Manager.

SSM Agent potrebbe anche essere preinstallato su AMIs found in Marketplace AWS o nel AMIs repository Community, ma AWS non li supporta. AMIs

## Verifica lo stato di Agente SSM

A seconda di quando è stata inizializzata, un'istanza creata da un'AMI nell'elenco precedente potrebbe non avere SSM Agent già installato. È anche possibile che l'agente sia preinstallato in un'istanza, ma non sia in esecuzione. Pertanto, ti consigliamo di verificare lo stato di SSM Agent prima di provare a utilizzare Systems Manager su un'istanza per la prima volta.

Utilizza la procedura seguente per verificare che SSM Agent sia installato e in esecuzione in un'istanza. Se l'agente non è installato, puoi installarlo manualmente sulle istanze [Linux](#), [macOS](#) e [Windows Server](#).

Per verificare l'installazione di Agente SSM su un'istanza

1. Dopo aver avviato una nuova istanza, attendi qualche minuto per inicializzarla.
2. Connettiti all'istanza utilizzando il tuo metodo preferito. Ad esempio, puoi usare SSH per connetterti alle istanze Linux o usare Remote Desktop per connetterti alle istanze Windows Server.
3. Controlla lo stato di SSM Agent eseguendo il comando per il tipo di sistema operativo dell'istanza.

| Sistema operativo                  | Comando                                                                                                                                                                                                        |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Amazon Linux 2 e Amazon Linux 2023 | <code>sudo systemctl status amazon-ssm-agent</code>                                                                                                                                                            |
| macOS                              | Non esiste alcun comando per controllare lo stato di SSM Agent su macOS. Puoi controllare lo stato individuando e valutando il file di log dell'agente <code>/var/log/amazon/ssm/amazon-ssm-agent.log</code> . |
| SUSE Linux Enterprise Server       | <code>sudo systemctl status amazon-ssm-agent</code>                                                                                                                                                            |
| Ubuntu Server (64 bit - Deb)       | <code>sudo systemctl status amazon-ssm-agent</code>                                                                                                                                                            |
| Ubuntu Server (64 bit - Snap)      | <code>sudo systemctl status snap.amazon-ssm-agent.amazon-ssm-agent.service</code>                                                                                                                              |
| Windows Server                     | <code>Get-Service AmazonSSMAgent</code>                                                                                                                                                                        |



**Tip**

Per visualizzare i comandi per il controllo dello stato di SSM Agent su tutti i tipi di sistema operativo supportati da Gestione dei segreti, consulta [Verifica Agente SSM stato e avvio dell'agente](#).

#### 4. Valuta l'output del comando per conoscere lo stato di SSM Agent.

Stato: Installato e funzionante

Nella maggior parte dei casi, l'output del comando indica che l'agente è installato e in esecuzione.

L'esempio seguente mostra che SSM Agent è installato e in esecuzione su un'istanza Amazon Linux 2.

```
amazon-ssm-agent.service - amazon-ssm-agent
Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor preset: enabled)
Active: active (running) since Wed 2021-10-20 19:09:29 UTC; 4min 6s ago
--truncated--
```

L'esempio seguente mostra che SSM Agent è installato e in esecuzione su un'istanza Windows Server.

| Status  | Name           | DisplayName      |
|---------|----------------|------------------|
| -----   | ----           | -----            |
| Running | AmazonSSMAgent | Amazon SSM Agent |

Stato: Installato ma non in esecuzione

Nella maggior parte dei casi, l'output del comando indica che l'agente è installato ma non è in esecuzione.

L'esempio seguente mostra che SSM Agent è installato ma non è in esecuzione su un'istanza Amazon Linux 2.

```
amazon-ssm-agent.service - amazon-ssm-agent
Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor
 preset: enabled)
Active: inactive (dead) since Wed 2021-10-20 22:16:41 UTC; 18s ago
--truncated--
```

L'esempio seguente mostra che SSM Agent è installato ma non in esecuzione su un'istanza Windows Server.

| Status  | Name           | DisplayName      |
|---------|----------------|------------------|
| -----   | ----           | -----            |
| Stopped | AmazonSSMAgent | Amazon SSM Agent |

Se l'agente è installato ma non è in esecuzione, puoi attivarlo manualmente utilizzando i comandi per il tipo di sistema operativo dell'istanza.

| Sistema operativo                  | Comando                                                                                                                    |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Amazon Linux 2 e Amazon Linux 2023 | <pre>sudo systemctl enable amazon-ssm-agent  sudo systemctl start amazon-ssm-agent</pre>                                   |
| macOS                              | <pre>sudo launchctl load -w /Library/LaunchDaemons/com.amazon.aws.ssm.plist  sudo launchctl start com.amazon.aws.ssm</pre> |

| Sistema operativo             | Comando                                                                                               |
|-------------------------------|-------------------------------------------------------------------------------------------------------|
| SUSE Linux Enterprise Server  | <pre>sudo systemctl enable amazon-ssm-agent</pre><br><pre>sudo systemctl start amazon-ssm-agent</pre> |
| Ubuntu Server (64 bit - Deb)  | <pre>sudo systemctl enable amazon-ssm-agent</pre><br><pre>sudo systemctl start amazon-ssm-agent</pre> |
| Ubuntu Server (64 bit - Snap) | <pre>sudo snap start amazon-ssm-agent</pre>                                                           |
| Windows Server                | Esegui il seguente comando in PowerShell.<br><br><pre>Start-Service AmazonSSMAgent</pre>              |

Stato: Non installato

Nella maggior parte dei casi, l'output del comando indica che l'agente non è installato.

L'esempio seguente mostra che SSM Agent non è installato su un'istanza Amazon Linux 2.

```
Unit amazon-ssm-agent.service could not be found.
```

L'esempio seguente mostra che SSM Agent non è installato su un'istanza Windows Server.

```
Get-Service : Cannot find any service with service name 'AmazonSSMAgent'.
--truncated--
```

Se l'agente non è installato, puoi installarlo manualmente utilizzando la procedura per il tipo di sistema operativo:

- [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#)
- [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per macOS](#)

- [Installazione e disinstallazione manuali Agente SSM su istanze EC2 per Windows Server](#)

## Utilizzo di SSM Agent sulle istanze EC2 per Linux

AWS Systems Manager Agent (SSM Agent) elabora le richieste di Systems Manager e configura la macchina come specificato nella richiesta. Utilizza le procedure descritte nei seguenti argomenti per installare, configurare o disinstallare SSM Agent su sistemi operativi Linux.

### Argomenti

- [Verifica della firma di Agente SSM](#)
- [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#)
- [Configurazione Agente SSM usare un proxy su nodi Linux](#)

## Verifica della firma di Agente SSM

I pacchetti di installazione AWS Systems Manager Agent (SSM Agent) deb e rpm per le istanze Linux sono firmati crittograficamente. È possibile utilizzare una chiave pubblica per verificare che il pacchetto dell'agente sia originale e non modificato. Se i file sono danneggiati o sono stati alterati, la verifica non va a buon fine. È possibile verificare la firma del pacchetto di installazione utilizzando RPM o GPG. Le seguenti informazioni sono relative a SSM Agent 3.1.1141.0 o versioni successive.

Per trovare il file della firma corretto per l'architettura e il sistema operativo dell'istanza, consultare la tabella seguente.

**region** rappresenta l'identificatore di una regione Regione AWS supportata da AWS Systems Manager, ad esempio per la regione Stati Uniti orientali (us-east-2Ohio). Per un elenco dei **region** valori supportati, vedere la colonna Regione negli [endpoint del servizio Systems Manager](#) in. Riferimenti generali di Amazon Web Services

| Architecture | Sistema operativo                                 | URL del file della firma                                                                                                           | Nome del file di download dell'agente |
|--------------|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| x86_64       | AlmaLinux, Amazon Linux 2, Amazon Linux 2023RHEL, | <a href="https://s3.region.amazonaws.com/amazon-ssm-region/">https://s3. <b>region</b>.amazonaws.com/amazon-ssm-<b>region</b>/</a> | amazon-ssm-agent.rpm                  |

| Architecture | Sistema operativo            | URL del file della firma                                                                                                                                                                                                     | Nome del file di download dell'agente |
|--------------|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
|              | Oracle Linux, Rocky Linux    | latest/linux_amd64/amazon-ssm-agent.rpm.sig<br><br>https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm.sig                                                                       |                                       |
| x86_64       | Debian Server, Ubuntu Server | https://s3. <i>region</i> .amazonaws.com/amazon-ssm- <i>region</i> /latest/debian_amd64/amazon-ssm-agent.deb.sig<br><br>https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/debian_amd64/amazon-ssm-agent.deb.sig | amazon-ssm-agent.deb                  |

| Architecture | Sistema operativo                             | URL del file della firma                                                                                                                                                                                                                                                                                                                                                                                                                           | Nome del file di download dell'agente |
|--------------|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| ARM64        | Amazon Linux 2,<br>Amazon Linux 2023,<br>RHEL | <a href="https://s3.amazonaws.com/amazon-ssm-&lt;i&gt;region&lt;/i&gt;/latest/linux_arm64/amazon-ssm-agent.rpm.sig">https://s3.amazonaws.com/amazon-ssm-<i>region</i>/latest/linux_arm64/amazon-ssm-agent.rpm.sig</a><br><br><a href="https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_arm64/amazon-ssm-agent.rpm.sig">https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_arm64/amazon-ssm-agent.rpm.sig</a> | amazon-ssm-agent.rpm                  |

## Verifica del Agente SSM pacchetto su un server Linux (v3.3.4851.0 e versioni successive)

### Prima di iniziare

Le procedure per GPG e RPM in questa sezione si applicano alla versione 3.3.4851.0 e successive. SSM Agent Prima di verificare la firma di SSM Agent, assicuratevi di aver scaricato il pacchetto agente più recente per il vostro sistema operativo. Ad esempio, [https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux\\_arm64/amazon-ssm-agent.rpm](https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_arm64/amazon-ssm-agent.rpm). Per ulteriori informazioni sul caricamento di pacchetti dell'SSM Agent, consulta [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#).

Se utilizzate la versione dell'agente da 3.3.1802.0 a 3.3.4793.0, seguite le istruzioni riportate in [Verifica del Agente SSM pacchetto su un server Linux \(v3.3.1802.0 e versioni successive\)](#) Per

la versione dell'agente 3.3.1611.0 o precedente, segui le istruzioni in. [Verifica del Agente SSM pacchetto su un server Linux \(v3.3.1611.0 e versioni precedenti\)](#)

## GPG

Per verificare il Agente SSM pacchetto su un server Linux (v3.3.4851.0 e versioni successive)

1. Copia la seguente chiave pubblica e salvala in un file denominato `amazon-ssm-agent.gpg`.

### Important

La seguente chiave pubblica scade il 25 novembre 2027. Pubblicheremo una nuova chiave pubblica in questo argomento prima della scadenza di quella precedente. Per ricevere una notifica quando la nuova chiave sarà disponibile, iscriviti al feed RSS relativo a questo argomento.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

```
Version: GnuPG v2.0.22 (GNU/Linux)
```

```
mQINBGohhG8BEACxN0k7TM1ywHjW0qrSyH9npRDUjpWpAyCD8L1Yu7nLnxEbtU0k
HgQIo1scTWuwogaBZpAzg22A25A1o0rhX8BGTokh71Xm3LbQT8dDQUdT7WRT14R5
p7786TN79p4DqD3/JyzjiD/keTYyhp1BWdyk5BEcqlyVj9Pf/106Cr0JgGD1oGYK
71RqMtmX1f86/mKveWvjJTPAF26dkDJZecnrheyEA99X10Nm8zA1K6h09JTHHBmW
MgDPXDSsVeEyXi1PUJFhZJ2HXVG2tS9ioVM309tMX6B3W5woT7w8SA6uV2Pf0jMm
oYmMuCmQM8/7/v0LQ5Jm+6Wui5dZyWArqt0QXcSledRf7xhmug3Qa5maqY2Ttcn
XqTaH3WaBLtJZYqDJcsUH99AXqdQkozsCHHL2NmXRiShyLCX4VBKzH8j5kDNGeSL
uiICbj1Tufh7LDuIwd0QnX9gvB6j/SF3YVqJl4DAjCs40DYpwm+36RZjQkbwELzX
zXnDoNgjR5tXCiNdxJLuzemQy7FcDc90fEbpDX03rN7iceavBmZbZ5Tlu53fgpzd
kf1D80wfjNJa9AXh2zweC1G0ut2QU+cZco0q5/QPtQELNqvgaUsQtKCECTerz8S
ugriZD4Tnd4FJUgoqX+/iwCwesyWjGkotxi7aJluLtz+znNT9SgeMCoJmQARAQAB
tCdTU00gQWdlbnQgPHNzbS1hZ2VudC1zaWduZXJAYW1hem9uLmNvbT6JAJ8EEwEC
ACKFamohhG8CGy8FCQLGmIAHCwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRAn
hNvziNGdRnXVD/9bP0IX6aU+qur66fTws8RLDs//6Vx93e81H6p4W+RXL+wW7Ajc
/REB7PPgc5ohW80/LwxHP2g8cZiSK7fp9cRbX0DqiVY14mAWQNfxGcWpBxcEsyO
UGF6oRjiibL1BcJLFJgVZ/H4pT0xNEDJNlJpRn7ZVxm0vrVVUUh4a4WFXUkspRXm
q37eIMm76p969L5SNjY+F8Ld6hjmRiRopg4f/+lf/+e6R+fofS0VE3Ip/YpPH1DR
plwQJrMk1XFjm+JTsdtqMTIKv38j7HANmUgDGLsuQNN8048n6ve8koVZLSrv9FAi
eLSNsSiurLEpkLM0QP0FviagK7zB/d/zScpGquBU9dPF0oTq/sNFhnZr+PA7MAek
r4W0P8kasS3LWgn/rqqIOw/PDm2mmUaIwm4Xen0e81JFKUGp6ssU0j4PIQKwGaL/
S2xTex25ZaNaQKXv2JUmriGycpCjIaniEHZ60bBN1kSg00m0a5Yg3X9Qw+ezt51o
Pi6H6NdE0IwNzNcbJI2UvphwR9L92Br/J9E1YbHRdgmz26SZErNTh/+zKPXk4iD
```

```

YibpQ804cPfA0mJB0DwzqL5BBfVJ0/rLtQ2ymuHaqKbKEc0KuJ6vWmOH9q1MB1v5
YiZeUw5Ls2uuaxhKTUYrCE4LuU1AtNW63+/TP+ciBg1bq5H5aBn5tSCYV4kCHAQQ
AQIABgUCaiGEcQAKCRB90Jej2tf1/PUvD/43D4uSk84EFEbvXhSxazhieLpzoMq1
zYcx0WjRF9+8bYq9NQ1C7gYDI3xS7y0NYfNWHdPU2FF070bu9XhZp2gQ+NqyyVTj
GoivF2uIhM6xsE1r9ZXXMLap4xbnPTfbLgQIyXkb1Dw0VVK40yFF0HMuS0mXJN6m
/S+FP3TDcgoDxgyRsRAB0vGKPIJABtImR9Fg0tPEZpA4kbawieq5uBjv5Fol/ctl
jRZ51ksszlXhZd0t9/aBpe7XBHpfIlsItPVskHV6Kpc2741j+f0BVE70/1n/++FM
sxpQNuN7mdXXzMLASifVapPQGLBeHuxriHsgh+V6Arpswojy1uPgp6J8B/gQQ/B2
mebiGJrM/LwNPWj79QPPgzUFz6LqYnyhtJCWURWJjzHRSXsPWKgd98AXjkeSgUz9
8NV5p9Td1uZ0iYQ7Q1o58Ih6jfPFULnftiQuRnp/5ErhojV/zxKzjZNmB6YZ508M
nYrz5/++8LBc6uAf/Oq907CdfEkAYid8j2dFttksJbh1YVTnuo9vd4Bd0ovnB88V
dvyFJcFz1Wsys2vrH6CGmngYKStQHEA588/d1w1E7Z4A8XJJiBkBMZS0rWDMUjG
vihLPXN0srpdCZTI9jlznp60rRVP3P9fp3fXj1nJeIdMr30akz19Lze6T9jsDDWa
M98H0S1+MxUsAg==
=TP0v
-----END PGP PUBLIC KEY BLOCK-----

```

2. Importare la chiave pubblica nel keyring e osservare il valore della chiave restituito.

```
gpg --import amazon-ssm-agent.gpg
```

3. Verifica dell'impronta digitale. Assicurati di sostituirlo *key-value* con il valore del passaggio precedente. Usa GPG per verificare l'impronta digitale anche se usi RPM per verificare il pacchetto di installazione.

```
gpg --fingerprint key-value
```

Questo comando restituisce un output simile al seguente:

```

pub rsa4096 2026-06-04 [SCEA] [expires: 2027-11-25]
 Key fingerprint = 1C5B 395C BE5E 74E2 F1CA 2159 2784 DBF3 88D1 9D46
uid
 SSM Agent <ssm-agent-signer@amazon.com>

```

L'impronta digitale deve corrispondere a quanto riportato di seguito.

```
1C5B 395C BE5E 74E2 F1CA 2159 2784 DBF3 88D1 9D46
```

Se la stringa dell'impronta non corrisponde, non installare l'agente. Contatto. Supporto AWS

4. Scaricare il file della firma in base all'architettura e al sistema operativo dell'istanza, se non è stato ancora fatto.



5. Verificare la firma del pacchetto di installazione. Assicurati di sostituire *signature-filename* e *agent-download-filename* con i valori specificati durante il download del file della firma e dell'agente, come indicato nella tabella precedente di questo argomento.

```
gpg --verify signature-filename agent-download-filename
```

Ad esempio, per l'architettura x86\_64 su Amazon Linux 2:

```
gpg --verify amazon-ssm-agent.rpm.sig amazon-ssm-agent.rpm
```

Questo comando restituisce un output simile al seguente:

```
gpg: Signature made Mon 14 Jul 2026 12:00:00 AM UTC using RSA key ID 88D19D46
gpg: Good signature from "SSM Agent <ssm-agent-signer@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: 1C5B 395C BE5E 74E2 F1CA 2159 2784 DBF3 88D1 9D46
```

Se l'output include la frase `BAD signature`, controllare di avere eseguito la procedura correttamente. Se il problema persiste, contatta l'agente Supporto e non installarlo.

L'avviso sulla fiducia non significa che la firma non sia valida. Significa che non hai verificato la chiave pubblica. Puoi fidarti di una chiave solo se tu o qualcuno di cui ti fidi l'avete firmata.

Se l'output include la frase `Can't check signature: No public key`, verifica di aver scaricato la SSM Agent versione 3.3.4851.0 o successiva.

## RPM

Per verificare il Agente SSM pacchetto su un server Linux (v3.3.4851.0 e versioni successive)

1. Copia la seguente chiave pubblica e salvala in un file denominato `amazon-ssm-agent.gpg`.



### Important

La seguente chiave pubblica scade il 25 novembre 2027. Pubblicheremo una nuova chiave pubblica in questo argomento prima della scadenza di quella precedente. Per

ricevere una notifica quando la nuova chiave sarà disponibile, iscriviti al feed RSS relativo a questo argomento.

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v2.0.22 (GNU/Linux)

mQINBGohhG8BEACxN0k7TM1ywHjW0qrSyH9npRDUjpWAcD8L1Yu7nLnxEbT0k  
HgQIo1scTWuwogaBZpAzg22A25Alo0rhX8BGTokh71Xm3LbQT8dDQUdT7WRT14R5  
p7786TN79p4DqD3/JyzjiD/keTYyhp1BWdyk5BEcqlyVj9Pf/106Cr0JgGD1oGYK  
71RqMtmX1f86/mKveWvjJTPAF26dkDJZecnrheyEA99X10Nm8zA1K6h09JThHBmW  
MgDPXDSsVeEyXi1PUJFhZJ2HXVG2tS9ioVM309tMX6B3W5woT7w8SA6uV2Pf0jMm  
oYmMuCmQMU8/7/v0LQsJm+6Wui5dZyWArqt0qXcSledRf7xhmug3Qa5maqY2Ttcn  
XqTaH3WaBLtJZYqDJcsUH99AXqdQkozsCHHL2NmxRiShyLCX4VBKzH8j5kDNgeSL  
uiICbj1Tufh7LDuIwd0QnX9gvB6j/SF3YVqJl4DAjCs40DYpwm+36RZjQkbwELzX  
zXnDoNgjR5tXCiNdxJLuzemQy7FcDc90fEbpDX03rN7iceavBmZbZ5Tlu53fgpzd  
kf1D80wfjnYa9AXh2zweC1G0ut2QU+cZco0q5/QPtQELNqvgpAUstktCECTerz8S  
ugriZD4Tnd4FJUgoqX+/iWCWesyWjGkotxi7aJluLtz+znNT9SgeMCoJmQARAQAB  
tCdTU00gQWdlbnQgPHNzbS1hZ2VudC1zaWduZXJAYW1hem9uLmNvbT6JAj8EEwEC  
ACKFamohhG8CGy8FCQLGmIAHCwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRAn  
hNvziNgdRnXVD/9bP0IX6aU+qur66fTws8RLDs//6Vx93e81H6p4W+RXL+wW7Ajc  
/REB7PPgc5ohW80/LwxHP2g8cZiSK7fp9cRbX0DqiVY14mAWQNfxGcWpBxcEsyo  
UGF6oRjiibL1BcJLFJgVZ/H4pT0xNEDJNlJpRn7ZVXm0vrVVVUh4a4WFXUksPRXm  
q37eIMm76p969L5SNjY+F8Ld6hjmRiRopg4f/+lf/+e6R+fofS0VE3Ip/YpPH1DR  
plwQJrMk1XFjm+JTsdtqMTIKv38j7HANmUgDGLsuQNN8048n6ve8koVZLSrv9FAi  
eLSNsSIurLEpkLM0QP0FviagK7zB/d/zScpGquBU9dPF0oTq/sNFhnZr+PA7MAek  
r4WOP8kasS3LWgn/rqqIOw/PDm2mmUaIwm4Xen0e81JFKUGp6ssU0j4PIQKwGaL/  
S2xTex25ZaNaQKXv2JUmriGycpCjIaniEHZ60bBN1kSg00m0a5Yg3X9Qw+ezt51o  
Pi6H6NdE0IwNzNcbJI2UvphwR9L92Br/J9E1YbHRdgmz26SZERNTh/+zKPxk4iD  
YibpQ804cPfA0mJB0DwzqL5BBfVJ0/rLtQ2ymuHaqKbKEc0KuJ6vWMoH9q1MB1v5  
YiZeUw5Ls2uuaxhKTUYrCE4LuU1AtNW63+/TP+ciBg1bq5H5aBn5tSCYV4kCHAQQ  
AQIABgUCAiGECQAKCRB90Jej2tf1/PUvD/43D4uSk84EFEbvXhSxazhieLpzoMq1  
zYcx0WjRF9+8bYq9NQ1C7gYDI3xS7y0NYfNWHdPU2FF070bu9XhZp2gQ+NqyyVTj  
GoivF2uIhM6xsE1r9ZXXMLap4xbnPTfbLgQIyXkb1Dw0VVK40yFF0HMuS0mXJN6m  
/S+FP3TDcgoDxgyRsRAB0vGKPIJABt1mR9Fg0tPEZpA4kbawIEq5uBjv5Fol/ct1  
jRZ51ksszlXhZd0t9/aBpe7XBHpfIlsItPVskHV6Kpc2741j+f0BVE70/1n/++FM  
sxpQNuN7mdXXzMLASifVapPQGLBeHuxriHsgh+V6Arpswojy1uPgp6J8B/gQQ/B2  
mebiGJRm/LwNPWj79QPPgzUFz6LqYnyhtJCWURWJzjHRSXsPWKgd98AXjkeSgUz9  
8NV5p9Td1uZ0iYQ7Q1o58Ih6jFPFULnftiQuRnp/5ErhojV/zxKzjZnmB6YZ508M  
nYrz5/++8LBc6uAf/0q907CdfEkAYid8j2dFttksJbh1YVTnuo9vd4Bd0ovnB88V  
dvyFJcFz1Wsys2vrH6CGmngYKStQHEA588/d1w1E7Z4A8XJJiBKKBMZS0rWDMUjG  
vihLPXN0srpdCZTI9jlznp60rRVP3P9fp3fXj1nJeIdMr30akz19Lze6T9jsDDWa

```
M98H0S1+MxUsAg==
=Tp0v
-----END PGP PUBLIC KEY BLOCK-----
```

2. Importare la chiave pubblica nel keyring e osservare il valore della chiave restituito.

```
rpm --import amazon-ssm-agent.gpg
```

3. Verifica dell'impronta digitale. Usa GPG per verificare l'impronta digitale anche se usi RPM per verificare il pacchetto di installazione.

```
rpm -qa gpg-pubkey --qf '%{Description}' | gpg --with-fingerprint | grep -A 1
"ssm-agent-signer@amazon.com"
```

Questo comando restituisce un output simile al seguente:

```
pub 4096R/88D19D46 2026-06-04 SSM Agent <ssm-agent-signer@amazon.com>
Key fingerprint = 1C5B 395C BE5E 74E2 F1CA 2159 2784 DBF3 88D1 9D46
```

L'impronta digitale deve corrispondere a quanto riportato di seguito.

1C5B 395C BE5E 74E2 F1CA 2159 2784 DBF3 88D1 9D46

Se la stringa dell'impronta non corrisponde, non installare l'agente. Contatto. Supporto AWS

4. Verificare la firma del pacchetto di installazione. Assicurati di sostituirli *agent-download-filename* con i valori specificati durante il download dell'agente, come indicato nella tabella precedente di questo argomento.

```
rpm --checksig agent-download-filename
```

Ad esempio, per l'architettura x86\_64 su Amazon Linux 2:

```
rpm --checksig amazon-ssm-agent.rpm
```

Questo comando restituisce un output simile al seguente.

```
amazon-ssm-agent.rpm: digests signatures OK
```

Se l'output contiene SIGNATURES NOT OK o NOT OK (MISSING KEYS: (MD5) *key-id*), controlla se la procedura è stata eseguita correttamente e verifica di aver scaricato la SSM Agent versione 3.3.4851.0 o successiva. Se continui a ricevere questa risposta, contatta l'agente Supporto e non installarlo.

## Verifica del Agente SSM pacchetto su un server Linux (v3.3.1802.0 e versioni successive)

### Prima di iniziare

Le procedure per GPG e RPM in questa sezione si applicano alle versioni da 3.3.1802.0 a 3.3.4793.0. SSM Agent Si consiglia sempre di utilizzare la versione più recente dell'agente. Per informazioni, consulta [Verifica del Agente SSM pacchetto su un server Linux \(v3.3.4851.0 e versioni successive\)](#). Tuttavia, se avete un motivo specifico per continuare a utilizzare la versione dell'agente dalla versione 3.3.1802.0 alla 3.3.4793.0, seguite le istruzioni in una delle seguenti procedure.

### GPG

Per verificare il Agente SSM pacchetto su un server Linux (v3.3.1802.0 e versioni successive)

1. Copia la seguente chiave pubblica e salvala in un file denominato `amazon-ssm-agent.gpg`.

#### Important

La seguente chiave pubblica scade il 15-07-2026 (15 luglio 2026). Systems Manager pubblicherà una nuova chiave pubblica in questo argomento prima della scadenza di quella precedente. Ti invitiamo a sottoscrivere il feed RSS per questo argomento per ricevere una notifica quando sarà disponibile la nuova chiave.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

```
Version: GnuPG v2.0.22 (GNU/Linux)
```

```
mQINBGeRNq4BEACr1f5h6Pz+k+M+QCJJ2LfK7d2Tn9J8iJ9qBK2Vwvuxco1rpS0+
KEI3nTeySPuheximps8WOCADX4V1bsKxMZQLjQM4mA26m1Tiw9nAI4kod4bKjiuM
BMUTCD1wfnjH3zQi4kDUdbpfAEMiPgNLVLH85Wf+lhK+Zm+V38DYzLyVj03kX4wK
iG6RMoxz0BZa5gNsVq+j+oCUITGz/URxH713Rgo8WeoEegI0+7iCBLKg+PM0b7GV
2nzkwWJz796HdkqSg8BwXsYaLTrHxa2P1IpwPCisAky07gZaMd6Uj69dtMF0+V8a
```

```

Qee6b57qGuFKZw7h1Vvc85PbF1Gy/wNIpary57kUHBfUg1vYep/roJuEbJCq97r5
I2liLl4NAyrWb9r/TAVx1XvqM4iZUhxM8GAp0FywMdB9ZECClKa5HxuVmlm0Wg1
TXoYT0ZKeDg6ZoCvyhNxWneCNip74fohXymeFF5L/budhBwy5wuWsnIOgTGLo/4C
VgZHWCCn+d0Q3bx/s12QNqPg5/xzsxEtymXLdVdwLIsLdEQUnIvy8KTS5jol3Dwi
nnEEyhly6wdaw+qD0hkS0T/VnErrSMkYF8VJfa5GjhCBWkw9JVSkaP2CI/VH0gHM
MKR0nu1q0hRQBR7RmLYt98xu38BHJWmMf8Ga/HJuIxzD1VmkZ0PvDDESUwARAQAB
tCdTU00gQWdlbnQgPHNzbS1hZ2VudC1zaWduZXJAYW1hem9uLmNvbT6JAj8EEwEC
ACKFameRNq4CGy8FCQLGmIAHCwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRBR
q0BQ0AUuXTdND/9qldQ1E3dYjBVX0nbhiUQL594bkS5VoEX7D4fZ5UMVZa5pGiz+
husnoRUS9rH1cSeq7aHJu9hSCMuMdvRpuoo0CwLB+7HtzJvA02M01hcEkUYa6Qdj
njTzP0ZjnoenJmqF9SYmVqAI/VPa9mNQ10J+HQ3qh5i6w+Fow1VqEdXjZGrWijub
TqyN33i1Y26t70s/x8I9fUeNx37y/7Kama8LTdtv9GhWiMVBg2IuVf27HCMYofrQ
m2uCGe61IhtsnhsYaYupmljl+6qgdiuCiS9BASoIGtqTnu8lnKcGyGz6YnRszN+U
1bNE4w+UFpXWJF8ogpYcghJ06aW/LhjZnQSx3VliLdW8e0Jzou4lyWmiuL3ZY8eW
KA1D+7eYKS6N6fEJCEN02VX21cKtDfa0X+lqGIVyexKayMfpi+0frNzt/92YCPf5
3jkeS77vMMVqKIUiIp10CGv3XsFpIr6Bt2c2throYPDoQL3zvq6vvG40BKErQ4tT
Y+5vTc8MeNn3LdzTl9pusxTcKifRjQ7f5FIsl2CpAX8uQ+Qz+XwsYQ05PvyUDt0z
nU/MRZaP6HnqY42bzI9ZlKgXi9IE3MXIwoET9YyzFjkIDvat7S1B4uJCpeIqp/KM
OIrTmb7paGLYmBU6YqxNBkDWItNG7NeZzyhh/R/Qqb4vJaf4S+ZqD1RZXokCHAQQ
AQIABgUCZ5E2rwAKCRB90Jej2tf1/CdnD/46It+RNoE00TesZK5n2bijH5Eljw0E
4/UpMi1SV6t2zY7lIm7TcKNn18tynJNFqB6YXX0wSbBG/fbN2E9RaoUCZw23TmAv
amuHwrfSdqsHb7zzPF0bISYjqEDLQJj/gtEugUc6XY1dEpFSlWJI0vgryG04cFXI
uD2KY87ya4s1R+sEVAJ14K4R1UCiMmzJdR0NJNYJ0wBi1gkLEp6jG86ttiG2U7fY
pE2ibV+c0GEIFq8PIzqqENsn9KBuRH5ECbdBwfnsj2XfM4aR3ZtRIdWXkKkdP9Rs
yU5dTF/Y7XPI5h8/gp00+DM1XFBinQ1jE7A7eDYviEFd1ba8P7dIom3Q3gzKiWu
KTGpnykShs5NvpQmvGUF6JqDHI4RK9s3kLqsNyZkhenJfRBrJ/45fQAuP4CRedKF
7PSfX0Xp7kDnKuyK6wEUEfXXrqmuLGDmigTXbl05qgdyMwk0LjiY9znBZbHoKs76
Vp10oNgGnN19i3nuMcPf2npFICJv7kTIyn5Fh7pjWDCahl3U/PwoLjrrlEzpyStU
oXSZrK3kiaADEdS0DXJ18KYU0Pb27JbRr1ZbWnxb+039T0htssstulkR0v+IDGDQ
rQE1b12sKgcNFSzInzWrNGu4S06WN8DYzlrTZ9aSHj+37ZqpXAevi8W0FXKPV3PA
E6+08RI2451Dcg==
=aDkv
-----END PGP PUBLIC KEY BLOCK-----

```

2. Importare la chiave pubblica nel keyring e osservare il valore della chiave restituito.

```
gpg --import amazon-ssm-agent.gpg
```

3. Verifica dell'impronta digitale. Assicurati di sostituirlo *key-value* con il valore del passaggio precedente. Si consiglia di utilizzare GPG per verificare l'impronta digitale anche se si utilizza RPM per verificare il pacchetto di installazione.

```
gpg --fingerprint key-value
```

Questo comando restituisce un output simile al seguente:

```
pub 4096R/D0052E5D 2025-01-22 [expires: 2026-07-15]
 Key fingerprint = 4855 A9E6 8332 16D6 A77D 8FE4 51A8 E050 D005 2E5D
uid SSM Agent <ssm-agent-signer@amazon.com>
```

L'impronta digitale deve corrispondere a quanto riportato di seguito.

4855 A9E6 8332 16D6 A77D 8FE4 51A8 E050 D005 2E5D

Se la stringa dell'impronta non corrisponde, non installare l'agente. Contatto Supporto AWS.

4. Scaricare il file della firma in base all'architettura e al sistema operativo dell'istanza, se non è stato ancora fatto.
5. Verificare la firma del pacchetto di installazione. Assicurati di sostituire *signature-filename* e *agent-download-filename* con i valori specificati durante il download del file della firma e dell'agente, come indicato nella tabella precedente di questo argomento.

```
gpg --verify signature-filename agent-download-filename
```

Ad esempio, per l'architettura x86\_64 su Amazon Linux 2:

```
gpg --verify amazon-ssm-agent.rpm.sig amazon-ssm-agent.rpm
```

Questo comando restituisce un output simile al seguente:

```
gpg: Signature made Sat 08 Feb 2025 12:05:08 AM UTC using RSA key ID D0052E5D
gpg: Good signature from "SSM Agent <ssm-agent-signer@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: 4855 A9E6 8332 16D6 A77D 8FE4 51A8 E050 D005 2E5D
```

Se l'output include la frase `BAD signature`, controllare di avere eseguito la procedura correttamente. Se continui a ricevere questa risposta, contatta l'agente Supporto e non installarlo. Il messaggio di avviso relativo all'attendibilità non indica che la firma non sia valida, ma soltanto che la chiave pubblica non è stata verificata. Una chiave è considerata

attendibile solo se è stata firmata dall'utente o da un firmatario fidato. Se l'output include la frase `Can't check signature: No public key`, verifica di aver scaricato SSM Agent 3.1.1141.0 o una versione successiva.

## RPM

Per verificare il Agente SSM pacchetto su un server Linux (v3.3.1802.0 e versioni successive)

1. Copia la seguente chiave pubblica e salvala in un file denominato `amazon-ssm-agent.gpg`.

### Important

La seguente chiave pubblica scade il 15-07-2026 (15 luglio 2026). Systems Manager pubblicherà una nuova chiave pubblica in questo argomento prima della scadenza di quella precedente. Ti invitiamo a sottoscrivere il feed RSS per questo argomento per ricevere una notifica quando sarà disponibile la nuova chiave.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

```
Version: GnuPG v2.0.22 (GNU/Linux)
```

```
mQINBGeRNq4BEACr1f5h6Pz+k+M+QCJJ2LfK7d2Tn9J8iJ9qBK2Vwvuxco1rpS0+
KEI3nTeySPuheximps8W0CADX4V1bsKxMZQLjQM4mA26m1Tiw9nAI4kod4bKjiuM
BMUTCD1wfnjH3zQi4kDUdbpfAEMiPgNLVLH85Wf+lhK+Zm+V38DYzLyVj03kX4wK
iG6RMoxz0BZa5gNsVq+j+oCUITGz/URxH713Rgo8WeoEegI0+7iCBLKg+PM0b7GV
2nzkWJz796HdkqSg8BwXsYaLTrHxa2P1IpwPCisAky07gZaMd6Uj69dtMF0+V8a
Qee6b57qGuFKZw7h1Vvc85PbF1Gy/wNIpary57kUHBfUg1vYep/roJuEbJCq97r5
I2liL14NAyrWb9r/TAVx1XvqM4iZUhxM8GAp0FywMdB9ZECC1Ka5HxuVmlm0Wgl
TXoYT0ZKeDg6ZoCvyhNxWneCNip74fohXymeFF5L/budhBwy5wuW5ni0gTGLo/4C
VgZHWCCn+d0Q3bx/s12QNqPg5/xzSxetyXLdVdwLiSLdEQUnIvy8KTS5j0l3Dwi
nnEEyhly6wdaw+qD0hkS0T/VnErrSMkYF8VJfa5GjhCBWKw9JVSkaP2CI/VH0gHM
MKR0nu1q0hRQBR7RmLYt98xu38BHJWmMf8Ga/HJuIxzD1VmkZ0PvDDESUwARAQAB
tCdTU00gQWdlbnQgPHNzbS1hZ2VudC1zaWduZXJAYW1hem9uLmNvbT6JAj8EEwEC
ACKFameRNq4CGy8FCQLGmIAHCwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRBR
q0BQ0AUuXTdND/9qldQ1E3dYjBVX0nbhiUQL594bkS5VoEX7D4fZ5UMVZa5pGiz+
husnoRUS9rH1cSeq7aHJu9hSCMuMdvRpuoo0CwLB+7HtzJvA02M01hcEkUYa6Qdj
njTzP0ZjnoenJmqF9SYmVqAI/VPa9mNQ10J+HQ3qh5i6w+Fow1VqEdXjZGrWijub
TqyN33i1Y26t70s/x8I9fUeNx37y/7Kama8LTdtv9GhWiMVBg2IuVf27HCMYofrQ
m2uCGe61IhtsnhsYaYupmljl+6qgdiuCiS9BAs0IGtqTnu81nKcGyGz6YnRsZn+U
1bNE4w+UFpXWJF8ogpYcghJ06aW/LhjZnQsX3VliLdW8e0Jzou41yWmiuL3ZY8eW
```

```

KA1D+7eYKS6N6fEJCeN02VX2lCkTdFa0X+lqGIVyexKayMfpi+0frNzt/92YCpF5
3jkeS77vMMVqKIUiIp10CGv3XsFpIr6Bt2c2throYPDoQL3zvq6vvG40BKeRQ4tT
Y+5vTc8MeNn3LdzTl9pusxTcKifrJq7f5FIsl2CpAX8uQ+Qz+XWsYQ05PvyUDtOz
nU/MRZaP6HnqY42bzI9ZlKgXi9IE3MXIwoET9YyzFjkIDvat7S1B4uJCpeIqp/KM
OIrTmb7paGLYmBU6YqxNBkDWItNG7NeZzyhh/R/Qqb4vJaf4S+ZqD1RZXokCHAQQ
AQIABgUCZ5E2rwAKCRB90Jej2tf1/CdnD/46It+RNoE00TesZK5n2bijH5Eljw0E
4/UpMi1SV6t2zY7lIm7TcKNn18tynJNFqB6YXX0wSbBG/fbN2E9RaoUCZw23TmAv
amuHwrfSdqsHb7zzPF0bISYjqEDLQJj/gtEugUc6XY1dEpFS1WJI0vgryG04cFXI
uD2KY87ya4s1R+sEVAJ14K4R1UCiMmzJdR0NJNYJ0wBi1gkLEp6jG86ttiG2U7fY
pE2ibV+c0GeIFq8PIzqqENsn9KBuRH5EcbdBwfnSJ2XfM4aR3ZtRIdWXkKkdP9Rs
yU5dTF/Y7XPI5h8/gp00+DM1XFBinQ1jE7A7eDYviEFd1ba8P7dIom3Q3gzKiWu
KTGpnykShs5NvpQmvGUF6JqDHI4RK9s3kLqsNyZkhenJfRBrJ/45fQAuP4CRedkF
7PSfX0Xp7kDnKuyK6wEUEfXXrqmuLGDmigTXbl05qgdyMwk0LjiY9znBZbHoKs76
Vp10oNgGnN19i3nuMcPf2npFICJv7kTIyn5Fh7pjWDCahl3U/PwoLjrrlEzpyStU
oXSZrK3kiAADEdS0DXJl8KYU0Pb27JbRr1ZbWnxb+039T0htssstulkR0v+IDGDQ
rQE1b12sKgcnFSzInzWrNGu4S06WN8DYzlrTZ9aSHj+37ZqpXAevi8W0FXKPV3PA
E6+08RI2451Dcg==
=aDkv
-----END PGP PUBLIC KEY BLOCK-----

```

2. Importare la chiave pubblica nel keyring e osservare il valore della chiave restituito.

```
rpm --import amazon-ssm-agent.gpg
```

3. Verifica dell'impronta digitale. Si consiglia di utilizzare GPG per verificare l'impronta digitale anche se si utilizza RPM per verificare il pacchetto di installazione.

```
rpm -qa gpg-pubkey --qf '%{Description}' | gpg --with-fingerprint | grep -A 1
"ssm-agent-signer@amazon.com"
```

Questo comando restituisce un output simile al seguente:

```

pub 4096R/D0052E5D 2025-01-22 SSM Agent <ssm-agent-signer@amazon.com>
Key fingerprint = 4855 A9E6 8332 16D6 A77D 8FE4 51A8 E050 D005 2E5D

```

L'impronta digitale deve corrispondere a quanto riportato di seguito.

4855 A9E6 8332 16D6 A77D 8FE4 51A8 E050 D005 2E5D

Se la stringa dell'impronta non corrisponde, non installare l'agente. Contatto. Supporto AWS



4. Verificare la firma del pacchetto di installazione. Assicurati di sostituirli *agent-download-filename* con i valori specificati durante il download dell'agente, come indicato nella tabella precedente di questo argomento.

```
rpm --checksig agent-download-filename
```

Ad esempio, per l'architettura x86\_64 su Amazon Linux 2:

```
rpm --checksig amazon-ssm-agent.rpm
```

Questo comando restituisce un output simile al seguente.

```
amazon-ssm-agent.rpm: rsa sha1 md5 OK
```

Se pgp manca dall'output e la chiave pubblica è stata importata, l'agente non è firmato. Se l'output contiene la frase NOT OK (MISSING KEYS: (MD5) *key-id*), controlla di avere eseguito la procedura correttamente e verifica di avere scaricato SSM Agent 3.1.1141.0 o una versione successiva. Se continui a ricevere questa risposta, contatta l'agente Supporto e non installarlo.

## Verifica del Agente SSM pacchetto su un server Linux (v3.3.1611.0 e versioni precedenti)

### Prima di iniziare

Le procedure per GPG e RPM in questa sezione si applicano alla versione dell'SSM Agent 3.3.1611.0 e alle versioni precedenti. Si consiglia sempre di utilizzare la versione più recente dell'agente. Per informazioni, consulta [Verifica del Agente SSM pacchetto su un server Linux \(v3.3.4851.0 e versioni successive\)](#). Tuttavia, se hai un motivo specifico per continuare a utilizzare la versione dell'agente 3.3.1611.0 o quella precedente, segui le istruzioni in una delle seguenti procedure.

### GPG

Per verificare il Agente SSM pacchetto su un server Linux (v3.3.1611.0 e versioni precedenti)

1. Copia la seguente chiave pubblica e salvala in un file denominato `amazon-ssm-agent.gpg`.

**⚠ Important**

La chiave pubblica mostrata di seguito è scaduta il 17-02-2025 (17 febbraio 2025) e funziona per la versione 3.3.1611.0 e le versioni precedenti, fino alla 3.2.1542.0, e solo se è stata utilizzata in precedenza per verificare la firma dell'agente. Systems Manager pubblicherà una nuova chiave pubblica in questo argomento prima della scadenza di quella precedente. Ti invitiamo a sottoscrivere il feed RSS per questo argomento per ricevere una notifica quando sarà disponibile la nuova chiave.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

```
Version: GnuPG v2.0.22 (GNU/Linux)
```

```
mQENBGtIoIBCAD2M1aoGIE0FXynAHM/jtuvdAVVaX3Q4ZejTqrX+Jq8E1AMhxy0
GzHu2CDtCYxtVxXK3unptLVt2kGgJwNbhYC393jDeZx5dCda4Nk2YXX1UK3P461i
axuuXRzMYvfM4RZn+7bJTU635tA07q9Xm6MGD4TCTvsjBfVi0xbrx0g5ozWbJdSw
fSR8MwUirFmFpAefRlYfCEuZ8FHywa9U6jLeWt20/kqrZliJ0AGjGzXtB7EZkqKb
faCCxikjvvhF1awdEqSK4DQorC/0vQc4I5kP5y2CJbtXvX073QH2yE75JMDIIx9x
r0sIRUoSfK3UirWa0VuAnEE5ueKzZNqGG1J1ABEBAAG0J1NTTSBBZ2VudCA8c3Nt
LWFnZW50LXNpZ251ckBhbWF6b24uY29tPokBPwQTAQIAKQUCZ00iggIbLwUJAsaY
gAcLCQgHawIBBhUIAgkKCwQWAgMBAh4BAheAAAJELwfSVyX3QTt+icH/A//tJsW
I+7Ay8FGJh8dJPNy++HIBjVSfDGNJFWNbw1Z8uZcazHEcUCH3FhW4CLQLTZ30VPz
qvFwzDtrDVIN/Y9EGDhLMFvimrE+/z4o1WsJ5DANf6BnX8I5UNICrt5d8SWH1BEJ
2FWIBZFgKyTDI6XzRC5x4ahtgp0VAGeeKDehs+wh6Ga4W0/K4GsViP1Kyr+Ic2br
NAIq0q0IHYN1q9zam3Y0+jKwEuNmTj+Bjyzshyv/X8S0JWwoXJhkexk0vWeBYNNt
5wI4QcSteyfIzp6K1QF8q11Hzz9D9WaPfcBEYyqh7vLEARobkbQMBzpkmaZua241
0RaWG50HRvrgm4aJAhwEEAECAAYFAmTtIoMACgkQfdCXo9rX9fwwqBAAzkTgYJ38
sWgxp7Ux/81F2BWR1sVkmP79i++fXyJlKI8xtcJFQZhzeUos69KBUCy7mgx5bYU
P7NA5o9DUBwz/QS0i1Cqm4+jtFlX0MXe4FikXcqfDPnnzN8mVB2H+fa43iHR1PuH
GgUWuNdxzSoIYRmLZXWmeN5YXPcmix1hLzcE2T0Qn1m0Kcu2fKdLtBQ8KiEkjju
naoLxnUcyk1zMhaha+LzEkQd0yasix0ggy1N2ViWVnlmfy0niuXDxW0qZWPdLstF
00DiX3iqGmkH3rDfy6nvxxBR4GIs+MGD72fpWzzrINDgkGI2i2t1+0AX/mps3aTy
+ftlgrim8stYWB58XXDAb0vad06sNye5/zDzfr0I9HupJrTzFhaYJQjWPas1INto
LDJnBXohiUIPRYRcy/k012oFHDWZHT3H6CyjK9UD5U1xA9H7dsJurANs6F0VRe+7
34uJyxDZ/W7zLG4AVG0zxibrUSoaJxwc0jVPVsQAlrwG/GTs7tcAccsJqbJ1Py/w
9AgJl8VU2qc8P0sHNXk348gjP7C8PDnGmPZFzr9f5INctRushpiv7onX+aWJVX7T
n2uX/TP3LCyH/MsrNjrJ0QnMYFRLQitciP0E+F+eA3v9CY6mDuyb8JSx5HuGGUsG
S4bKB0cA8vimEpwPoT8CE7fdsZ3Qkwdu+pw=
```

```
=zr5w
```

```
-----END PGP PUBLIC KEY BLOCK-----
```

2. Importare la chiave pubblica nel keyring e osservare il valore della chiave restituito.

```
gpg --import amazon-ssm-agent.gpg
```

3. Verifica dell'impronta digitale. Assicurati di sostituirlo *key-value* con il valore del passaggio precedente. Si consiglia di utilizzare GPG per verificare l'impronta digitale anche se si utilizza RPM per verificare il pacchetto di installazione.

```
gpg --fingerprint key-value
```

Questo comando restituisce un output simile al seguente.

```
pub 2048R/97DD04ED 2023-08-28 [expired: 2025-02-17]
 Key fingerprint = DE92 C7DA 3E56 E923 31D6 2A36 BC1F 495C 97DD 04ED
uid SSM Agent <ssm-agent-signer@amazon.com>
```

L'impronta digitale deve corrispondere a quanto riportato di seguito.

DE92 C7DA 3E56 E923 31D6 2A36 BC1F 495C 97DD 04ED

Se la stringa dell'impronta non corrisponde, non installare l'agente. Contatto Supporto AWS.

4. Scaricare il file della firma in base all'architettura e al sistema operativo dell'istanza, se non è stato ancora fatto.
5. Verificare la firma del pacchetto di installazione. Assicurati di sostituire *signature-filename* e *agent-download-filename* con i valori specificati durante il download del file della firma e dell'agente, come indicato nella tabella precedente di questo argomento.

```
gpg --verify signature-filename agent-download-filename
```

Ad esempio, per l'architettura x86\_64 su Amazon Linux 2:

```
gpg --verify amazon-ssm-agent.rpm.sig amazon-ssm-agent.rpm
```

Questo comando restituisce un output simile al seguente:

```
gpg: Signature made Fri 10 Jan 2025 01:54:18 AM UTC using RSA key ID 97DD04ED
gpg: Good signature from "SSM Agent <ssm-agent-signer@amazon.com>"
gpg: Note: This key has expired!
```

Primary key fingerprint: DE92 C7DA 3E56 E923 31D6 2A36 BC1F 495C 97DD 04ED

Se l'output include la frase `BAD signature`, controllare di avere eseguito la procedura correttamente. Se continui a ricevere questa risposta, contatta l'agente Supporto e non installarlo. Il messaggio di avviso relativo all'attendibilità non indica che la firma non sia valida, ma soltanto che la chiave pubblica non è stata verificata. Una chiave è considerata attendibile solo se è stata firmata dall'utente o da un firmatario fidato. Se l'output include la frase `Can't check signature: No public key`, verifica di aver scaricato SSM Agent 3.1.1141.0 o una versione successiva.

## RPM

Per verificare il Agente SSM pacchetto su un server Linux (v3.3.1611.0 e versioni precedenti)

1. Copia la seguente chiave pubblica e salvala in un file denominato `amazon-ssm-agent.gpg`.

### Important

La chiave pubblica mostrata di seguito è scaduta il 17-02-2025 (17 febbraio 2025) e funziona per la versione 3.3.1611.0 e le versioni precedenti, fino alla 3.2.1542.0, e solo se è stata utilizzata in precedenza per verificare la firma dell'agente. Systems Manager pubblicherà una nuova chiave pubblica in questo argomento prima della scadenza di quella precedente. Ti invitiamo a sottoscrivere il feed RSS per questo argomento per ricevere una notifica quando sarà disponibile la nuova chiave.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

```
Version: GnuPG v2.0.22 (GNU/Linux)
```

```
mQENBGtTioIBCAD2M1aoGIE0FXynAHM/jtuvdAVVaX3Q4ZejTqrX+Jq8ElAMhxy0
GzHu2CDtCYxtVxXK3unptLVt2kGgJwNbhYC393jDeZx5dCda4Nk2YXX1UK3P461i
axuuXRzMYvfM4RZn+7bJTU635tA07q9Xm6MGD4TCTvsjBfVi0xbrx0g5ozWbJdSw
fSR8MwUrRfmFpAefRlYfCEuZ8FHywa9U6jLeWt20/kqrZliJ0AGjGzXtB7EZkqKb
faCCxikjjvhF1awdEqSK4DQorC/0vQc4I5kP5y2CJbtXvX073QH2yE75JMDIIx9x
r0sIRUoSfK3UUrWa0VuAnEE5ueKzZNqGG1J1ABEBAAG0J1NTTSBBZ2VudCA8c3Nt
LWFnZW50LXNpZ251ckBhbWF6b24uY29tPokBPwQTAQIAKQUCZ00iggIbLwUJAsaY
gAcLCQgHAWIBBhUIAgkKCwQWAgMBAh4BAheAAAJELwFSVyX3QTt+icH/A//tJsW
I+7Ay8FGJh8dJPNy++HIBjVSfdGNJFWNbw1Z8uZcazHEcUCH3FhW4CLQLT30VPz
qvFwzDtRDVIN/Y9EGDhLMFvimrE+/z4o1WsJ5DANf6BnX8I5UNICrt5d8SWH1BEJ
```

```

2FWIBZFgKyTDI6XzRC5x4ahtgp0VAGeeKDehs+wh6Ga4W0/K4GsviP1Kyr+Ic2br
NAIq0q0IHYN1q9zam3Y0+jKwEuNmTj+Bjyzshyv/X8S0JWwoXJhkexk0vWeBYNNt
5wI4QcSteyfIzp6K1QF8q11Hzz9D9WaPfcBEYyYhq7vLEARobkbQMBzpkmaZua241
0RaWG50HRvrgm4aJAhwEEAECAAYFamTtIoMACGkQfdCXo9rX9fwwqBAAzkTgYJ38
sWgxp7Ux/81F2BWR1sVkmP79i++fXyJlKI8xtcJFQZhzeUos69KBUCy7mgx5bYU
P7NA5o9DUbwz/QS0i1Cqm4+jtF1X0MXe4FikXcqfDPnnzN8mVB2H+fa43iHR1PuH
GgUWuNdxxSoIYRmLZXWmeN5YXPcmixlhLzcE2T0Qn1m0Kcu2fKdLtBQ8KiEkmjiu
naoLxnUcyk1zMhaha+LzEkQd0yasix0ggylN2ViWVnlmfy0niuXDxW0qZWPdLStF
00DiX3iqGmkH3rDfy6nvxxBR4GIs+MGD72fpWzzrINDgkGI2i2t1+0AX/mps3aTy
+ftlgrim8stYWB58XXDAB0vad06sNye5/zDzfr0I9HupJrTzFhaYJQjWPas1INto
LDJnBXohiUIPRYRcy/k012oFHDWZHT3H6CyjK9UD5U1xA9H7dsJurAns6F0VRe+7
34uJyxDZ/W7zLG4AVG0zxibrUSoaJxwc0jVPVsQAlrwG/GTs7tcAccsJqbJ1Py/w
9AgJl8VU2qc8P0sHNXk348gJP7C8PDnGmpZFzr9f5INctRushpiv7onX+aWJVX7T
n2uX/TP3LCyH/MsrNjrJ0QnMYFRLQitciP0E+F+eA3v9CY6mDuyb8JSx5HuGGUsG
S4bKB0cA8vimEpwPoT8CE7fdsZ3Qkwdu+pw=
=zi5w
-----END PGP PUBLIC KEY BLOCK-----

```

2. Importare la chiave pubblica nel keyring e osservare il valore della chiave restituito.

```
rpm --import amazon-ssm-agent.gpg
```

3. Verifica dell'impronta digitale. Si consiglia di utilizzare GPG per verificare l'impronta digitale anche se si utilizza RPM per verificare il pacchetto di installazione.

```
rpm -qa gpg-pubkey --qf '%{Description}' | gpg --with-fingerprint | grep -A 1
"ssm-agent-signer@amazon.com"
```

Questo comando restituisce un output simile al seguente:

```
pub 2048R/97DD04ED 2023-08-28 SSM Agent <ssm-agent-signer@amazon.com>
Key fingerprint = DE92 C7DA 3E56 E923 31D6 2A36 BC1F 495C 97DD 04ED
```

L'impronta digitale deve corrispondere a quanto riportato di seguito.

```
DE92 C7DA 3E56 E923 31D6 2A36 BC1F 495C 97DD 04ED
```

Se la stringa dell'impronta non corrisponde, non installare l'agente. Contatto. Supporto AWS

4. Verificare la firma del pacchetto di installazione. Assicurati di sostituirli *agent-download-filename* con i valori specificati durante il download dell'agente, come indicato nella tabella precedente di questo argomento.

```
rpm --checksig agent-download-filename
```

Ad esempio, per l'architettura x86\_64 su Amazon Linux 2:

```
rpm --checksig amazon-ssm-agent.rpm
```

Questo comando restituisce un output simile al seguente.

```
amazon-ssm-agent.rpm: rsa sha1 md5 OK
```

Se pgp manca dall'output e la chiave pubblica è stata importata, l'agente non è firmato. Se l'output contiene la frase NOT OK (MISSING KEYS: (MD5) *key-id*), controlla di avere eseguito la procedura correttamente e verifica di avere scaricato SSM Agent 3.1.1141.0 o una versione successiva. Se continui a ricevere questa risposta, contatta l'agente Supporto e non installarlo.

## Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux

Prima di installare manualmente AWS Systems Manager Agent (SSM Agent) su un sistema operativo Amazon Elastic Compute Cloud (Amazon EC2) Linux, consulta le seguenti informazioni.

### Installazione su altri tipi di macchine

Le procedure in questa sezione sono progettate specificamente per le istanze Amazon EC2. Per server on-premises, macchine virtuali o altri ambienti non EC2, utilizza lo strumento `ssm-setup-cli` come descritto in [Come installare l'SSM Agent su nodi Linux ibridi](#).

L'utilizzo delle procedure di installazione di EC2 su sistemi non EC2 può potenzialmente causare vulnerabilità di sicurezza. Lo strumento `ssm-setup-cli` fornisce protezioni di sicurezza aggiuntive per macchine non EC2.

Ti consigliamo vivamente di evitare l'uso di versioni del sistema operativo che hanno raggiunto End-of-Life (EOL). I fornitori di sistemi operativi, tra cui AWS in genere, non forniscono patch di sicurezza o altri aggiornamenti per le versioni che hanno raggiunto l'EOL. Continuare a utilizzare un sistema EOL aumenta notevolmente il rischio di non essere in grado di applicare gli aggiornamenti, comprese le correzioni di sicurezza e altri problemi

operativi. AWS non verifica la funzionalità di Systems Manager su versioni del sistema operativo che hanno raggiunto la fine del ciclo di vita.

## URL del file di installazione SSM Agent

È possibile accedere ai file di installazione SSM Agent archiviati in qualsiasi pubblicità Regione AWS. Forniamo inoltre i file di installazione in un bucket Amazon Simple Storage Service (Amazon S3) disponibile a livello globale che puoi utilizzare come fonte alternativa o di backup dei file.

Se stai installando l'agente manualmente su una o due istanze, puoi utilizzare i comandi descritti nelle procedure di Installazione rapida che forniamo per risparmiare tempo. I comandi forniti in queste procedure possono anche essere passati alle istanze Amazon EC2 come script tramite i dati utente.

Se stai creando uno script o un modello da utilizzare per l'installazione dell'agente su più istanze, ti consigliamo di utilizzare i file di installazione all'interno di o in prossimità della Regione AWS in cui ti trovi geograficamente. Per le installazioni in blocco, questo accorgimento può aumentare la velocità dei download e ridurre la latenza. In questi casi, ti consigliamo di utilizzare le procedure di Creazione di comandi di installazione personalizzati descritte negli argomenti di installazione.

## Amazon Machine Images con l'agente preinstallato

SSM Agent è preinstallato su some Amazon Machine Images (AMIs) fornito da AWS. Per informazioni, consulta [Trova AMI con il Agente SSM preinstallato](#).

## Mantenere l'agente aggiornato

Una versione aggiornata di SSM Agent viene distribuita ogni volta che vengono aggiunti nuovi strumenti a Systems Manager o eseguiti aggiornamenti degli strumenti esistenti. Il mancato utilizzo della versione più recente dell'agente può impedire al nodo gestito di utilizzare vari strumenti e funzionalità di Systems Manager. Per questo motivo, ti consigliamo di automatizzare il processo di aggiornamento di SSM Agent sulle macchine. Per informazioni, consulta [Automatizzazione degli aggiornamenti a Agente SSM](#). Iscriviti alla pagina [Note di rilascio di SSM Agent](#) su GitHub per ricevere notifiche sugli aggiornamenti di SSM Agent.

## Scelta del sistema operativo

Per visualizzare la procedura di installazione manuale di SSM Agent nel sistema operativo specificato, scegli un collegamento dall'elenco seguente:

 Note

Per un elenco delle versioni supportate di ciascuno dei seguenti sistemi operativi, consultare [Sistemi operativi supportati per Systems Manager](#).

- [AlmaLinux](#)
- [Amazon Linux 2 e Amazon Linux 2023](#)
- [Debian Server](#)
- [Oracle Linux](#)
- [Red Hat Enterprise Linux](#)
- [Rocky Linux](#)
- [Ubuntu Server](#)

## Disinstallazione di SSM Agent dalle istanze Linux

Usa il gestore di pacchetti del sistema operativo per disinstallare SSM Agent dalle istanze Linux. A seconda del sistema operativo, il comando di disinstallazione sarà simile al seguente comando di esempio:

```
sudo dpkg -r amazon-ssm-agent
```

## Installazione manuale Agente SSM sulle AlmaLinux istanze

Usa le informazioni in questa sezione per aiutarti a installare o reinstallare manualmente SSM Agent su un' AlmaLinux istanza.

### Prima di iniziare

Prima di eseguire l'installazione SSM Agent su un' AlmaLinux istanza, tieni presente quanto segue:

- Assicurati che Python 3 sia installato sulla tua AlmaLinux istanza. Questo è necessario SSM Agent per funzionare correttamente.
- Per informazioni importanti relative all'installazione di SSM Agent su tutti i sistemi Linux-based operativi, vedere [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#).



## Argomenti

- [Comandi di installazione rapida per Agente SSM acceso AlmaLinux](#)
- [Crea comandi di installazione degli agenti personalizzati per la tua AlmaLinux regione](#)

### Comandi di installazione rapida per Agente SSM acceso AlmaLinux

Completa la seguente procedura per installare manualmente SSM Agent su una singola istanza. Questa procedura utilizza i file di installazione disponibili a livello globale.

### Prima di iniziare

Prima di eseguire l'installazione SSM Agent su un' AlmaLinux istanza, tieni presente quanto segue:

- Assicurati che Python 3 sia installato sulla tua AlmaLinux istanza. Questo è necessario SSM Agent per funzionare correttamente.

### Per installare Agente SSM su AlmaLinux

1. Connettiti alla tua AlmaLinux istanza usando il tuo metodo preferito, ad esempio SSH.
2. Copia il comando per l'architettura della tua istanza ed eseguilo sull'istanza.

#### Note

Anche se gli URL nei comandi seguenti includono una `ec2-downloads-windows` directory, questi sono i file di installazione globali corretti per AlmaLinux

### Istanze x86\_64

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm
```

### Istanze ARM64

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_arm64/amazon-ssm-agent.rpm
```

3. (Consigliato) Esegui il seguente comando per verificare se l'agente è in esecuzione.

```
sudo systemctl status amazon-ssm-agent
```

Nella maggior parte dei casi, il comando segnala che l'agente è in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
 Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendor>
 Active: active (running) since Tue 2025-04-19 16:40:41 UTC; 9s ago
 Main PID: 4898 (amazon-ssm-agent)
 Tasks: 14 (limit: 4821)
 Memory: 34.6M
 CGroup: /system.slice/amazon-ssm-agent.service
 ##4898 /usr/bin/amazon-ssm-agent
 ##4954 /usr/bin/ssm-agent-worker
 --truncated--
```

In rari casi, il comando segnala che l'agente è installato ma non in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
 Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendor>
 Active: inactive (dead) since Tue 2025-04-19 16:42:05 UTC; 2s ago
 --truncated--
```

Per attivare l'agente in questi casi, esegui i comandi seguenti.

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

Crea comandi di installazione degli agenti personalizzati per la tua AlmaLinux regione

Quando esegui l'installazione di SSM Agent su più istanze utilizzando uno script o un modello, consigliamo di utilizzare i file di installazione archiviati nella Regione AWS in cui stai lavorando.

Per i comandi seguenti, forniamo esempi che utilizzano un bucket S3 accessibile pubblicamente nella Regione Stati Uniti orientali (Ohio) (us-east-2).

 Tip

Puoi anche sostituire un URL globale nella procedura [Comandi di installazione rapida per Agente SSM acceso AlmaLinux](#) descritta in precedenza in questo argomento con un URL Regionale personalizzato creato da te.

Nel comando seguente, sostituisci **region** con le tue informazioni. Per un elenco dei **region** valori supportati, vedere la colonna Regione negli endpoint del servizio [Systems Manager](#) in. Riferimenti generali di Amazon Web Services

x86\_64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

Guarda l'esempio seguente.

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

ARM64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_arm64/amazon-ssm-agent.rpm
```

Guarda l'esempio seguente.

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_arm64/amazon-ssm-agent.rpm
```

## Installazione manuale di SSM Agent su istanze Amazon Linux 2 e Amazon Linux 2023

Nella maggior parte dei casi, i Amazon Machine Images (AMIs) per Amazon Linux 2 e Amazon Linux 2023 forniti da sono AWS dotati di AWS Systems Manager Agent (SSM Agent) preinstallato per impostazione predefinita. Per ulteriori informazioni, consulta [Trova AMI con il Agente SSM preinstallato](#).

Nel caso in cui SSM Agent non sia preinstallato su una nuova istanza Amazon Linux 2 o Amazon Linux 2023 oppure tu debba reinstallare manualmente l'agente, utilizza le informazioni contenute in questa pagina.

## Prima di iniziare

Prima di installare SSM Agent su un'istanza Amazon Linux 2 o Amazon Linux 2023, tieni presente quanto segue:

- Per informazioni importanti relative all'installazione di SSM Agent su tutti i sistemi Linux-based operativi, consulta [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#).
- Se si utilizza un comando yum per aggiornare SSM Agent su un nodo gestito dopo che l'agente è stato installato o aggiornato utilizzando il documento SSM AWS-UpdateSSMAgent, è possibile che venga visualizzato il seguente messaggio: "Warning: RPMDB altered outside of yum." Questo messaggio è previsto e può essere ignorato in modo sicuro.

## Argomenti

- [Comandi di installazione rapida per SSM Agent su Amazon Linux 2 o Amazon Linux 2023](#)
- [Creare comandi di installazione dell'agente personalizzati per Amazon Linux 2 o Amazon Linux 2023 nella regione in uso](#)

## Comandi di installazione rapida per SSM Agent su Amazon Linux 2 o Amazon Linux 2023

Completa la seguente procedura per installare manualmente SSM Agent su una singola istanza. Questa procedura utilizza i file di installazione disponibili a livello globale.

Per installare SSM Agent su Amazon Linux 2 o Amazon Linux 2023 utilizzando comandi rapidi di copia e incolla

1. Connettiti all'istanza Amazon Linux 2 o Amazon Linux 2023 utilizzando il tuo metodo preferito, come ad esempio SSH.
2. Copia il comando per l'architettura della tua istanza ed eseguilo sull'istanza.

 Note

Anche se gli URL nei seguenti comandi includono una directory `ec2-downloads-windows`, questi sono i file di installazione globale corretti per Amazon Linux 2 e Amazon Linux 2023.

## x86\_64

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm
```

## ARM64

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_arm64/amazon-ssm-agent.rpm
```

3. (Consigliato) Esegui il seguente comando per verificare se l'agente è in esecuzione.

```
sudo systemctl status amazon-ssm-agent
```

Nella maggior parte dei casi, il comando segnala che l'agente è in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor preset: enabled)
Active: active (running) since Wed 2021-10-20 19:09:29 UTC; 4min 6s ago
 --truncated--
```

In rari casi, il comando segnala che l'agente è installato ma non in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor preset: enabled)
Active: inactive (dead) since Wed 2021-10-20 22:16:41 UTC; 18s ago
 --truncated--
```

Per attivare l'agente in questi casi, esegui il comando seguente.

```
sudo systemctl start amazon-ssm-agent
```

Creare comandi di installazione dell'agente personalizzati per Amazon Linux 2 o Amazon Linux 2023 nella regione in uso

Quando esegui l'installazione di SSM Agent su più istanze utilizzando uno script o un modello, consigliamo di utilizzare i file di installazione archiviati nella Regione AWS in cui stai lavorando.

Per i comandi seguenti, forniamo esempi che utilizzano un bucket S3 accessibile pubblicamente nella Regione Stati Uniti orientali (Ohio) (us-east-2).

#### Tip

Puoi anche sostituire un URL globale nella procedura [Comandi di installazione rapida per SSM Agent su Amazon Linux 2 o Amazon Linux 2023](#) descritta in precedenza in questo argomento con un URL Regionale personalizzato creato da te.

Nel comando seguente, sostituiscilo **region** con le tue informazioni. Per un elenco dei **region** valori supportati, vedere la colonna Regione negli [endpoint del servizio Systems Manager](#) in. Riferimenti generali di Amazon Web Services

x86\_64

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

Guarda l'esempio seguente.

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

ARM64

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_arm64/amazon-ssm-agent.rpm
```

Guarda l'esempio seguente.

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/linux_arm64/amazon-ssm-agent.rpm
```

## Installazione manuale di SSM Agent sulle istanze CentOS Stream

I Amazon Machine Images (AMIs) per CentOS Stream questo sono forniti da AWS non vengono forniti con AWS Systems Manager Agent (SSM Agent) preinstallato per impostazione predefinita. Per un elenco di AWS AMIs gestite su cui l'agente potrebbe essere preinstallato, consulta la sezione [Trova AMI con il Agente SSM preinstallato](#).

Utilizza le informazioni contenute in questa sezione per installare o reinstallare manualmente SSM Agent su un'istanza CentOS Stream.

Prima di iniziare

Prima di installare SSM Agent su un'istanza CentOS Stream, prendi nota di quanto segue:

- Per informazioni importanti relative all'installazione di SSM Agent su tutti i sistemi Linux-based operativi, vedere [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#).

Argomenti

- [Comandi di installazione rapida per SSM Agent su CentOS Stream](#)
- [Creazione di comandi di installazione dell'agente personalizzati per CentOS Stream nella Regione in uso](#)

Comandi di installazione rapida per SSM Agent su CentOS Stream

Completa la seguente procedura per installare manualmente SSM Agent su una singola istanza. Questa procedura utilizza i file di installazione disponibili a livello globale.

Per installare SSM Agent su CentOS Stream

1. Connettiti all'istanza CentOS Stream utilizzando il tuo metodo preferito, come ad esempio SSH.
2. Copia il comando per l'architettura della tua istanza ed eseguilo sull'istanza.

 Note

Anche se gli URL nei seguenti comandi includono una directory `ec2-downloads-windows`, questi sono i file di installazione globale corretti per CentOS Stream.

## Istanze x86\_64

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm
```

## Istanze ARM64

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_arm64/amazon-ssm-agent.rpm
```

3. (Consigliato) Esegui il seguente comando per verificare se l'agente è in esecuzione.

```
sudo systemctl status amazon-ssm-agent
```

Nella maggior parte dei casi, il comando segnala che l'agente è in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
 Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendo>
 Active: active (running) since Tue 2025-04-19 16:40:41 UTC; 9s ago
 Main PID: 4898 (amazon-ssm-agen)
 Tasks: 14 (limit: 4821)
 Memory: 34.6M
 CGroup: /system.slice/amazon-ssm-agent.service
 ##4898 /usr/bin/amazon-ssm-agent
 ##4954 /usr/bin/ssm-agent-worker
 --truncated--
```

In rari casi, il comando segnala che l'agente è installato ma non in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
 Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendo>
```



```
Active: inactive (dead) since Tue 2025-04-19 16:42:05 UTC; 2s ago
--truncated
```

Per attivare l'agente in questi casi, esegui i comandi seguenti.

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

Creazione di comandi di installazione dell'agente personalizzati per CentOS Stream nella Regione in uso

Quando esegui l'installazione di SSM Agent su più istanze utilizzando uno script o un modello, consigliamo di utilizzare i file di installazione archiviati nella Regione AWS in cui stai lavorando.

Per i comandi seguenti, forniamo esempi che utilizzano un bucket S3 accessibile pubblicamente nella Regione Stati Uniti orientali (Ohio) (us-east-2).

#### Tip

Puoi anche sostituire un URL globale nella procedura [Comandi di installazione rapida per SSM Agent su CentOS Stream](#) descritta in precedenza in questo argomento con un URL Regionale personalizzato creato da te.

Nel comando seguente, sostituiscilo **region** con le tue informazioni. Per un elenco dei **region** valori supportati, vedere la colonna Regione negli [endpoint del servizio Systems Manager](#) in. Riferimenti generali di Amazon Web Services

x86\_64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

Guarda l'esempio seguente.

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

## ARM64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_arm64/amazon-ssm-agent.rpm
```

Guarda l'esempio seguente.

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_arm64/amazon-ssm-agent.rpm
```

## Installazione manuale di SSM Agent su istanze Debian Server

I Amazon Machine Images (AMIs) per Debian Server questo sono forniti da AWS non vengono forniti con AWS Systems Manager Agent (SSM Agent) preinstallato per impostazione predefinita. Per un elenco di AWS AMIs gestite su cui l'agente potrebbe essere preinstallato, consulta la sezione [Trova AMI con il Agente SSM preinstallato](#).

Utilizza le informazioni contenute in questa sezione per installare o reinstallare manualmente SSM Agent su un'istanza Debian Server.

### Prima di iniziare

Prima di installare SSM Agent su un'istanza Debian Server, prendi nota di quanto segue:

- Per informazioni importanti relative all'installazione di SSM Agent su tutti i sistemi Linux-based operativi, vedere [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#).

### Argomenti

- [Comandi di installazione rapida per SSM Agent su Debian Server](#)
- [Creazione di comandi di installazione dell'agente personalizzati per Debian Server nella Regione in uso](#)

### Comandi di installazione rapida per SSM Agent su Debian Server

Completa la seguente procedura per installare manualmente SSM Agent su una singola istanza. Questa procedura utilizza i file di installazione disponibili a livello globale.

## Per installare SSM Agent su Debian Server

1. Connettiti all'istanza Debian Server utilizzando il tuo metodo preferito, come ad esempio SSH.
2. Esegui il comando seguente per creare una directory temporanea sull'istanza.

```
mkdir /tmp/ssm
```

3. Esegui il comando seguente per passare alla directory temporanea.

```
cd /tmp/ssm
```

4. Copia il comando per l'architettura della tua istanza ed eseguilo sull'istanza.

### Note

Anche se gli URL nei seguenti comandi includono una directory `ec2-downloads-windows`, questi sono i file di installazione globale corretti per Debian Server. Per Debian Server 8 è supportata l'architettura `x86_64`.

### Istanze x86\_64

```
wget https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/debian_amd64/amazon-ssm-agent.deb
```

### Istanze ARM64

```
wget https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/debian_arm64/amazon-ssm-agent.deb
```

5. Eseguire il seguente comando seguente.

```
sudo dpkg -i amazon-ssm-agent.deb
```

6. (Consigliato) Esegui il seguente comando per verificare se l'agente è in esecuzione.

```
sudo systemctl status amazon-ssm-agent
```

Nella maggior parte dei casi, il comando segnala che l'agente è in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
 Loaded: loaded (/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor
 Active: active (running) since Tue 2025-04-19 16:25:03 UTC; 4s ago
Main PID: 628 (amazon-ssm-agen)
 CGroup: /system.slice/amazon-ssm-agent.service
 ##628 /usr/bin/amazon-ssm-agent
 ##650 /usr/bin/ssm-agent-worker
 --truncated--
```

In rari casi, il comando segnala che l'agente è installato ma non in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
 Loaded: loaded (/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor
 Active: inactive (dead) since Tue 2025-04-19 16:26:30 UTC; 5s ago
Main PID: 628 (code=exited, status=0/SUCCESS)
 --truncated--
```

Per attivare l'agente in questi casi, esegui i comandi seguenti.

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

Creazione di comandi di installazione dell'agente personalizzati per Debian Server nella Regione in uso

Quando esegui l'installazione di SSM Agent su più istanze utilizzando uno script o un modello, consigliamo di utilizzare i file di installazione archiviati nella Regione AWS in cui stai lavorando.

Per i comandi seguenti, forniamo esempi che utilizzano un bucket S3 accessibile pubblicamente nella Regione Stati Uniti orientali (Ohio) (us-east-2).

 Tip

Puoi anche sostituire un URL globale nella procedura [Comandi di installazione rapida per SSM Agent su Debian Server](#) descritta in precedenza in questo argomento con un URL Regionale personalizzato creato da te.

Nel comando seguente, sostituiscilo **region** con le tue informazioni. Per un elenco dei **region** valori supportati, vedere la colonna Regione negli [endpoint del servizio Systems Manager](#) in. Riferimenti generali di Amazon Web Services

x86\_64

```
wget https://s3.region.amazonaws.com/amazon-ssm-region/latest/debian_amd64/amazon-ssm-agent.deb
```

```
sudo dpkg -i amazon-ssm-agent.deb
```

Guarda l'esempio seguente.

```
wget https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/debian_amd64/amazon-ssm-agent.deb
```

```
sudo dpkg -i amazon-ssm-agent.deb
```

ARM64

```
wget https://s3.region.amazonaws.com/amazon-ssm-region/latest/debian_arm64/amazon-ssm-agent.deb
```

```
sudo dpkg -i amazon-ssm-agent.deb
```

Guarda l'esempio seguente.

```
wget https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/debian_arm64/amazon-ssm-agent.deb
```

```
sudo dpkg -i amazon-ssm-agent.deb
```

## Installazione manuale di SSM Agent su istanze Oracle Linux

I Amazon Machine Images (AMIs) per Oracle Linux questo sono forniti da AWS non vengono forniti con AWS Systems Manager Agent (SSM Agent) preinstallato per impostazione predefinita. Per un elenco di AMIs gestite da AWS su cui l'agente potrebbe essere preinstallato, consulta la sezione [Trova AMI con il Agente SSM preinstallato](#).

Utilizza le informazioni contenute in questa sezione per installare o reinstallare manualmente SSM Agent su un'istanza Oracle Linux.

### Prima di iniziare

Prima di installare SSM Agent su un'istanza Oracle Linux, prendi nota di quanto segue:

- Per informazioni importanti relative all'installazione di SSM Agent su tutti i sistemi Linux-based operativi, vedere [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#).
- Se si utilizza un comando yum per aggiornare SSM Agent su un nodo gestito dopo che l'agente è stato installato o aggiornato utilizzando il documento SSM AWS-UpdateSSMAgent, è possibile che venga visualizzato il seguente messaggio: "Warning: RPMDB altered outside of yum." Questo messaggio è previsto e può essere ignorato in modo sicuro.

### Argomenti

- [Comandi di installazione rapida per SSM Agent su Oracle Linux](#)
- [Creazione di comandi di installazione dell'agente personalizzati per Oracle Linux nella Regione in uso](#)

### Comandi di installazione rapida per SSM Agent su Oracle Linux

Completa la seguente procedura per installare manualmente SSM Agent su una singola istanza. Questa procedura utilizza i file di installazione disponibili a livello globale.

Installare SSM Agent su Oracle Linux utilizzando comandi rapidi di copia e incolla

1. Connettiti all'istanza Oracle Linux utilizzando il tuo metodo preferito, come ad esempio SSH.
2. Copia il comando seguente ed eseguilo sull'istanza.

 Note

Anche se l'URL nei seguenti comandi include una directory `ec2-downloads-windows`, questi sono i file di installazione globale corretti per Oracle Linux.

x86\_64

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm
```

3. (Consigliato) Esegui il seguente comando per verificare se l'agente è in esecuzione.

```
sudo systemctl status amazon-ssm-agent
```

Nella maggior parte dei casi, il comando segnala che l'agente è in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor preset: enabled)
Active: active (running) since Wed 2021-10-20 19:09:29 UTC; 4min 6s ago
 --truncated--
```

In rari casi, il comando segnala che l'agente è installato ma non in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor preset: enabled)
Active: inactive (dead) since Wed 2021-10-20 22:16:41 UTC; 18s ago
 --truncated--
```

Per attivare l'agente in questi casi, esegui i comandi seguenti.

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

Creazione di comandi di installazione dell'agente personalizzati per Oracle Linux nella Regione in uso

Quando esegui l'installazione di SSM Agent su più istanze utilizzando uno script o un modello, consigliamo di utilizzare i file di installazione archiviati nella Regione AWS in cui stai lavorando.

Per i comandi seguenti, forniamo esempi che utilizzano un bucket S3 accessibile pubblicamente nella Regione Stati Uniti orientali (Ohio) (us-east-2).

#### Tip

Puoi anche sostituire un URL globale nella procedura [Comandi di installazione rapida per SSM Agent su Oracle Linux](#) descritta in precedenza in questo argomento con un URL Regionale personalizzato creato da te.

Nel comando seguente, sostituiscilo *region* con le tue informazioni. Per un elenco dei *region* valori supportati, vedere la colonna Regione negli [endpoint del servizio Systems Manager](#) in. Riferimenti generali di Amazon Web Services

x86\_64

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

Guarda l'esempio seguente.

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

## Installazione manuale di SSM Agent su istanze Red Hat Enterprise Linux

I Amazon Machine Images (AMIs) for Red Hat Enterprise Linux (RHEL) forniti da AWS non vengono forniti con AWS Systems Manager Agent (SSM Agent) preinstallato per impostazione predefinita. Per un elenco dei AWS gestiti AMIs su cui l'agente potrebbe essere preinstallato, vedere. [Trova AMI con il Agente SSM preinstallato](#)



Utilizza le informazioni contenute in questa sezione per installare o reinstallare manualmente SSM Agent su un'istanza RHEL.

### Prima di iniziare

Prima di installare SSM Agent su un'istanza RHEL, prendi nota di quanto segue:

- Per informazioni importanti relative all'installazione di SSM Agent su tutti i sistemi Linux-based operativi, vedere [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#).
- Se si utilizza un comando yum per aggiornare SSM Agent su un nodo gestito, dopo che l'agente è stato installato o aggiornato utilizzando il documento SSM AWS-UpdateSSMAgent, è possibile che venga visualizzato il seguente messaggio: "Warning: RPMDB altered outside of yum." Questo messaggio è previsto e può essere tranquillamente ignorato.

### Argomenti

- [Installa Agente SSM on RHEL 8.x, 9.x e 10.x](#)
- [Per installare SSM Agent su RHEL 7.x](#)

### Installa Agente SSM on RHEL 8.x, 9.x e 10.x

Le Amazon Machine Images (AMIs) per RHEL 8 e 9 fornite da AWS non vengono fornite con AWS Systems Manager Agent (SSM Agent) preinstallato per impostazione predefinita. Utilizza le informazioni contenute in questa pagina per installare o reinstallare l'agente sulle istanze RHEL 8 e 9.

### Prima di iniziare

Prima di installare SSM Agent su un'istanza RHEL 8, 9 o 10, prendi nota di quanto segue:

- Assicurati che Python 2 o Python 3 siano installati sulla tua istanza RHEL 8, 9 o 10. Questo è necessario per funzionare SSM Agent correttamente.

### Argomenti

- [Comandi di installazione rapida per Agente SSM on RHEL 8, 9 e 10](#)
- [Crea comandi di installazione dell'agente personalizzati per RHEL 8, 9 e 10 nella tua regione](#)

## Comandi di installazione rapida per Agente SSM on RHEL 8, 9 e 10

Completa la seguente procedura per installare manualmente SSM Agent su una singola istanza. Questa procedura utilizza i file di installazione disponibili a livello globale.

Per installare Agente SSM on RHEL 8.x, 9.x o 10.x

1. Connettiti all'istanza RHEL 8, 9 o 10 utilizzando il tuo metodo preferito, come ad esempio SSH.
2. Copia il comando per l'architettura della tua istanza ed esegilo sull'istanza.

### Note

Anche se gli URL nei seguenti comandi includono una directory `ec2-downloads-windows`, questi sono i file di installazione globale corretti per RHEL 8, 9 e 10.

### Istanze x86\_64

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm
```

### Istanze ARM64

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_arm64/amazon-ssm-agent.rpm
```

3. (Consigliato) Esegui il seguente comando per verificare se l'agente è in esecuzione.

```
sudo systemctl status amazon-ssm-agent
```

Nella maggior parte dei casi, il comando segnala che l'agente è in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
 Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendor>
 Active: active (running) since Tue 2025-04-19 16:40:41 UTC; 9s ago
 Main PID: 4898 (amazon-ssm-agent)
 Tasks: 14 (limit: 4821)
 Memory: 34.6M
 CGroup: /system.slice/amazon-ssm-agent.service
```

```
##4898 /usr/bin/amazon-ssm-agent
##4954 /usr/bin/ssm-agent-worker
--truncated--
```

In rari casi, il comando segnala che l'agente è installato ma non in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendor>
Active: inactive (dead) since Tue 2025-04-19 16:42:05 UTC; 2s ago
--truncated--
```

Per attivare l'agente in questi casi, esegui i comandi seguenti.

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

Crea comandi di installazione dell'agente personalizzati per RHEL 8, 9 e 10 nella tua regione

Quando esegui l'installazione di SSM Agent su più istanze utilizzando uno script o un modello, consigliamo di utilizzare i file di installazione archiviati nella Regione AWS in cui stai lavorando.

Per i comandi seguenti, forniamo esempi che utilizzano un bucket S3 accessibile pubblicamente nella Regione Stati Uniti orientali (Ohio) (us-east-2).

#### Tip

Puoi anche sostituire un URL globale nella procedura [Comandi di installazione rapida per Agente SSM on RHEL 8, 9 e 10](#) descritta in precedenza in questo argomento con un URL Regionale personalizzato creato da te.

Nel comando seguente, sostituisci *region* con le tue informazioni. Per un elenco dei *region* valori supportati, vedere la colonna Regione negli endpoint del servizio [Systems Manager](#) in [Riferimenti generali di Amazon Web Services](#)

## x86\_64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

Guarda l'esempio seguente.

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

## ARM64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_arm64/amazon-ssm-agent.rpm
```

Guarda l'esempio seguente.

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_arm64/amazon-ssm-agent.rpm
```

Per installare SSM Agent su RHEL 7.x

I Amazon Machine Images (AMIs) for RHEL 7 forniti da AWS non vengono forniti con AWS Systems Manager Agent (SSM Agent) preinstallato per impostazione predefinita. Utilizza le informazioni contenute in questa sezione per installare o reinstallare l'agente sulle istanze RHEL 7.

### Argomenti

- [Comandi di installazione rapida per SSM Agent su RHEL 7](#)
- [Creazione di comandi di installazione dell'agente personalizzati per RHEL 7 nella regione in uso](#)

### Comandi di installazione rapida per SSM Agent su RHEL 7

Completa la seguente procedura per installare manualmente SSM Agent su una singola istanza. Questa procedura utilizza i file di installazione disponibili a livello globale.

Per installare SSM Agent su RHEL 7.x

1. Connettiti all'istanza RHEL 7 utilizzando il tuo metodo preferito, come ad esempio SSH.
2. Copia il comando per l'architettura della tua istanza ed esegilo sull'istanza.

 Note

Anche se gli URL nei seguenti comandi includono una directory `ec2-downloads-windows`, questi sono i file di installazione globale corretti per RHEL 7.

## Istanze x86\_64

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm
```

## Istanze ARM64

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_arm64/amazon-ssm-agent.rpm
```

3. (Consigliato) Esegui il seguente comando per verificare se l'agente è in esecuzione.

```
sudo systemctl status amazon-ssm-agent
```

Nella maggior parte dei casi, il comando segnala che l'agente è in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
 Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendor
 preset: disabled)
 Active: active (running) since Tue 2025-04-19 16:47:36 UTC; 22s ago
 Main PID: 1342 (amazon-ssm-agen)
 CGroup: /system.slice/amazon-ssm-agent.service
 ##1342 /usr/bin/amazon-ssm-agent
 ##1362 /usr/bin/ssm-agent-worker
 --truncated--
```

In rari casi, il comando segnala che l'agente è installato ma non in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
 Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendor
 preset: disabled)
```

```
Active: inactive (dead) since Tue 2025-04-19 16:48:56 UTC; 5s ago
Process: 1342 ExecStart=/usr/bin/amazon-ssm-agent (code=exited, status=0/SUCCESS)
Main PID: 1342 (code=exited, status=0/SUCCESS)
--truncated--
```

Per attivare l'agente in questi casi, esegui i comandi seguenti.

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

Creazione di comandi di installazione dell'agente personalizzati per RHEL 7 nella regione in uso

Quando esegui l'installazione di SSM Agent su più istanze utilizzando uno script o un modello, consigliamo di utilizzare i file di installazione archiviati nella Regione AWS in cui stai lavorando.

Per i comandi seguenti, forniamo esempi che utilizzano un bucket S3 accessibile pubblicamente nella Regione Stati Uniti orientali (Ohio) (us-east-2).

#### Tip

Puoi anche sostituire un URL globale nella procedura [Comandi di installazione rapida per SSM Agent su RHEL 7](#) descritta in precedenza in questo argomento con un URL Regionale personalizzato creato da te.

Nel comando seguente, sostituiscilo *region* con le tue informazioni. Per un elenco dei *region* valori supportati, vedere la colonna Regione negli [endpoint del servizio Systems Manager](#) in. Riferimenti generali di Amazon Web Services

x86\_64

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

Guarda l'esempio seguente.

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

## ARM64

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_arm64/amazon-ssm-agent.rpm
```

Guarda l'esempio seguente.

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_arm64/amazon-ssm-agent.rpm
```

## Installazione manuale Agente SSM on Rocky Linux Istanze

I Amazon Machine Images (AMIs) per Rocky Linux i quali sono forniti da AWS non vengono forniti con AWS Systems Manager Agent (SSM Agent) preinstallato per impostazione predefinita. Per un elenco di AMIs gestite da AWS su cui l'agente potrebbe essere preinstallato, consulta la sezione [Trova AMI con il Agente SSM preinstallato](#).

Utilizza le informazioni contenute in questa sezione per installare o reinstallare manualmente SSM Agent su un'istanza Rocky Linux.

Prima di iniziare

Prima di installare SSM Agent su un'istanza Rocky Linux, prendi nota di quanto segue:

- Per informazioni importanti relative all'installazione di SSM Agent su tutti i sistemi Linux-based operativi, vedere [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#).

### Argomenti

- [Comandi di installazione rapida per Agente SSM on Rocky Linux](#)
- [Creare comandi di installazione dell'agente personalizzati per Rocky Linux nella tua regione](#)

### Comandi di installazione rapida per Agente SSM on Rocky Linux

Completa la seguente procedura per installare manualmente SSM Agent su una singola istanza. Questa procedura utilizza i file di installazione disponibili a livello globale.

## Prima di iniziare

Prima di installare SSM Agent su un'istanza Rocky Linux, prendi nota di quanto segue:

- Assicurati che Python 2 o Python 3 siano installati sulla tua Rocky Linux istanza. Questo è necessario per funzionare SSM Agent correttamente.

Per installare Agente SSM on Rocky Linux

1. Connettiti all'istanza Rocky Linux utilizzando il tuo metodo preferito, come ad esempio SSH.
2. Copia il comando per l'architettura della tua istanza ed esegilo sull'istanza.

### Note

Anche se gli URL nei seguenti comandi includono una directory `ec2-downloads-windows`, questi sono i file di installazione globale corretti per Rocky Linux.

### Istanze x86\_64

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm
```

### Istanze ARM64

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_arm64/amazon-ssm-agent.rpm
```

3. (Consigliato) Esegui il seguente comando per verificare se l'agente è in esecuzione.

```
sudo systemctl status amazon-ssm-agent
```

Nella maggior parte dei casi, il comando segnala che l'agente è in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
 Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendor>
 Active: active (running) since Tue 2025-04-19 16:40:41 UTC; 9s ago
 Main PID: 4898 (amazon-ssm-agen)
```



```
Tasks: 14 (limit: 4821)
Memory: 34.6M
CGroup: /system.slice/amazon-ssm-agent.service
 ##4898 /usr/bin/amazon-ssm-agent
 ##4954 /usr/bin/ssm-agent-worker
 --truncated--
```

In rari casi, il comando segnala che l'agente è installato ma non in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendo>
Active: inactive (dead) since Tue 2025-04-19 16:42:05 UTC; 2s ago
 --truncated--
```

Per attivare l'agente in questi casi, esegui i comandi seguenti.

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

Creare comandi di installazione dell'agente personalizzati per Rocky Linux nella tua regione

Quando esegui l'installazione di SSM Agent su più istanze utilizzando uno script o un modello, consigliamo di utilizzare i file di installazione archiviati nella Regione AWS in cui stai lavorando.

Per i comandi seguenti, forniamo esempi che utilizzano un bucket S3 accessibile pubblicamente nella Regione Stati Uniti orientali (Ohio) (us-east-2).

#### Tip

Puoi anche sostituire un URL globale nella procedura [Comandi di installazione rapida per Agente SSM on Rocky Linux](#) descritta in precedenza in questo argomento con un URL Regionale personalizzato creato da te.

Nel comando seguente, sostituisci *region* con le tue informazioni. Per un elenco dei *region* valori supportati, vedere la colonna Regione negli endpoint del servizio [Systems Manager](#) in. Riferimenti generali di Amazon Web Services

x86\_64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

Guarda l'esempio seguente.

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

ARM64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_arm64/amazon-ssm-agent.rpm
```

Guarda l'esempio seguente.

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_arm64/amazon-ssm-agent.rpm
```

## Installazione manuale di SSM Agent sulle istanze SUSE Linux Enterprise Server

Nella maggior parte dei casi, i Amazon Machine Images (AMIs) for SUSE Linux Enterprise Server (SLES) AWS forniti da hanno AWS Systems Manager Agent (SSM Agent) preinstallato per impostazione predefinita. Per ulteriori informazioni, consulta [Trova AMI con il Agente SSM preinstallato](#).

Nel caso in cui SSM Agent non sia preinstallato su una nuova istanza SLES oppure tu debba reinstallare manualmente l'agente, utilizza le informazioni contenute in questa pagina.

Prima di iniziare

Prima di installare SSM Agent su un'istanza SLES, prendi nota di quanto segue:

- Per informazioni importanti relative all'installazione di SSM Agent su tutti i sistemi Linux-based operativi, vedere [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#).

## Argomenti

- [Comandi di installazione rapida per SSM Agent su SLES](#)
- [Creazione di comandi di installazione dell'agente personalizzati per SLES nella Regione in uso](#)

### Comandi di installazione rapida per SSM Agent su SLES

Completa la seguente procedura per installare manualmente SSM Agent su una singola istanza. Questa procedura utilizza i file di installazione disponibili a livello globale.

Installare SSM Agent su SLES utilizzando comandi rapidi di copia e incolla

1. Connettiti all'istanza SLES utilizzando il tuo metodo preferito, come ad esempio SSH.
2. Opzione 1: Usa un comando zypper:

- Esegui il comando seguente:

```
sudo zypper install amazon-ssm-agent
```

- Inserisci y in risposta a eventuali prompt.

Opzione 2: Usa un comando rpm.

- Creare una directory temporanea sull'istanza.

```
mkdir /tmp/ssm
```

- Passare alla directory temporanea.

```
cd /tmp/ssm
```

- Eseguire i seguenti comandi uno alla volta per scaricare ed eseguire il programma di installazione di SSM Agent.

#### Note

Anche se gli URL nei seguenti comandi includono una directory `ec2-downloads-windows`, questi sono i file di installazione globale corretti per SLES.

### Istanze x86\_64:

```
wget https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_amd64/
amazon-ssm-agent.rpm
```

### Istanze ARM64:

```
wget https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_arm64/
amazon-ssm-agent.rpm
```

- Eseguire il seguente comando seguente.

```
sudo rpm --install amazon-ssm-agent.rpm
```

- (Consigliato) Esegui il seguente comando per verificare se l'agente è in esecuzione.

```
sudo systemctl status amazon-ssm-agent
```

Nella maggior parte dei casi, il comando segnala che l'agente è in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2025-02-21 23:13:28 UTC; 7s ago
Main PID: 2102 (amazon-ssm-agent)
Tasks: 15 (limit: 512)
CGroup: /system.slice/amazon-ssm-agent.service
##2102 /usr/sbin/amazon-ssm-agent
##2107 /usr/sbin/ssm-agent-worker
--truncated--
```

In rari casi, il comando segnala che l'agente è installato ma non in esecuzione, come mostrato nell'esempio seguente.

```
amazon-ssm-agent.service - amazon-ssm-agent
Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; disabled;
vendor preset: disabled)
Active: inactive (dead)
```

```
--truncated--
```

Per attivare l'agente in questi casi, esegui i comandi seguenti.

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

Creazione di comandi di installazione dell'agente personalizzati per SLES nella Regione in uso

Quando esegui l'installazione di SSM Agent su più istanze utilizzando uno script o un modello, consigliamo di utilizzare i file di installazione archiviati nella Regione AWS in cui stai lavorando.

Per i comandi seguenti, forniamo esempi che utilizzano un bucket S3 accessibile pubblicamente nella Regione Stati Uniti orientali (Ohio) (us-east-2).

#### Tip

Puoi anche sostituire un URL globale nella procedura [Comandi di installazione rapida per SSM Agent su SLES](#) descritta in precedenza in questo argomento con un URL Regionale personalizzato creato da te.

Nel comando seguente, sostituiscilo *region* con le tue informazioni. Per un elenco dei *region* valori supportati, vedere la colonna Regione negli [endpoint del servizio Systems Manager](#) in. Riferimenti generali di Amazon Web Services

x86\_64

```
wget https://s3.region.amazonaws.com/amazon-ssm-region/latest/linux_amd64/amazon-ssm-agent.rpm
```

```
sudo rpm --install amazon-ssm-agent.rpm
```

Guarda l'esempio seguente.

```
wget https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/linux_amd64/amazon-ssm-agent.rpm
```

```
sudo rpm --install amazon-ssm-agent.rpm
```

## ARM64

```
wget https://s3.region.amazonaws.com/amazon-ssm-region/latest/linux_arm64/amazon-ssm-agent.rpm
```

```
sudo rpm --install amazon-ssm-agent.rpm
```

Guarda l'esempio seguente.

```
wget https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/linux_arm64/amazon-ssm-agent.rpm
```

```
sudo rpm --install amazon-ssm-agent.rpm
```

## Installazione manuale Agente SSM on Ubuntu Server Istanze

Nella maggior parte dei casi, i Amazon Machine Images (AMIs) for Ubuntu Server that AWS vengono forniti con AWS Systems Manager Agent (SSM Agent) preinstallato per impostazione predefinita. Per ulteriori informazioni, consulta [Trova AMI con il Agente SSM preinstallato](#).

Nel caso in cui SSM Agent non sia preinstallato su una nuova istanza Ubuntu Server oppure tu debba reinstallare manualmente l'agente, utilizza le informazioni contenute in questa pagina.

### Prima di iniziare

Prima di installare SSM Agent su un'istanza Ubuntu Server, prendi nota di quanto segue:

- Per informazioni importanti relative all'installazione di SSM Agent su tutti i sistemi Linux-based operativi, vedere [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux](#).

### Argomenti

- [Installa Agente SSM on Ubuntu Server 18.04, 20.04, 22.04 LTS, 23.10, 24.04 LTS, 24.0 e 25.04](#)

## Installa Agente SSM on Ubuntu Server 18.04, 20.04, 22.04 LTS, 23.10, 24.04 LTS, 24.0 e 25.04

### Prima di iniziare

Prima di procedere all'installazione SSM Agent su una versione Ubuntu Server 18.04, 20.04, 22.04 LTS, 23.10, 24.04 LTS, 24.0 e 25.04, tieni presente quanto segue:

### Posizioni dei file del programma di installazione SSM Agent

Nelle versioni Ubuntu Server 18.04, 20.04, 22.04 LTS, 23.10, 24.04 LTS, 24.0 e 25.04, i file di installazione, inclusi i file binari degli agenti e i file di configurazione, vengono memorizzati nella seguente directory: `/snap/amazon-ssm-agent/current/`. Se apporti modifiche ai file di configurazione in questa directory, devi copiare questi file dalla cartella `/snap` nella cartella `/etc/amazon/ssm/`. I file di log e della libreria non sono cambiati (`/var/lib/amazon/ssm/`, `/var/log/amazon/ssm/`).

### Utilizzo del canale candidate di Snap

Il canale candidato nell'archivio Snap contiene l'ultima versione di SSM Agent (incluse tutte le ultime correzioni di bug), non il canale stabile. Per ulteriori informazioni sulle differenze tra i canali candidati e stabili, consulta l'indirizzo. Risk-levels <https://snapcraft.io/docs/channels>

Se desideri tenere traccia delle informazioni sulla SSM Agent versione sul canale candidato, esegui il comando seguente sulle istanze LTS a Ubuntu Server 64 bit 20.04 e 18.04.

```
sudo snap switch --channel=candidate amazon-ssm-agent
```

### Snap consigliati per le versioni 18.04 e successive

Su Ubuntu Server 18.04, 20.04, 22.04 LTS, 23.10, 24.04 LTS, 24.0 e 25.04, consigliamo di utilizzare solo Snap. Verifica anche che solo un'istanza dell'agente sia installata e in esecuzione sulle istanze.

### Messaggio di errore `Maximum timeout exceeded`

A causa di un problema noto con Snap, potrebbe essere visualizzato un errore di `Maximum timeout exceeded` con i comandi snap. Se si verifica questo errore, esegui i seguenti comandi uno alla volta per avviare l'agente, arrestalo e verificane lo stato:

```
sudo systemctl start snap.amazon-ssm-agent.amazon-ssm-agent.service
```

```
sudo systemctl stop snap.amazon-ssm-agent.amazon-ssm-agent.service
```

```
sudo systemctl status snap.amazon-ssm-agent.amazon-ssm-agent.service
```

Per installare Agente SSM on Ubuntu Server 18.04, 20.04, 22.04 LTS, 23.10, 24.04 LTS, 24.0 e 25.04 (con pacchetto Snap)

1. SSM Agent viene installato, per impostazione predefinita, nelle versioni Ubuntu Server 18.04, 20.04, 22.04 LTS, 23.10, 24.04 LTS, 24.0 e 25.04 con un identificatore uguale o successivo. AMIs 20180627

Se si deve installare SSM Agent su un server on-premises o se è necessario reinstallare l'agente, è possibile utilizzare il seguente script. [Non è necessario specificare un URL per il download, poiché il snap comando scarica automaticamente l'agente dall'app store Snap all'indirizzo. https://snapcraft.io](https://snapcraft.io)

```
sudo snap install amazon-ssm-agent --classic
```

2. Eseguire il seguente comando per stabilire se SSM Agent è in esecuzione.

```
sudo snap list amazon-ssm-agent
```

3. Eseguire il comando seguente per avviare il servizio se il comando precedente restituisce `amazon-ssm-agent is stopped, inactive o disabled`.

```
sudo snap start amazon-ssm-agent
```

4. Controllare lo stato dell'agente.

```
sudo snap services amazon-ssm-agent
```

## Configurazione Agente SSM usare un proxy su nodi Linux

È possibile configurare AWS Systems Manager Agent (SSM Agent) per comunicare tramite un proxy HTTP creando un file di configurazione sostitutivo e aggiungendo `http_proxy no_proxy` impostazioni al file. `https_proxy` Un file di sostituzione mantiene le impostazioni proxy anche se si installano versioni più o meno recenti di SSM Agent. Questa sezione include le procedure per creare un file di sostituzione sia negli ambienti upstart che systemd. Se intendi utilizzare Session Manager, ricorda che i server proxy HTTPS non sono supportati.



## Argomenti

- [Configura Agente SSM usare un proxy \(upstart\)](#)
- [Configura Agente SSM usare un proxy \(systemd\)](#)

## Configura Agente SSM usare un proxy (upstart)

Usare la procedura seguente per creare un file di configurazione sostitutiva per un ambiente upstart.

Per configurare Agente SSM usare un proxy (upstart)

1. Connettersi all'istanza gestita in cui è installato SSM Agent.
2. Aprire un editor semplice come VIM e, a seconda che si stia utilizzando un server proxy HTTP o un server proxy HTTPS, aggiungere una delle seguenti configurazioni.

Per un server proxy HTTP:

```
env http_proxy=http://hostname:port
env https_proxy=http://hostname:port
env no_proxy=IP address for instance metadata services (IMDS)
```

Per un server proxy HTTPS:

```
env http_proxy=http://hostname:port
env https_proxy=https://hostname:port
env no_proxy=IP address for instance metadata services (IMDS)
```

### Important

Aggiungi al file l'impostazione `no_proxy` e specifica l'indirizzo IP. L'indirizzo IP per `no_proxy` è l'endpoint dei servizi di metadati di istanza (IMDA) per Systems Manager. Se non viene specificato `no_proxy`, le chiamate a Systems Manager acquisiscono l'identità dal servizio proxy (se il fallback IMDSv1 è abilitato) oppure le chiamate a Systems Manager hanno esito negativo (se è applicato IMDSv2).

- Per IPv4, specifica `no_proxy=169.254.169.254`.
- Per IPv6, specifica `no_proxy=[fd00:ec2::254]`. L'indirizzo IPv6 del servizio metadati dell'istanza è compatibile con i comandi IMDSv2. L'indirizzo IPv6 è

accessibile solo su istanze costruite sul [sistema Nitro AWS](#). Per ulteriori informazioni, consulta [Come funziona il servizio di metadati di istanza versione 2](#) nella Guida per l'utente di Amazon EC2.

3. Salvare il file con il nome `amazon-ssm-agent.override` nella posizione seguente: `/etc/init/`
4. Arrestare e riavviare SSM Agent utilizzando i seguenti comandi.

```
sudo service stop amazon-ssm-agent
sudo service start amazon-ssm-agent
```

#### Note

Per ulteriori informazioni sul funzionamento dei file `.override` in ambienti Upstart, consultare [init: configurazione del processo daemon init di Upstart](#).

## Configura Agente SSM usare un proxy (systemd)

Utilizzare la procedura seguente per configurare SSM Agent per l'utilizzo di un proxy in un ambiente systemd.

#### Note

Alcuni dei passaggi nella procedura contengono istruzioni esplicite per le istanze Ubuntu Server in cui SSM Agent è stato installato tramite Snap.

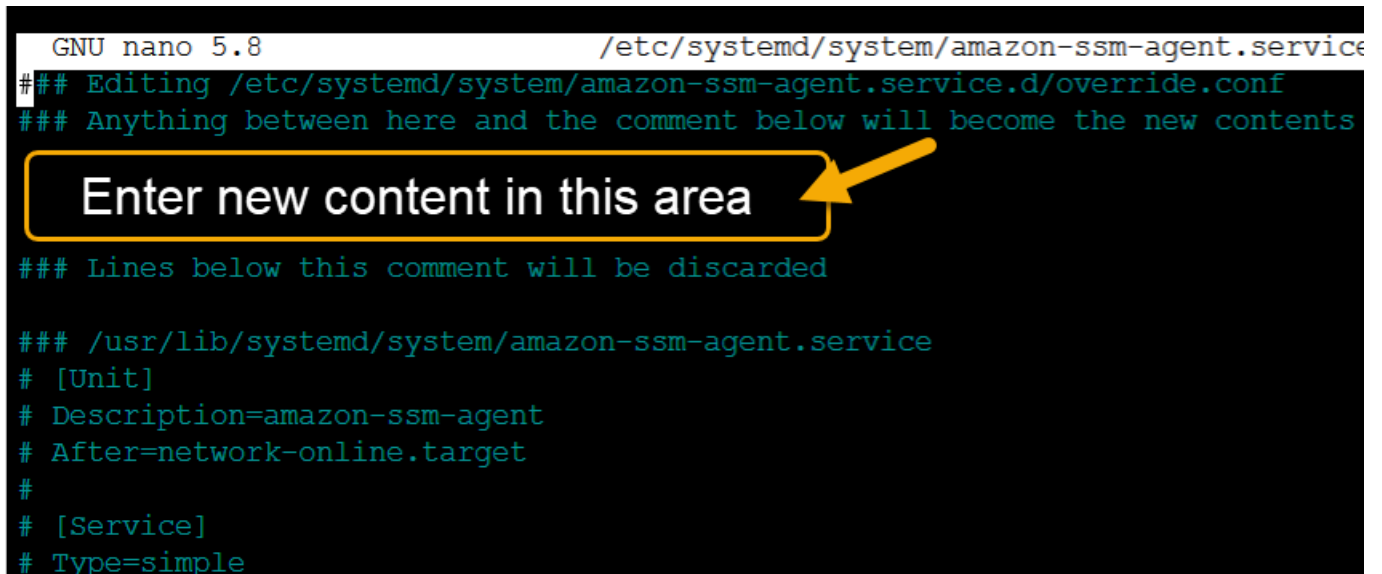
1. Connettersi all'istanza in cui è installato SSM Agent.
2. A seconda del tipo di sistema operativo, eseguire uno dei seguenti comandi.
  - Sulle istanze di Ubuntu Server dove SSM Agent viene installato utilizzando uno snap:

```
sudo systemctl edit snap.amazon-ssm-agent.amazon-ssm-agent
```

Su altri sistemi operativi:

```
sudo systemctl edit amazon-ssm-agent
```

3. Aprire un editor semplice come VIM e, a seconda che si stia utilizzando un server proxy HTTP o un server proxy HTTPS, aggiungere una delle seguenti configurazioni.



```
GNU nano 5.8 /etc/systemd/system/amazon-ssm-agent.service
Editing /etc/systemd/system/amazon-ssm-agent.service.d/override.conf
Anything between here and the comment below will become the new contents

Enter new content in this area

Lines below this comment will be discarded

/usr/lib/systemd/system/amazon-ssm-agent.service
[Unit]
Description=amazon-ssm-agent
After=network-online.target
#
[Service]
Type=simple
```

Per un server proxy HTTP:

```
[Service]
Environment="http_proxy=http://hostname:port"
Environment="https_proxy=http://hostname:port"
Environment="no_proxy=IP address for instance metadata services (IMDS)"
```

Per un server proxy HTTPS:

```
[Service]
Environment="http_proxy=http://hostname:port"
Environment="https_proxy=https://hostname:port"
Environment="no_proxy=IP address for instance metadata services (IMDS)"
```

### ⚠ Important

Aggiungi al file l'impostazione `no_proxy` e specifica l'indirizzo IP. L'indirizzo IP per `no_proxy` è l'endpoint dei servizi di metadati di istanza (IMDA) per Systems Manager. Se non viene specificato `no_proxy`, le chiamate a Systems Manager acquisiscono

l'identità dal servizio proxy (se il fallback IMDSv1 è abilitato) oppure le chiamate a Systems Manager hanno esito negativo (se è applicato IMDSv2).

- Per IPv4, specifica `no_proxy=169.254.169.254`.
- Per IPv6, specifica `no_proxy=[fd00:ec2::254]`. L'indirizzo IPv6 del servizio metadati dell'istanza è compatibile con i comandi IMDSv2. L'indirizzo IPv6 è accessibile solo su istanze costruite sul [sistema Nitro AWS](#). Per ulteriori informazioni, consulta [Come funziona il servizio di metadati di istanza versione 2](#) nella Guida per l'utente di Amazon EC2.

4. Salvare le modifiche. Il sistema crea automaticamente uno dei file riportati di seguito, a seconda del tipo di sistema operativo.

- Sulle istanze di Ubuntu Server dove SSM Agent viene installato utilizzando uno snap:

```
/etc/systemd/system/snap.amazon-ssm-agent.amazon-ssm-agent.service.d/override.conf
```

- Nelle istanze Amazon Linux 2, Amazon Linux 2023 e RHEL:

```
/etc/systemd/system/amazon-ssm-agent.service.d/override.conf
```

- Su altri sistemi operativi:

```
/etc/systemd/system/amazon-ssm-agent.service.d/amazon-ssm-agent.override
```

5. Riavvia SSM Agent utilizza uno dei seguenti comandi, a seconda del tipo di sistema operativo.

- Sulle istanze di Ubuntu Server installate utilizzando uno snap:

```
sudo systemctl daemon-reload && sudo systemctl restart snap.amazon-ssm-agent.amazon-ssm-agent
```

- Su altri sistemi operativi:

```
sudo systemctl daemon-reload && sudo systemctl restart amazon-ssm-agent
```

 Note

Per ulteriori informazioni sull'utilizzo dei file `.override` in ambienti `systemd`, consultare [Modifica dei file di unità esistenti](#) [nella](#) Guida per gli amministratori di sistema di Red Hat Enterprise Linux 7.

## Utilizzo di SSM Agent sulle istanze EC2 per macOS

AWS Systems Manager (SSM Agent) elabora le richieste di Systems Manager e configura la macchina come specificato nella richiesta. Utilizzare le seguenti procedure per installare, configurare o disinstallare SSM Agent per macOS.

 Note

SSM Agent è preinstallato per default su Amazon Machine Images (AMIs) per macOS. Non è necessario installare SSM Agent su un'istanza Amazon Elastic Compute Cloud (Amazon EC2) per macOS a meno che non sia stato disinstallato.

Il codice sorgente per SSM Agent è disponibile su [GitHub](#) in modo da poter adattare l'agente per soddisfare le esigenze dell'utente. Ti consigliamo di inviare le [richieste pull](#) per le modifiche da includere. Tuttavia, AWS attualmente non fornisce il supporto per eseguire copie modificate di questo software.

 Note

Per visualizzare i dettagli sulle diverse versioni di SSM Agent, consultare le [note di rilascio](#).

Prima di installare manualmente SSM Agent su un sistema operativo macOS, esaminare le seguenti informazioni.

- SSM Agent è installato per impostazione predefinita sulle istanze EC2 e Amazon Machine Images supportato da Systems Manager. Per ulteriori informazioni, consulta l'[elenco di sistemi operativi supportati per macOS](#).

Non è necessario installare manualmente SSM Agent sulle istanze EC2 macOS a meno che non sia stato disinstallato.

- Le istanze EC2 per non macOS sono supportate in tutte le Regioni AWS. Per visualizzare gli elenchi delle regioni in cui sono supportate le istanze basate su x86 e le istanze M1 EC2 per macOS, consulta [Carichi di lavoro macOS](#) nelle Domande frequenti su Amazon EC2.
- Una versione aggiornata di SSM Agent viene distribuita ogni volta che vengono aggiunti nuovi strumenti a Systems Manager o eseguiti aggiornamenti degli strumenti esistenti. Il mancato utilizzo della versione più recente dell'agente può impedire al nodo gestito di utilizzare vari strumenti e funzionalità di Systems Manager. Per questo motivo, ti consigliamo di automatizzare il processo di aggiornamento di SSM Agent sulle macchine. Per informazioni, consulta [Automatizzazione degli aggiornamenti a Agente SSM](#). Iscriviti alla pagina [Note di rilascio di SSM Agent](#) su GitHub per ricevere notifiche sugli aggiornamenti di SSM Agent.

## Argomenti

- [Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per macOS](#)

## Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per macOS

Connettersi all'istanza macOS e procedere nel seguente modo per installare AWS Systems Manager Agent (SSM Agent). Seguire queste fasi su ogni istanza che esegue comandi tramite Systems Manager. I comandi forniti in questa procedura possono anche essere passati alle istanze Amazon EC2 come script tramite i dati utente.

### Important

Si consiglia vivamente di evitare l'uso di versioni del sistema operativo che hanno raggiunto End-of-Life (EOL). I fornitori di sistemi operativi, tra cui AWS in genere, non forniscono patch di sicurezza o altri aggiornamenti per le versioni che hanno raggiunto l'EOL. Continuare a utilizzare un sistema EOL aumenta notevolmente il rischio di non essere in grado di applicare gli aggiornamenti, comprese le correzioni di sicurezza e altri problemi operativi. AWS non verifica la funzionalità di Systems Manager su versioni del sistema operativo che hanno raggiunto la fine del ciclo di vita.

## Prima di iniziare

Installa `wget` utilizzando Homebrew.

Per installare SSM Agent su macOS

1. Scarica il file del programma di installazione dell'agente per istanze `x86_64` utilizzando il seguente comando.

Nel comando seguente, sostituiscilo `region` con le tue informazioni. Per un elenco dei `region` valori supportati, vedere la colonna Regione negli [endpoint del servizio Systems Manager](#) in.

Riferimenti generali di Amazon Web Services

```
sudo wget https://s3.region.amazonaws.com/amazon-ssm-region/latest/darwin_amd64/
amazon-ssm-agent.pkg
```

Utilizza seguente il comando per le istanze Apple silicon.

```
sudo wget https://s3.region.amazonaws.com/amazon-ssm-region/latest/darwin_arm64/
amazon-ssm-agent.pkg
```

Ecco un esempio.

```
sudo wget https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
darwin_amd64/amazon-ssm-agent.pkg
```

2. Utilizzare il seguente comando per eseguire il programma di installazione di SSM Agent.

`x86_64`:

```
sudo installer -pkg amazon-ssm-agent.pkg -target /
```

3. Controllare lo stato dell'agente.

Per determinare se SSM Agent è in esecuzione, controllare il log dell'agente all'indirizzo `/var/log/amazon/ssm/amazon-ssm-agent.log`.

4. Eseguire il comando seguente per avviare il servizio se il log dell'agente indica che "amazon-ssm-agent è stato arrestato".

```
sudo launchctl load -w /Library/LaunchDaemons/com.amazon.aws.ssm.plist && sudo
launchctl start com.amazon.aws.ssm
```

### Important

Una versione aggiornata di SSM Agent viene distribuita ogni volta che vengono aggiunti nuovi strumenti a Systems Manager o eseguiti aggiornamenti degli strumenti esistenti. Il mancato utilizzo della versione più recente dell'agente può impedire al nodo gestito di utilizzare vari strumenti e funzionalità di Systems Manager. Per questo motivo, ti consigliamo di automatizzare il processo di aggiornamento di SSM Agent sulle macchine. Per informazioni, consulta [Automatizzazione degli aggiornamenti a Agente SSM](#). Iscriviti alla pagina [Note di rilascio di SSM Agent](#) su GitHub per ricevere notifiche sugli aggiornamenti di SSM Agent.

## Disinstallazione Agente SSM from macOS Istanze

macOS non supporta in modo nativo la disinstallazione di file PKG. Per disinstallarlo SSM Agent da un'istanza Amazon EC2 per macOS, utilizza lo script AWS gestito dalla seguente posizione.

<https://github.com/aws/amazon-ssm-agent/blob/mainline/Tools/src/update/darwin/uninstall.sh>

## Lavorare con Agente SSM su istanze EC2 per Windows Server

AWS Systems Manager Agent (SSM Agent) è preinstallato, per impostazione predefinita, sul Amazon Machine Images modulo (AMIs) Windows Server fornito da AWS. Il supporto è fornito per le seguenti versioni del sistema operativo (OS).

- Windows Server 2012 R2 AMIs pubblicate a novembre 2016 o successivamente
- Windows Server 2016, 2019, 2022 (escluse le versioni Nano) e 2025

### Note di supporto per le versioni precedenti

Le AMIs (AMI) Windows Server pubblicate prima di novembre 2016 utilizzano il servizio EC2Config per l'elaborazione delle richieste e la configurazione delle istanze.

A meno che tu non abbia un motivo specifico per utilizzare il servizio EC2Config o una versione precedente per SSM Agent elaborare le richieste di Systems Manager, ti consigliamo di scaricare e



installare la versione più recente su ciascuna delle SSM Agent tue istanze Amazon Elastic Compute Cloud (Amazon EC2) o su macchine non EC2 configurate per Systems Manager in un ambiente ibrido e multicloud. [???](#)

## Mantenere Agente SSM aggiornamento

Una versione aggiornata di SSM Agent viene distribuita ogni volta che vengono aggiunti nuovi strumenti a Systems Manager o eseguiti aggiornamenti degli strumenti esistenti. Il mancato utilizzo della versione più recente dell'agente può impedire al nodo gestito di utilizzare vari strumenti e funzionalità di Systems Manager. Per questo motivo, ti consigliamo di automatizzare il processo di aggiornamento di SSM Agent sulle macchine. Per informazioni, consulta [Automatizzazione degli aggiornamenti a Agente SSM](#). Iscriviti alla pagina [Note di rilascio di SSM Agent](#) su GitHub per ricevere notifiche sugli aggiornamenti di SSM Agent.

Per visualizzare i dettagli sulle diverse versioni di SSM Agent, consultare le [note di rilascio](#).

## Argomenti

- [Installazione e disinstallazione manuali Agente SSM su istanze EC2 per Windows Server](#)
- [Configurazione di SSM Agent per utilizzare un proxy per le istanze Windows Server](#)

## Installazione e disinstallazione manuali Agente SSM su istanze EC2 per Windows Server

AWS Systems Manager Agent (SSM Agent) è preinstallato, per impostazione predefinita, su quanto segue Amazon Machine Images (AMIs) Windows Server fornito da Amazon:

- Windows Server 2012 R2 AMIs pubblicate a novembre 2016 o successivamente
- Windows Server 2016, 2019, 2022 (escluse le versioni Nano) e 2025

### Important

Ti consigliamo vivamente di evitare di utilizzare versioni del sistema operativo che hanno raggiunto End-of-Life (EOL). I fornitori di sistemi operativi, tra cui AWS in genere, non forniscono patch di sicurezza o altri aggiornamenti per le versioni che hanno raggiunto il termine di scadenza. Continuare a utilizzare un sistema EOL aumenta notevolmente il rischio di non poter applicare gli aggiornamenti, comprese le correzioni di sicurezza, e altri problemi

operativi. AWS non verifica la funzionalità di Systems Manager sulle versioni del sistema operativo che hanno raggiunto il termine di scadenza.

## Installa Agente SSM sulle istanze EC2 per Windows Server

Se necessario, è possibile scaricare e installare manualmente la versione più recente di SSM Agent sull'istanza Amazon Elastic Compute Cloud (Amazon EC2) per Windows Server utilizzando la seguente procedura. I comandi forniti in questa procedura possono anche essere passati alle istanze Amazon EC2 come script tramite i dati utente.

SSM Agent richiede Windows PowerShell 3.0 o versioni successive per eseguire determinati AWS Systems Manager documenti (documenti SSM) sulle Windows Server istanze (ad esempio, il documento precedente). AWS-ApplyPatchBaseline Verifica che le istanze Windows Server eseguano Windows Management Framework 3.0 o versioni successive. Questo framework include Windows. PowerShell Per ulteriori informazioni, consulta [Windows Management Framework 3.0](#).

### Installazione su altri tipi di macchine

Questa procedura descritta in questo argomento è valida specificamente per l'installazione o la reinstallazione dell'SSM Agent su un'istanza EC2 per Windows Server. Per server on-premises, macchine virtuali o altri ambienti non EC2, utilizza lo strumento `ssm-setup-cli` come descritto in [the section called “Installa Agente SSM su ibrido Windows Server nodi”](#). L'utilizzo delle procedure di installazione di EC2 su sistemi non EC2 può potenzialmente causare vulnerabilità di sicurezza. Lo strumento `ssm-setup-cli` fornisce protezioni di sicurezza aggiuntive per macchine non EC2.

Per installare manualmente la versione più recente di Agente SSM su istanze EC2 per Windows Server

1. Connettiti alla tua istanza utilizzando Remote Desktop o Windows. PowerShell Per ulteriori informazioni, consulta [Connessione all'istanza](#) nella Guida per l'utente di Amazon EC2.
2. Scaricare l'ultima versione di SSM Agent sull'istanza. Puoi eseguire il download utilizzando PowerShell i comandi o un link per il download diretto.

 Note

Gli URL in questo passaggio ti consentono di effettuare il download SSM Agent da qualsiasi Regione AWS sito. Se desideri scaricare l'agente da una regione specifica, utilizza invece un Region-specific URL:

```
https://amazon-ssm-region.s3.region.amazonaws.com/latest/
windows_amd64/AmazonSSMAgentSetup.exe
```

*region* rappresenta l'identificatore di una regione Regione AWS supportata da AWS Systems Manager, ad esempio us-east-2 per la regione Stati Uniti orientali (Ohio). Per un elenco dei *region* valori supportati, vedere la colonna Regione negli endpoint [del servizio](#) Systems Manager in. Riferimenti generali di Amazon Web Services

## PowerShell

Esegui i tre PowerShell comandi seguenti in ordine. Questi comandi consentono di scaricare SSM Agent senza modificare le impostazioni di protezione avanzata di Internet Explorer (IE), quindi installare l'agente e rimuovere il file di installazione.

## 64-bit

```
[System.Net.ServicePointManager]::SecurityProtocol = 'TLS12'
$progressPreference = 'silentlyContinue'
Invoke-WebRequest `
 https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/
windows_amd64/AmazonSSMAgentSetup.exe `
 -OutFile $env:USERPROFILE\Desktop\SSMAgent_latest.exe
```

## 32-bit

```
[System.Net.ServicePointManager]::SecurityProtocol = 'TLS12'
$progressPreference = 'silentlyContinue'
Invoke-WebRequest `
 https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/
windows_386/AmazonSSMAgentSetup.exe `
 -OutFile $env:USERPROFILE\Desktop\SSMAgent_latest.exe
```

```
Start-Process `
 -FilePath $env:USERPROFILE\Desktop\SSMAgent_latest.exe `
```

```
-ArgumentList "/S" `
-Wait
```

```
rm -Force $env:USERPROFILE\Desktop\SSMAgent_latest.exe
```

### Download diretto

Scaricare la versione più recente dell'istanza SSM Agent utilizzando il seguente link. Se lo desideri, aggiorna questo URL con un URL Regione AWS specifico.

[https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/windows\\_amd64/AmazonSSMAgentSetup.exe](https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/windows_amd64/AmazonSSMAgentSetup.exe)

Esegui il file AmazonSSMAgentSetup.exe scaricato per installare SSM Agent.

3. Avvia o riavvia SSM Agent inviando il seguente comando in PowerShell:

```
Restart-Service AmazonSSMAgent
```

#### Note

Per disinstallare SSM Agent da un'istanza di Windows Server, apri Pannello di controllo, quindi Programmi. Scegli l'opzione Disinstalla un programma. Apri il menu contestuale di Amazon SSM Agent e scegli Disinstalla.

## Configurazione di SSM Agent per utilizzare un proxy per le istanze Windows Server

Le informazioni incluse in questo argomento valgono per le istanze di Windows Server create a partire da novembre 2016 che non utilizzano l'opzione di installazione Nano. Se intendi utilizzare Session Manager, ricorda che i server proxy HTTPS non sono supportati.

### Prima di iniziare

Prima di configurare SSM Agent per l'utilizzo di un proxy, considera quanto segue.

Nella procedura seguente, si esegue un comando per configurare SSM Agent per l'utilizzo di un proxy. Il comando include un'impostazione `no_proxy` con un indirizzo IP. L'indirizzo IP è l'endpoint

dei servizi di metadati di istanza (IMDS) per Systems Manager. Se non viene specificato `no_proxy`, le chiamate a Systems Manager acquisiscono l'identità dal servizio proxy (se il fallback IMDSv1 è abilitato) oppure le chiamate a Systems Manager hanno esito negativo (se è applicato IMDSv2).

- Per IPv4, specifica `no_proxy=169.254.169.254`.
- Per IPv6, specifica `no_proxy=[fd00:ec2::254]`. L'indirizzo IPv6 del servizio metadati dell'istanza è compatibile con i comandi IMDSv2. L'indirizzo IPv6 è accessibile solo su istanze costruite sul [sistema Nitro AWS](#). Per ulteriori informazioni, consulta [Come funziona il servizio di metadati di istanza versione 2](#) nella Guida per l'utente di Amazon EC2.

Per configurare l'SSM Agent per l'utilizzo di un proxy

1. Utilizzando Remote Desktop o Windows PowerShell, connettiti all'istanza che desideri configurare per utilizzare un proxy.
2. Esegui il seguente blocco di comandi in PowerShell. Sostituisci *hostname* e *port* con le informazioni sul tuo proxy.

```
$serviceKey = "HKLM:\SYSTEM\CurrentControlSet\Services\AmazonSSMAgent"
$keyInfo = (Get-Item -Path $serviceKey).GetValue("Environment")
$proxyVariables = @"http_proxy=hostname:port", "https_proxy=hostname:port",
 "no_proxy=IP address for instance metadata services (IMDS)"

if ($keyInfo -eq $null) {
 New-ItemProperty -Path $serviceKey -Name Environment -Value $proxyVariables -
 PropertyType MultiString -Force
} else {
 Set-ItemProperty -Path $serviceKey -Name Environment -Value $proxyVariables
}

Restart-Service AmazonSSMAgent
```

Dopo aver eseguito il comando precedente, è possibile esaminare i registri SSM Agent per confermare che le impostazioni proxy siano state applicate. Le voci nei registri sono simili alle seguenti. Per ulteriori informazioni sui log SSM Agent, consulta [Visualizzazione Agente SSM log](#).

```
2020-02-24 15:31:54 INFO Getting IE proxy configuration for current user: The operation
completed successfully.
```

```
2020-02-24 15:31:54 INFO Getting WinHTTP proxy default configuration: The operation
completed successfully.
2020-02-24 15:31:54 INFO Proxy environment variables:
2020-02-24 15:31:54 INFO http_proxy: hostname:port
2020-02-24 15:31:54 INFO https_proxy: hostname:port
2020-02-24 15:31:54 INFO no_proxy: IP address for instance metadata services (IMDS)
2020-02-24 15:31:54 INFO Starting Agent: amazon-ssm-agent - v2.3.871.0
2020-02-24 15:31:54 INFO OS: windows, Arch: amd64
```

Per reimpostare la configurazione proxy dell'SSM Agent

1. Utilizzando Remote Desktop o Windows PowerShell, connettiti all'istanza da configurare.
2. Se ti sei connesso tramite Remote Desktop, avvia PowerShell come amministratore.
3. Esegui il seguente blocco di comandi in PowerShell.

```
Remove-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\AmazonSSMAgent -
Name Environment
Restart-Service AmazonSSMAgent
```

## Precedenza impostazione proxy SSM Agent

Quando si configurano le impostazioni proxy per le istanze SSM Agent su Windows Server, è importante capire che queste impostazioni vengono valutate e applicate alla configurazione dell'agente quando SSM Agent viene avviato. La modalità di configurazione delle impostazioni proxy per un'istanza Windows Server consente di determinare se altre impostazioni potrebbero sostituire quelle desiderate. L'agente utilizza le prime impostazioni proxy che trova.

### Important

SSM Agent comunica utilizzando il protocollo HTTPS. Per questo motivo, è necessario configurare il parametro `HTTPS proxy` utilizzando una delle seguenti opzioni di impostazione.

Le impostazioni proxy di SSM Agent sono valutate nel seguente ordine.

1. Impostazioni del registro AmazonSSMAgent (HKLM:\SYSTEM\CurrentControlSet\Services\AmazonSSMAgent)

2. Variabili di ambiente System (http\_proxy, https\_proxy, no\_proxy)
3. Variabili di ambiente dell'account utente LocalSystem (http\_proxy, https\_proxy, no\_proxy)
4. Impostazioni del browser (HTTP, secure, exceptions)
5. Impostazioni del proxy WinHTTP (http=, https=, bypass-list=)

## Impostazioni del proxy di SSM Agent e servizi di Systems Manager

Se lo hai configurato SSM Agent per utilizzare un proxy e utilizzi AWS Systems Manager strumenti come Run Command and Patch Manager che utilizzano PowerShell il client Windows Update durante la loro esecuzione sulle Windows Server istanze, configura impostazioni proxy aggiuntive. In caso contrario, l'operazione potrebbe non riuscire perché le impostazioni proxy utilizzate dal PowerShell client Windows Update non vengono ereditate dalla configurazione del SSM Agent proxy.

Per Run Command, configurare le impostazioni del proxy WinINet sulle istanze di Windows Server. I comandi [System.Net.WebRequest]::DefaultWebProxy forniti sono per sessione. Per applicare queste configurazioni ai comandi di rete successivi eseguiti in Run Command, questi comandi devono precedere gli altri PowerShell comandi nello stesso aws:runPowershellScript input del plug-in.

I seguenti PowerShell comandi restituiscono le impostazioni WinINet proxy correnti e applicano le impostazioni proxy a WinINet

```
[System.Net.WebRequest]::DefaultWebProxy

$proxyServer = "http://hostname:port"
$proxyBypass = "169.254.169.254"
$WebProxy = New-Object System.Net.WebProxy($proxyServer,$true,$proxyBypass)

[System.Net.WebRequest]::DefaultWebProxy = $WebProxy
```

Per Patch Manager, configurare le impostazioni proxy a livello di sistema in modo che il client Windows Update possa eseguire la scansione e il download degli aggiornamenti. Si consiglia di utilizzare Run Command per eseguire i comandi seguenti perché questi vengono eseguiti sull'account SYSTEM e le impostazioni si applicano a livello di sistema. I seguenti comandi netsh restituiscono le impostazioni del proxy corrente e applicano le impostazioni del proxy al sistema locale.

```
netsh winhttp show proxy
```

```
netsh winhttp set proxy proxy-server="hostname:port" bypass-list="169.254.169.254"
```

Per ulteriori informazioni sull'utilizzo di Run Command, consultare [AWS Systems Manager Run Command](#).

## Verifica Agente SSM stato e avvio dell'agente

Questo argomento elenca i comandi per verificare se AWS Systems Manager Agent (SSM Agent) è in esecuzione su ogni sistema operativo supportato. L'argomento fornisce inoltre i comandi per avviare l'agente se non è in esecuzione.

### Note

Questi comandi richiedono che SSM Agent sia già installato nel nodo gestito. È necessario disporre dei privilegi di amministratore su Windows o root/sudo accedere su Linux e macOS per eseguire questi comandi.

| Sistema operativo                  | Comando per controllare lo stato di SSM Agent                                                              | Comando per l'avvio di SSM Agent                                                                              |
|------------------------------------|------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Amazon Linux 2 e Amazon Linux 2023 | <code>sudo systemctl status amazon-ssm-agent</code>                                                        | <code>sudo systemctl enable amazon-ssm-agent</code><br><br><code>sudo systemctl start amazon-ssm-agent</code> |
| Debian Server 11 e 12              | <code>sudo systemctl status amazon-ssm-agent</code>                                                        | <code>sudo systemctl enable amazon-ssm-agent</code><br><br><code>sudo systemctl start amazon-ssm-agent</code> |
| macOS                              | Controllare il file di log dell'agente all'indirizzo <code>/var/log/amazon/ssm/amazon-ssm-agent.log</code> | <code>sudo launchctl load -w /Library/LaunchDaemons/com.amazon.aws.ssm.plist</code>                           |



| Sistema operativo                                                     | Comando per controllare lo stato di SSM Agent                                     | Comando per l'avvio di SSM Agent                                                                              |
|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
|                                                                       |                                                                                   | <code>sudo launchctl start com.amazon.aws.ssm</code>                                                          |
| Oracle Linux                                                          | <code>sudo systemctl status amazon-ssm-agent</code>                               | <code>sudo systemctl enable amazon-ssm-agent</code><br><br><code>sudo systemctl start amazon-ssm-agent</code> |
| Red Hat Enterprise Linux (RHEL) 7.x, 8.x, 9.x e 10.x                  | <code>sudo systemctl status amazon-ssm-agent</code>                               | <code>sudo systemctl enable amazon-ssm-agent</code><br><br><code>sudo systemctl start amazon-ssm-agent</code> |
| SUSE Linux Enterprise Server (SLES)                                   | <code>sudo systemctl status amazon-ssm-agent</code>                               | <code>sudo systemctl enable amazon-ssm-agent</code><br><br><code>sudo systemctl start amazon-ssm-agent</code> |
| Ubuntu Server 18.04, 20.04, 22.04 LTS, 23.10, 24.04 LTS, 24.0 e 25.04 | <code>sudo systemctl status snap.amazon-ssm-agent.amazon-ssm-agent.service</code> | <code>sudo snap start amazon-ssm-agent</code>                                                                 |
| Windows Server                                                        | Esegui in: PowerShell<br><br><code>Get-Service AmazonSSMAgent</code>              | Esegui in modalità PowerShell amministratore:<br><br><code>Start-Service AmazonSSMAgent</code>                |

#### Ulteriori informazioni

- [Utilizzo di SSM Agent sulle istanze EC2 per Linux](#)
- [Lavorare con Agente SSM su istanze EC2 per Windows Server](#)

- [Verifica del Agente SSM numero di versione](#)

## Verifica del Agente SSM numero di versione

Alcune AWS Systems Manager funzionalità hanno dei prerequisiti che includono l'installazione di una versione minima di Systems Manager Agent (SSM Agent) sui nodi gestiti. È possibile ottenere la versione di SSM Agent attualmente installata nei nodi gestiti utilizzando la console di Systems Manager o accedendo ai nodi.

### Note

Per visualizzare i dettagli sulle versioni precedenti, consulta le note di [SSM Agent rilascio su GitHub](#)

Nelle procedure seguenti viene descritto come ottenere la versione di SSM Agent attualmente installata nei nodi gestiti.

Per verificare il numero di versione di Agente SSM installato su un nodo gestito

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Nella colonna SSM Agent version (Versione di ), prendi nota del numero di Agent version (Versione dell'agente).

Per ottenere la versione attualmente installata Agente SSM versione dall'interno del sistema operativo

Per ottenere la versione di SSM Agent attualmente installata dal sistema operativo, scegliere tra le schede seguenti.

## Amazon Linux 2 and Amazon Linux 2023

### Note

Questo comando varia a seconda del programma di gestione dei pacchetti per il sistema operativo in uso.

1. Accedi al tuo nodo gestito.
2. Eseguire il seguente comando seguente.

```
yum info amazon-ssm-agent
```

Questo comando restituisce un output simile al seguente.

```
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Installed Packages
Name : amazon-ssm-agent
Arch : x86_64
Version : 3.0.655.0
```

## Debian Server

1. Accedi al tuo nodo gestito.
2. Eseguire il seguente comando seguente.

```
apt list amazon-ssm-agent
```

Questo comando restituisce un output simile al seguente.

```
apt list amazon-ssm-agent
Listing... Done
amazon-ssm-agent/now 3.0.655.0-1 amd64 [installed,local]

3.0.655.0 is the version of SSM agent
```

## macOS

1. Accedi al tuo nodo gestito.
2. Esegui il seguente comando seguente.

```
pkgutil --pkg-info com.amazon.aws.ssm
```

## RHEL

1. Accedi al tuo nodo gestito.
2. Esegui il comando seguente per RHEL 7, 8, 9 e 10.

```
yum info amazon-ssm-agent
```

Questo comando restituisce un output simile al seguente.

```
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Installed Packages
Name : amazon-ssm-agent
Arch : x86_64
Version : 3.0.655.0
```

Esegui il comando seguente per l'utilità del pacchetto DNF.

```
dnf info amazon-ssm-agent
```

## SLES

1. Accedi al tuo nodo gestito.
2. Esegui il comando seguente per SLES 15.x.

```
zypper info amazon-ssm-agent
```

Questo comando restituisce un output simile al seguente.

```
Loading repository data...
Reading installed packages...
```

```
Information for package amazon-ssm-agent:

Repository : @System
Name : amazon-ssm-agent
Version : 3.0.655.0-1
```

## Ubuntu Server

1. Accedi al tuo nodo gestito.
2. Esegui il comando seguente per Ubuntu Server 18.04, 20.04, 22.04 LTS, 23.10, 24.04 LTS, 24.0 e 25.04.

```
sudo snap list amazon-ssm-agent
```

Questo comando restituisce un output simile al seguente.

```
snap list amazon-ssm-agent
Name Version Rev Tracking Publisher Notes
amazon-ssm-agent 3.0.529.0 3552 latest/stable/... aws# classic-

3.0.529.0 is the version of SSM agent
```

## Windows

1. Accedi al tuo nodo gestito.
2. Esegui il PowerShell comando seguente.

```
& "C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe" -version
```

Questo comando restituisce un output simile al seguente.

```
SSM Agent version: 3.1.804.0
```

Si consiglia di utilizzare l'ultima versione di SSM Agent in modo da poter beneficiare delle funzionalità nuove o aggiornate. Per assicurarti che le tue istanze gestite eseguano sempre la versione più

aggiornata di SSM Agent, puoi automatizzare il processo di aggiornamento di SSM Agent. Per ulteriori informazioni, consulta [Automatizzazione degli aggiornamenti a Agente SSM](#).

## Visualizzazione Agente SSM log

AWS Systems Manager Agent (SSM Agent) scrive informazioni su esecuzioni, comandi, azioni pianificate, errori e stati di integrità nei file di registro su ciascun nodo gestito. Puoi visualizzare i file di log connettendoti manualmente a un nodo gestito oppure puoi inviare automaticamente i log ad Amazon CloudWatch Logs. Per ulteriori informazioni sull'invio dei CloudWatch log a Logs, consulta [Registrazione e monitoraggio AWS Systems Manager](#).

È possibile visualizzare i log di SSM Agent sui nodi gestiti nelle seguenti posizioni.

Linux and macOS

```
/var/log/amazon/ssm/
```

Windows

```
%PROGRAMDATA%\Amazon\SSM\Logs\
```

Per i nodi gestiti Linux, i file di SSM Agent `stderr` e `stdout` vengono scritti nella seguente directory: `/var/lib/amazon/ssm/`.

Per i nodi gestiti Windows, i file `stderr` e `stdout` di SSM Agent vengono scritti nella seguente directory: `%PROGRAMDATA%\Amazon\SSM\InstanceData\`.

Per informazioni su come abilitare la registrazione di debug di SSM Agent, consulta [Consentire Agente SSM registrazione di debug](#).

Per ulteriori informazioni sulla configurazione `cihub/seeelog`, consulta [Seeelog Wiki](#) su GitHub. Per esempi di `cihub/seeelog` configurazioni, consulta il [repository](#) `cihub/seeelog` degli esempi su GitHub.

## Consentire Agente SSM registrazione di debug

La procedura seguente permette di abilitare la registrazione di debug di SSM Agent nei nodi gestiti.

## Linux and macOS

Consentire Agente SSM registrazione di debug su Linux e macOS nodi gestiti

1. Utilizzali Session Manager per connetterti al nodo gestito in cui desideri consentire la registrazione di debug oppure accedi al nodo gestito. Per ulteriori informazioni, consulta [Utilizzo di Session Manager](#).
2. Individua il file `seelog.xml.template`.

Linux:

Sulla maggior parte dei tipi di nodo gestito Linux, il file si trova nella directory `/etc/amazon/ssm/seelog.xml.template`.

Nelle versioni Ubuntu Server 20.04 e 18.04 LTS, il file si trova nella directory `/snap/amazon-ssm-agent/current/seelog.xml.template`. Copiare questo file dalla directory `/snap/amazon-ssm-agent/current/` alla directory `/etc/amazon/ssm/` prima di apportare qualsiasi modifica.

macOS:

Sui tipi di istanza macOS, il file si trova nella directory `/opt/aws/ssm/seelog.xml.template`.

3. Modificare il nome del file da `seelog.xml.template` a `seelog.xml`.

### Note

Su Ubuntu Server 20.04 e 18.04 LTS, il file `seelog.xml` deve essere creato nella directory `/etc/amazon/ssm/`. È possibile creare questa directory e il file eseguendo i seguenti comandi.

```
sudo mkdir -p /etc/amazon/ssm
```

```
sudo cp -p /snap/amazon-ssm-agent/current/seelog.xml.template /etc/amazon/ssm/seelog.xml
```

4. Modifica il file `seelog.xml` per cambiare il comportamento di registrazione predefinito. Cambiare il valore `minlevel` da `info` a `debug`, come mostrato nell'esempio seguente.

```
<seelog type="adaptive" mininterval="2000000" maxinterval="100000000"
critmsgcount="500" minlevel="debug">
```

5. (Facoltativo) Riavviare SSM Agent utilizzando il seguente comando.

Linux:

```
sudo service amazon-ssm-agent restart
```

macOS:

```
sudo /opt/aws/ssm/bin/amazon-ssm-agent restart
```

## Windows

Consentire Agente SSM effettuare il debug durante l'accesso Windows Server nodi gestiti

1. Utilizzare Session Manager per connettersi al nodo gestito in cui abilitare la registrazione di debug oppure accedere ai nodi gestiti. Per ulteriori informazioni, consulta [Utilizzo di Session Manager](#).
2. Crea una copia del file `seelog.xml.template`. Cambia il nome della copia in `seelog.xml`. Il file si trova nella directory seguente:

```
%PROGRAMFILES%\Amazon\SSM\seelog.xml.template
```

3. Modifica il file `seelog.xml` per cambiare il comportamento di registrazione predefinito. Cambiare il valore `minlevel` da `info` a `debug`, come mostrato nell'esempio seguente.

```
<seelog type="adaptive" mininterval="2000000" maxinterval="100000000"
critmsgcount="500" minlevel="debug">
```

4. Individuare la voce seguente:

```
filename="{{LOCALAPPDATA}}\Amazon\SSM\Logs\{{EXECUTABLENAME}}.log"
```

Modificare questa voce in modo che utilizzi il percorso seguente:

```
filename="C:\ProgramData\Amazon\SSM\Logs\{{EXECUTABLENAME}}.log"
```

5. Individuare la voce seguente:



```
filename="{{LOCALAPPDATA}}\Amazon\SSM\Logs\errors.log"
```

Modificare questa voce in modo che utilizzi il percorso seguente:

```
filename="C:\ProgramData\Amazon\SSM\Logs\errors.log"
```

6. Riavviare SSM Agent utilizzando il seguente PowerShell comando in modalità amministratore.

```
Restart-Service AmazonSSMAgent
```

## Limitare l'accesso ai comandi a livello di root tramite SSM Agent

AWS Systems Manager Agent (SSM Agent) viene eseguito su istanze Amazon Elastic Compute Cloud (Amazon EC2) e altri tipi di macchine [in ambienti ibridi e multicloud](#) utilizzando le autorizzazioni root (Linux) o le autorizzazioni SYSTEM (). Windows Server Poiché questi sono il massimo livello di privilegi di accesso al sistema, qualunque entità attendibile autorizzata a inviare comandi a SSM Agent dispone di autorizzazioni root o SYSTEM. (Nel AWS, un'entità attendibile che può eseguire azioni e accedere alle risorse in è chiamata principale. AWS Un principale può essere un Utente root dell'account AWS utente o un ruolo.)

Tale livello di accesso è necessario affinché un principale invii comandi di Systems Manager autorizzati a SSM Agent, ma fa anche sì che un principale esegua un codice malware sfruttando potenziali vulnerabilità in SSM Agent.

In particolare, le autorizzazioni per eseguire i comandi [SendCommand](#) e [StartSession](#) dovrebbero essere attentamente limitate. Un buon punto di partenza è quello di concedere le autorizzazioni per ciascun comando solo a determinate principali nella tua organizzazione. Tuttavia, ti consigliamo di rafforzare ulteriormente la posizione di sicurezza limitando i nodi gestiti su cui una principale può eseguire questi comandi. Questa operazione può essere eseguita nella policy IAM assegnata al principale. Nella policy IAM, puoi includere una condizione che limiti l'utente nell'eseguire comandi solo sui nodi gestiti contrassegnati da tag o da una combinazione di tag specifici.

Supponiamo ad esempio di disporre di due parchi istanze di server, uno per i test e l'altro per la produzione. Nella policy IAM applicata ai tecnici junior, va specificato che possono eseguire comandi solo sulle istanze contrassegnate con `ssm:resourceTag/testServer`. Ma per un gruppo più ridotto di tecnici di livello superiore, che devono accedere a tutte le istanze, va autorizzato l'accesso

alle istanze contrassegnate con `ssm:resourceTag/testServer` e con `ssm:resourceTag/productionServer`.

Seguendo questo approccio, se i tecnici junior tentano di eseguire un comando su un'istanza di produzione, l'accesso verrà rifiutato perché la policy IAM a loro assegnata non fornisce un accesso esplicito alle istanze contrassegnate dal tag `ssm:resourceTag/productionServer`.

Per maggiori informazioni ed esempi, consultare i seguenti argomenti:

- [Limitazione Run Command accesso basato su tag](#)
- [Limitazione dell'accesso alla sessione in base ai tag dell'istanza](#)

## Automatizzazione degli aggiornamenti a Agente SSM

AWS rilascia una nuova versione di AWS Systems Manager Agent (SSM Agent) quando aggiungiamo o aggiorniamo gli strumenti di Systems Manager. Se i nodi gestiti utilizzano una versione precedente dell'agente, non è possibile utilizzare i nuovi strumenti o beneficiare di quelli aggiornati. Per questi motivi, si consiglia di automatizzare il processo di aggiornamento SSM Agent nei nodi gestiti utilizzando uno dei metodi descritti di seguito.

Aggiornare gli agenti sul sistema operativo Bottlerocket

SSM Agent sul sistema operativo Bottlerocket non può essere aggiornato utilizzando il documento `AWS-UpdateSSMAgent` di Systems Manager Command. Gli aggiornamenti vengono gestiti all'interno del container di controllo Bottlerocket. Per ulteriori informazioni, consulta [Container di controllo Bottlerocket](#) e [Operatore di aggiornamento Bottlerocket](#) su GitHub.

macOS requisito della versione

Se un'istanza esegue macOS versione 11.0 (Big Sur) o successiva, per eseguire il documento `AWS-UpdateSSMAgent`, l'istanza deve avere SSM Agent versione 3.1.941.0 o successiva. Se l'istanza esegue una versione di SSM Agent precedente alla 3.1.941.0, aggiorna il tuo SSM Agent per eseguire `AWS-UpdateSSMAgent` eseguendo i comandi `brew update` e `brew upgrade amazon-ssm-agent`.

| Metodo                                                         | Informazioni                                                                                 |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Aggiornamento automatico su tutti i nodi gestiti (consigliato) | Puoi configurare tutti i nodi gestiti del tuo Account AWS sistema per verificare e scaricare |

| Metodo                            | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                   | <p>automaticamente nuove versioni diSSM Agent. A tale scopo, scegli Aggiorna automaticamente SSM Agent nella scheda Impostazioni di Fleet Manager, come descritto più avanti in questo argomento.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Aggiornamento globale o selettivo | <p>È possibile State Manager utilizzarlo per creare un'associazione che viene scaricata e installata automaticamente SSM Agent sui nodi gestiti. Se si desidera limitare l'interruzione ai carichi di lavoro, è possibile creare una finestra di manutenzione di Systems Manager per eseguire l'installazione durante i periodi di tempo designati. Entrambi i metodi permettono di creare una configurazione di aggiornamento globale per tutti i nodi gestiti o scegliere selettivamente quali istanze devono essere aggiornate. Per informazioni sulla creazione di un'associazione State Manager, consultare e <a href="#">Procedura dettagliata: aggiorna SSM Agent automaticamente con AWS CLI</a>. Per ulteriori informazioni sulla creazione di una finestra di manutenzione, consulta <a href="#">Tutorial: creazione di una finestra di manutenzione per l'applicazione di patch tramite console</a>.</p> |

| Metodo                                               | Informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Aggiornamento globale o selettivo per nuovi ambienti | Se stai iniziando a usare Systems Manager, ti consigliamo di utilizzare l'opzione Update Systems Manager (SSM) Agent ogni due settimane in. Quick Setup ConQuick Setup, è possibile creare una configurazione di aggiornamento globale per tutti i nodi gestiti o scegliere selettivamente quali nodi gestiti vengono aggiornati. Per ulteriori informazioni, consulta <a href="#">Configura la gestione degli host di Amazon EC2 utilizzando Configurazione rapida</a> . |

Se preferisci eseguire l'aggiornamento manuale SSM Agent sui nodi gestiti, puoi abbonarti alle notifiche che vengono AWS pubblicate quando viene rilasciata una nuova versione dell'agente. Per informazioni, consulta [Abbonarsi a Agente SSM notifiche](#). Dopo aver sottoscritto le notifiche, è possibile utilizzare Run Command per aggiornare manualmente uno o più nodi gestiti con la versione più recente. Per ulteriori informazioni, consulta [Aggiornamento di SSM Agent utilizzando Run Command](#).

## Aggiornamento automatico Agente SSM

È possibile configurare Systems Manager in modo che si aggiorni automaticamente SSM Agent su tutti Linux-based i nodi Windows-based gestiti del sistema Account AWS. Se si abilita questa opzione, Systems Manager verifica automaticamente ogni due settimane la presenza di una nuova versione dell'agente. Se è presente una nuova versione, Systems Manager aggiorna automaticamente l'agente alla versione più recente rilasciata utilizzando il documento SSM AWS-UpdateSSMAgent. Ti invitiamo a scegliere questa opzione per assicurarti che i tuoi nodi gestiti eseguano sempre la versione più aggiornata di SSM Agent.

### Note

Se si utilizza un comando yum per aggiornare SSM Agent su un nodo gestito dopo che l'agente è stato installato o aggiornato utilizzando il documento SSM AWS-UpdateSSMAgent, è possibile che venga visualizzato il seguente messaggio: "Warning:

RPMDDB altered outside of yum." Questo messaggio è previsto e può essere ignorato in modo sicuro.

Per aggiornare automaticamente Agente SSM

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Fleet Manager.
3. Seleziona la scheda Impostazioni.
4. Nell'area Aggiornamento automatico dell'agente, scegli Aggiorna automaticamente SSM Agent.

Per modificare la versione di SSM Agent a cui il parco istanze si aggiorna, scegli Edit (Modifica) in Agent auto update (Aggiornamento automatico dell'agente) nella scheda Settings (Impostazioni). Quindi inserire il numero di versione di SSM Agent a cui si desidera eseguire l'aggiornamento in Version (Versione) sotto Parameters (Parametri). Se non è specificata, l'agente verrà aggiornato alla versione più recente.

Per interrompere l'implementazione automatica delle versioni aggiornate di SSM Agent su tutti i nodi gestiti nell'account, scegli Delete (Elimina) in Agent auto update (Aggiornamento automatico dell'agente) nella scheda Settings (Impostazioni). Questa azione elimina l'associazione State Manager che aggiorna automaticamente SSM Agent sui nodi gestiti.

## Abbonarsi a Agente SSM notifiche

Amazon Simple Notification Service (Amazon SNS) può avvisarti quando vengono rilasciate nuove versioni di AWS Systems Manager Agent (SSM Agent). Utilizza la procedura seguente per effettuare l'iscrizione a queste notifiche.

### Tip

È possibile inoltre iscriversi alle notifiche consultando la pagina [Note di rilascio dell'SSM Agent](#) su GitHub.

Per abbonarsi a Agente SSM notifiche

1. Apri la console Amazon SNS all'indirizzo <https://console.aws.amazon.com/sns/v3/home>.

2. Dal selettore Regione nella barra di navigazione, scegli Stati Uniti orientali (Virginia settentrionale), se non è già selezionata. Devi selezionare questa opzione Regione AWS perché le notifiche Amazon SNS a SSM Agent cui ti stai abbonando vengono generate solo da questa regione.
3. Nel riquadro di navigazione scegliere Iscrizioni.
4. Scegli Crea iscrizione.
5. Per Crea iscrizione, esegui le seguenti operazioni:
  - a. Per ARN dell'argomento, utilizza il seguente Amazon Resource Name (ARN):  

```
arn:aws:sns:us-east-1:720620558202:SSM-Agent-Update
```
  - b. Per Protocollo, seleziona Email o SMS.
  - c. Per Endpoint, a seconda che tu abbia scelto Email o SMS nel passaggio precedente, inserisci un indirizzo e-mail o un prefisso e un numero per ricevere le notifiche.
  - d. Scegli Crea iscrizione.
6. Se scegli Email, riceverai un messaggio e-mail che ti chiede di confermare l'abbonamento. Aprire il messaggio e seguire le istruzioni per completare l'iscrizione.

Quando esce una nuova versione di SSM Agent, inviamo notifiche agli iscritti. Se non desideri più ricevere queste notifiche, segui la procedura seguente per annullare la sottoscrizione.

Per annullare l'iscrizione a Agente SSM notifiche

1. Aprire la console Amazon SNS.
2. Nel riquadro di navigazione, scegli Iscrizioni.
3. Seleziona la sottoscrizione, quindi scegli Elimina. Quando viene richiesta la conferma, seleziona Elimina.

## Risoluzione dei problemi Agente SSM

In caso di problemi nell'esecuzione delle operazioni sui nodi gestiti, potrebbe esserci un problema con AWS Systems Manager Agent (SSM Agent). Le informazioni seguenti sono utili per visualizzare i file di log di SSM Agent e risolvere i problemi relativi all'agente. Se il tuo agente sembra non rispondere o ha una frequenza di comunicazione ridotta, consulta [Comprensione Agente SSM ibernazione](#).

## Argomenti

- [Agente SSM non è aggiornato](#)
- [Risolvi i problemi utilizzando Agente SSM file di log](#)
- [File watcher non riesce con troppi file aperti \(Linux\)](#)
- [I file di log dell'agente non ruotano \(Windows\)](#)
- [Impossibile connettersi agli endpoint SSM](#)
- [Verifica la configurazione VPC](#)
- [Verifica gli attributi del tuo VPC DNS-related](#)
- [Verifica le regole di accesso sui gruppi di sicurezza degli endpoint](#)
- [Usa ssm-cli per risolvere i problemi di disponibilità dei nodi gestiti](#)

## Agente SSM non è aggiornato

Una versione aggiornata di SSM Agent viene distribuita ogni volta che vengono aggiunti nuovi strumenti a Systems Manager o eseguiti aggiornamenti degli strumenti esistenti. Il mancato utilizzo della versione più recente dell'agente può impedire al nodo gestito di utilizzare vari strumenti e funzionalità di Systems Manager. Per questo motivo, ti consigliamo di automatizzare il processo di aggiornamento di SSM Agent sulle macchine. Per informazioni, consulta [Automatizzazione degli aggiornamenti a Agente SSM](#). Iscriviti alla pagina [Note di rilascio di SSM Agent](#) su GitHub per ricevere notifiche sugli aggiornamenti di SSM Agent.

## Risolvi i problemi utilizzando Agente SSM file di log

SSM Agent registra informazioni nei file seguenti. Le informazioni in questi file possono agevolare la risoluzione dei problemi. Per ulteriori informazioni sui file di log di SSM Agent, incluso come attivare la registrazione di debug, consultare [Visualizzazione Agente SSM log](#).

### Note

Se si sceglie di visualizzare questi registri utilizzando Esplora file di Windows, ricordarsi di consentire la visualizzazione di file nascosti e file di sistema in Opzioni cartella.

### Su Windows

- %PROGRAMDATA%\Amazon\SSM\Logs\amazon-ssm-agent.log

- %PROGRAMDATA%\Amazon\SSM\Logs\errors.log

Su Linux e macOS

- /var/log/amazon/ssm/amazon-ssm-agent.log
- /var/log/amazon/ssm/errors.log

Per i nodi gestiti Linux, è possibile trovare ulteriori informazioni nel file messages scritte nella directory seguente: /var/log.

Per ulteriori informazioni sulla risoluzione dei problemi utilizzando i log dell'agente, consulta [Come posso utilizzare i log di SSM Agent per risolvere i problemi relativi all'SSM Agent nella mia istanza gestita?](#) nel Knowledge Center di AWS re:Post.

## File watcher non riesce con **troppi file aperti** (Linux)

SSM Agent utilizza file watcher per la comunicazione tra processi e processi di lavoro. Questo meccanismo può essere utilizzato da più operazioni di Systems Manager, incluse associazioni e sessioni. Session Manager Se l'agente non è in grado di creare un nuovo file watcher, il registro dell'agente può contenere una voce simile alla seguente:

```
ERROR [NewFileWatcherChannel @ filewatcherchannel.go:104] ... filewatcher listener
encountered error when start watcher: too many open files
```

A seconda del sistema operativo, il testo finale può essere `too many open files` o `otoo many open files`. Per questa firma specifica, la causa principale è l'esaurimento del limite di istanza Linux per utente (UID) di `inotify`. L'errore si verifica quando l'agente crea il watcher, prima di aggiungere un percorso al watcher.

Utilizzate il seguente comando sul nodo gestito per controllare l'attuale limite di istanze `inotify`:

```
sudo sysctl fs.inotify.max_user_instances
```

Il consiglio supportato per questa condizione è di impostare su.

`fs.inotify.max_user_instances 8192` Per applicare il valore al sistema in esecuzione, utilizzate il comando seguente:

```
sudo sysctl -w fs.inotify.max_user_instances=8192
```



Per mantenere il valore, create un file di configurazione sysctl e caricatelo:

```
printf '%s\n' 'fs.inotify.max_user_instances=8192' | sudo tee /etc/sysctl.d/99-amazon-ssm-agent.conf
sudo sysctl -p /etc/sysctl.d/99-amazon-ssm-agent.conf
```

#### Important

Dimensiona i limiti del sistema operativo in base al carico di lavoro sul nodo gestito e alle politiche del sistema operativo dell'organizzazione. Non applicare valori limite non correlati senza valutare altri processi eseguiti con lo stesso UID.

L'`fs.inotify.max_user_watches` impostazione limita il numero di percorsi che le istanze di inotify possono controllare. È diverso `fs.inotify.max_user_instances` e normalmente non deve essere modificato per questo errore di creazione dell'osservatore. Modificalo solo quando la diagnostica del sistema operativo mostra che il limite di watchcount è esaurito.

#### Note

Elabora i limiti dei file aperti, inclusi i limiti della shell `nofile` e le impostazioni, e le `systemd LimitNOFILE` impostazioni di sistema `fs.nr_open` e `fs.file-max` applicali ad altre condizioni di esaurimento dei descrittori di file. Non aumentano il limite di istanza inotify per UID e non risolvono questa firma specifica. `NewFileWatcherChannel`

## I file di log dell'agente non ruotano (Windows)

Se si specifica la rotazione del file di log basata sulla data nel file `seelog.xml` (sui nodi gestiti Windows Server) e i log non ruotano, specificare il parametro `fullname=true`. Ecco un esempio di file di configurazione `seelog.xml` con il parametro `fullname=true` specificato.

```
<seelog type="adaptive" mininterval="2000000" maxinterval="100000000"
critmsgcount="500" minlevel="debug">
 <exceptions>
 <exception filepattern="test*" minlevel="error" />
 </exceptions>
```

```
<outputs formatid="fmtinfo">
 <console formatid="fmtinfo" />
 <rollingfile type="date" datepattern="200601021504" maxrolls="4" filename="C:
\ProgramData\Amazon\SSM\Logs\amazon-ssm-agent.log" fullname="true" />
 <filter levels="error,critical" formatid="fmterror">
 <rollingfile type="date" datepattern="200601021504" maxrolls="4" filename="C:
\ProgramData\Amazon\SSM\Logs\errors.log" fullname="true" />
 </filter>
</outputs>
<formats>
 <format id="fmterror" format="%Date %Time %LEVEL [%FuncShort @ %File.%Line] %Msg
%n" />
 <format id="fmtdebug" format="%Date %Time %LEVEL [%FuncShort @ %File.%Line] %Msg
%n" />
 <format id="fmtinfo" format="%Date %Time %LEVEL %Msg%n" />
</formats>
</seelog>
```

## Impossibile connettersi agli endpoint SSM

SSM Agent deve permettere il traffico in uscita HTTPS (porta 443) verso i seguenti endpoint:

- `ssm.region.amazonaws.com`
- `ssmmessages.region.amazonaws.com`

*region* rappresenta l'identificatore di una regione Regione AWS supportata da AWS Systems Manager, ad esempio per la regione Stati Uniti orientali (`us-east-2Ohio`). Per un elenco dei *region* valori supportati, vedere la colonna Regione negli endpoint [del servizio](#) Systems Manager in. Riferimenti generali di Amazon Web Services

### Note

Prima del 2024, veniva richiesto anche `ec2messages.region.amazonaws.com`.

Per il Regioni AWS lancio prima del 2024, l'autorizzazione al traffico

`ssmmessages.region.amazonaws.com` è ancora obbligatoria ma facoltativa.

`ec2messages.region.amazonaws.com`

Per le regioni lanciate dal 2024 in poi, è necessario consentire l'accesso

al traffico a `ssmmessages.region.amazonaws.com`, ma gli endpoint

`ec2messages.region.amazonaws.com` non sono supportati per queste Regioni.

SSM Agent non funzionerà se non è in grado di comunicare con gli endpoint precedenti, come descritto, anche se utilizzi AWS provided Amazon Machine Images (AMIs) come Amazon Linux 2 o Amazon Linux 2023. La configurazione di rete deve disporre di un accesso a Internet aperto oppure è necessario disporre di endpoint del cloud privato virtuale (VPC) personalizzati configurati. Se non si prevede di creare un endpoint VPC personalizzato, controllare i gateway Internet o i gateway NAT. Per maggiori informazioni su come gestire gli endpoint VPC, consultare [Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager](#).

## Verifica la configurazione VPC

Se utilizzi un cloud privato virtuale (VPC), per gestire le istanze EC2 con Systems Manager, gli endpoint VPC devono essere configurati correttamente per `ssm.region.amazonaws.com`, e in alcuni casi spiegati in precedenza in questo argomento in `ssmmessages.region.amazonaws.com`, [Impossibile connettersi agli endpoint SSM](#) `ec2messages.region.amazonaws.com`

### Note

L'alternativa all'utilizzo di un endpoint VPC è l'abilitazione dell'accesso a Internet in uscita sulle istanze gestite. In questo caso, le istanze gestite devono consentire anche il traffico in uscita HTTPS (porta 443) verso i seguenti endpoint:

- `ssm.region.amazonaws.com`
- `ssmmessages.region.amazonaws.com`
- `ec2messages.region.amazonaws.com`

SSM Agent avvia tutte le connessioni al servizio Systems Manager nel cloud. Per questo motivo, non è necessario configurare il firewall per consentire il traffico in ingresso verso le istanze di Systems Manager.

Per ulteriori informazioni sulle chiamate a questi endpoint, consulta [Referenza: ec2messages, ssmmessages e altre operazioni API](#).

Per risolvere i problemi relativi agli endpoint VPC, esegui queste operazioni:

- Assicurati che gli endpoint VPC siano inclusi a livello di VPC. Quando l'endpoint VPC con un nome di servizio specifico non viene trovato sul VPC, verifica innanzitutto che il supporto DNS sia abilitato

a livello di VPC. Successivamente, crea un nuovo endpoint VPC e associalo a una sottorete in ogni zona di disponibilità.

- Assicurati che un nome DNS privato sia abilitato a livello di endpoint VPC. I nomi DNS privati sono abilitati per impostazione predefinita, ma a un certo punto potrebbero essere stati disabilitati manualmente.
- Assicurati che gli endpoint VPC esistenti siano associati alla sottorete appropriata. Inoltre, assicurati che il VPCE sia già associato a una sottorete in quella zona di disponibilità.

Per ulteriori informazioni, consulta i seguenti argomenti:

- [Accesso a un Servizio AWS utilizzando un endpoint VPC](#) nella Guida AWS PrivateLink
- [Associa un nome DNS privato](#) nella Guida AWS PrivateLink
- [Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager](#)

## Verifica gli attributi del tuo VPC DNS-related

Se utilizzi un cloud privato virtuale (VPC), come parte della verifica della configurazione del tuo VPC, assicurati che gli attributi `enableDnsSupport` e `enableDnsHostnames` siano abilitati.

Puoi abilitare questi attributi utilizzando l'azione API [ModifyVpcAttribute di Amazon EC2](#) o il comando [modify-vpc-attribute](#). AWS CLI <https://docs.aws.amazon.com/cli/latest/reference/ec2/modify-vpc-attribute.html>

Per informazioni sull'attivazione di questi attributi nella console di Amazon VPC, consulta [Visualizzazione e aggiornamento degli attributi DNS per il VPC](#) nella Guida per l'utente di Amazon VPC.

### Note

L'alternativa all'utilizzo di un endpoint VPC è l'abilitazione dell'accesso a Internet in uscita sulle istanze gestite. In questo caso, le istanze gestite devono consentire anche il traffico in uscita HTTPS (porta 443) verso i seguenti endpoint:

- `ssm.region.amazonaws.com`
- `ssmmessages.region.amazonaws.com`
- `ec2messages.region.amazonaws.com`

SSM Agent avvia tutte le connessioni al servizio Systems Manager nel cloud. Per questo motivo, non è necessario configurare il firewall per consentire il traffico in ingresso verso le istanze di Systems Manager.

Per ulteriori informazioni sulle chiamate a questi endpoint, consulta [Referenza: ec2messages, ssmmessages e altre operazioni API](#).

## Verifica le regole di accesso sui gruppi di sicurezza degli endpoint

Assicurati che tutti gli endpoint VPC che hai configurato (`ssm`, `ssmmessages` e `ec2messages`) includano una regola di ingresso nei relativi gruppi di sicurezza per consentire il traffico in ingresso sulla porta 443. Se necessario, puoi creare un nuovo gruppo di sicurezza nel VPC con una regola di ingresso per consentire il traffico sulla porta 443 per il blocco Classless Inter-Domain Routing (CIDR) per il VPC. Dopo aver creato il gruppo di sicurezza, collegalo a ciascun endpoint VPC.

Per ulteriori informazioni, consulta i seguenti argomenti:

- [Come posso creare endpoint VPC in modo da poter utilizzare Systems Manager per gestire istanze EC2 private senza accesso a Internet?](#) su re:POST AWS
- [Blocchi VPC CIDR](#) nella Guida per l'utente di Amazon VPC

## Usa `ssm-cli` per risolvere i problemi di disponibilità dei nodi gestiti

A partire da SSM Agent versione 3.1.501.0, è possibile utilizzare `ssm-cli` per determinare se un nodo gestito soddisfa i requisiti principali per essere gestito da Systems Manager e per apparire negli elenchi di nodi gestiti in Fleet Manager. `ssm-cli` è uno strumento a riga di comando autonomo incluso nell'installazione di SSM Agent. Sono inclusi comandi preconfigurati che raccolgono le informazioni richieste per la diagnostica del motivo per cui un'istanza Amazon EC2 o una macchina non EC2 confermata come in esecuzione non è inclusa negli elenchi dei nodi gestiti in Systems Manager. Questi comandi vengono eseguiti quando si specifica l'opzione `get-diagnostics`.

Per ulteriori informazioni, consulta [Risoluzione dei problemi di disponibilità dei nodi gestiti tramite `ssm-cli`](#).

# Sicurezza in AWS Systems Manager

La sicurezza cloud di Amazon Web Services (AWS) è la priorità più alta. 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 e voi. Il [modello di responsabilità condivisa](#) descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- **Sicurezza del cloud:** AWS è responsabile della protezione dell'infrastruttura in esecuzione Servizi AWS in Cloud AWS. AWS ti offre 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 maggiori informazioni sui programmi di conformità a cui si applicano AWS Systems Manager, consulta [Servizi AWS la sezione Scope by Compliance Program](#).
- **Sicurezza nel cloud:** la tua responsabilità è determinata da Servizio AWS ciò che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS Systems Manager. I seguenti argomenti illustrano come configurare l'Systems Manager per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzarne altri Servizi AWS che ti aiutino a monitorare e proteggere Systems Manager le tue risorse.

## Argomenti

- [Protezione dei dati in AWS Systems Manager](#)
- [Perimetri di dati in AWS Systems Manager](#)
- [Gestione delle identità e degli accessi per AWS Systems Manager](#)
- [Utilizzo di ruoli collegati ai servizi per Systems Manager](#)
- [Registrazione e monitoraggio AWS Systems Manager](#)
- [Convalida della conformità per AWS Systems Manager](#)
- [Resilienza nell' AWS Systems Manager](#)
- [Sicurezza dell'infrastruttura nell' AWS Systems Manager](#)
- [Analisi della configurazione e delle vulnerabilità in AWS Systems Manager](#)

- [Le migliori pratiche di sicurezza per Systems Manager](#)

## Protezione dei dati in AWS Systems Manager

La protezione dei dati si riferisce alla protezione dei dati in transito (durante il viaggio da e verso Systems Manager) e a riposo (mentre sono archiviati nei data AWS center).

Ulteriori informazioni su come il [modello di responsabilità condivisa](#) AWS si applica alla protezione dei dati in AWS Systems Manager. 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 Systems Manager 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.

## Crittografia dei dati

### Crittografia dei dati a riposo

#### Parameter Store parametri

I tipi di parametri che puoi creare inParameter Store, includono `String``StringList`, `eSecureString`.

Tutti i parametri, indipendentemente dal tipo, sono crittografati sia in transito che a riposo. In transito, i parametri vengono crittografati utilizzando Transport Layer Security (TLS), per creare una connessione HTTPS sicura per le richieste API. A riposo, sono crittografati con un Chiave di proprietà di AWS in AWS Key Management Service (AWS KMS). Per ulteriori informazioni sulla Chiave di proprietà di AWS crittografia, consulta [Chiavi di proprietà di AWS](#) la Guida per AWS Key Management Service gli sviluppatori.

Il `SecureString` tipo offre opzioni di crittografia aggiuntive ed è consigliato per tutti i dati sensibili. È possibile scegliere tra i seguenti tipi di chiavi AWS KMS per crittografare e decrittografare il valore di un parametro `SecureString`:

- La Chiave gestita da AWS per il tuo account
- Una chiave gestita dal cliente (CMK) che hai creato nel tuo account
- Un CMK in un altro Account AWS che è stato condiviso con te

Per ulteriori informazioni sulla AWS KMS crittografia, consulta la Guida [per gli](#) AWS Key Management Service sviluppatori.

#### Contenuto nei bucket S3

Come parte delle tue operazioni Systems Manager, puoi scegliere di caricare o archiviare i dati in uno o più bucket Amazon Simple Storage Service (Amazon S3).

Per informazioni sulla crittografia bucket S3, consulta [Protezione dei dati tramite crittografia](#) e [Protezione dei dati in Amazon S3](#) nella Guida per gli sviluppatori Amazon Simple Storage Service.



Di seguito sono riportati i tipi di dati che puoi caricare o che sono stati archiviati nei bucket S3 come parte delle attività Systems Manager:

- L'output dei comandi inRun Command, uno strumento in AWS Systems Manager
- Pacchetti inDistributor, uno strumento in AWS Systems Manager
- L'operazione di applicazione delle patch accedePatch Manager, uno strumento entra AWS Systems Manager
- Patch ManagerElenchi di override delle patch
- Script o Ansible playbook da eseguire in un flusso di lavoro runbook in Automation, uno strumento in AWS Systems Manager
- Chef InSpecprofili da utilizzare con le scansioni in Compliance, uno strumento in AWS Systems Manager
- AWS CloudTrail registri
- Login alla cronologia delle sessioniSession Manager, uno strumento AWS Systems Manager
- Rapporti daExplorer, uno strumento in AWS Systems Manager
- OpsData daOpsCenter, uno strumento in AWS Systems Manager
- AWS CloudFormation modelli da utilizzare con i flussi di lavoro di automazione
- Dati di conformità da una scansione di sincronizzazione dei dati di una risorsa
- Output delle richieste per creare o modificare l'associazione in State Manager, uno strumento di AWS Systems Manager nei nodi gestiti.
- Documenti di Systems Manager personalizzati (documenti SSM) che è possibile eseguire utilizzando il AWS Documento SSM gestito AWS-RunDocument

### CloudWatch Registri, gruppi di log

Come parte delle tue Systems Manager operazioni, puoi scegliere di trasmettere i dati a uno o più gruppi di CloudWatch log di Amazon Logs.

Per informazioni sulla crittografia dei gruppi di CloudWatch log Logs, [consulta Encrypt log data in CloudWatch Logs using AWS Key Management Service](#) nella Amazon CloudWatch Logs User Guide.

I seguenti sono i tipi di dati che potresti aver trasmesso in streaming a un gruppo di CloudWatch log Logs come parte delle tue Systems Manager attività:

- L'output dei comandi di Run Command

- L'output degli script eseguiti utilizzando l'operazione `aws:executeScript` in un runbook Automation
- Log della cronologia delle sessioni di Session Manager
- I log da SSM Agent sui tuoi nodi gestiti

## Crittografia dei dati in transito

Consigliamo di utilizzare un protocollo di crittografia quale Transport Layer Security (TLS) per eseguire la crittografia dei dati sensibili in transito tra i client e i nodi.

Systems Manager fornisce il seguente supporto per la crittografia dei dati in transito.

### Connessioni agli endpoint dell'API Systems Manager

Gli endpoint API di Systems Manager supportano solo connessioni protette tramite HTTPS. Quando gestisci Systems Manager le risorse con l' Console di gestione AWS, l'AWS SDK o l'API Systems Manager, tutte le comunicazioni sono crittografate con Transport Layer Security (TLS). Per un elenco completo degli endpoint API, consulta [Endpoint del Servizio AWS](#) nella Riferimenti generali di Amazon Web Services.

### Istanze gestite

AWS fornisce una connettività sicura e privata tra le istanze di Amazon Elastic Compute Cloud (Amazon EC2). Inoltre, crittografiamo automaticamente il traffico in transito tra istanze supportate nello stesso cloud privato virtuale (VPC o in VPC con peering, utilizzando algoritmi AEAD con crittografia a 256 bit. Tale funzione di crittografia utilizza le funzionalità di offload dell'hardware sottostante e non ha alcun impatto sulle prestazioni della rete. Le istanze supportate sono: C5n, G4, I3en, M5dn, M5n, P3dn, R5dn e R5n.

### Sessioni di Session Manager

Per impostazione predefinita, Session Manager utilizza TLS 1.3 per crittografare i dati delle sessioni trasmessi tra i computer locali di utenti nell'account e le istanze EC2. Puoi anche scegliere di crittografare ulteriormente i dati in transito utilizzando un file creato AWS KMS key in. AWS KMS la crittografia è disponibile per Standard\_Stream e InteractiveCommands tipi di NonInteractiveCommands sessione.

### Accesso a Run Command

Per impostazione predefinita, l'accesso remoto ai nodi mediante Run Command è crittografato utilizzando TLS 1.3 e le richieste per creare una connessione sono firmate utilizzando SigV4.

## Riservatezza del traffico Internet

Puoi utilizzare Amazon Virtual Private Cloud (Amazon VPC) per creare delimitatori tra le risorse nei nodi gestiti e nel traffico di controllo fra di esse, la rete on-premises e Internet. Per i dettagli, consulta la sezione [Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager](#).

Per ulteriori informazioni sulla sicurezza di Amazon Virtual Private Cloud, consulta [Riservatezza del traffico Internet in Amazon VPC](#) nella Guida per l'utente di Amazon VPC.

## Perimetri di dati in AWS Systems Manager

Un perimetro di dati è un insieme di barriere preventive presenti nel tuo AWS ambiente che aiutano a garantire che i tuoi dati siano accessibili solo da identità attendibili provenienti dalle reti e dalle risorse previste. Quando si implementano i controlli perimetrali dei dati, potrebbe essere necessario includere eccezioni per le risorse di proprietà del AWS servizio a cui Systems Manager accede per conto dell'utente.

Scenario di esempio: bucket S3 delle categorie di documenti SSM

Systems Manager accede a un bucket S3 AWS gestito per recuperare informazioni sulle categorie di documenti per. [AWS Systems Manager Documenti di](#) Questo bucket contiene metadati sulle categorie di documenti che aiutano a organizzare e classificare i documenti SSM nella console.

Modelli ARN delle risorse

```
arn:aws:s3:::ssm-document-categories-region
```

Esempi regionali:

- `arn:aws:s3:::ssm-document-categories-us-east-1`
- `arn:aws:s3:::ssm-document-categories-us-west-2`
- `arn:aws:s3:::ssm-document-categories-eu-west-1`
- `arn:aws:s3:::ssm-document-categories-ap-northeast-1`

Quando si è effettuato l'accesso

Questa risorsa è disponibile, quando l'utente visualizza i documenti SSM nella console Systems Manager o quando si utilizzano API che recuperano i metadati e le categorie dei documenti.

## Dati archiviati

Il bucket contiene file JSON con definizioni e metadati delle categorie di documenti. Questi dati sono di sola lettura e non contengono informazioni specifiche sul cliente.

## Identità utilizzata

Systems Manager accede a questa risorsa utilizzando le credenziali di AWS servizio per conto delle richieste dell'utente.

## Autorizzazioni richieste

`s3:GetObject` sui contenuti del bucket.

## Considerazioni sulle policy del perimetro dei dati

Quando si implementano i controlli perimetrali dei dati utilizzando le politiche di controllo dei servizi (SCP) o le politiche degli endpoint VPC con condizioni quali `aws:ResourceOrgID`, è necessario creare eccezioni per le risorse di proprietà del servizio richieste da Systems Manager. AWS

Ad esempio, se si utilizza un SCP per limitare l'accesso alle risorse esterne all'organizzazione, è necessario aggiungere un'eccezione per il bucket delle categorie di documenti SSM.

`aws:ResourceOrgID`

La policy dovrebbe consentire l'accesso a risorse esterne all'organizzazione, ma includerebbe un'eccezione per i bucket S3 appropriati, consentendo a Systems Manager di continuare a funzionare correttamente.

Allo stesso modo, se utilizzate le policy degli endpoint VPC per limitare l'accesso a S3, dovrete assicurarvi che i bucket delle categorie di documenti SSM siano accessibili tramite gli endpoint VPC.

## Scenario di esempio: API di registrazione dei nodi ibridi

I nodi ibridi non appartengono nativamente a un Account AWS, ma ne sono registrati. Per questo motivo, le `ssm:UpdateManagedInstancePublicKey` API `ssm:RegisterManagedInstance` `ssm:RequestManagedInstanceRoleToken`, e non utilizzano AWS Signature Version 4 (Sigv4) per l'autenticazione dei nodi ibridi.

Di conseguenza, la valutazione delle policy non può accedere a un'identità AWS principale o a chiavi di contesto globali come, e. `aws:PrincipalOrgId` `aws:PrincipalAccount` `aws:SourceAccount` Le policy di controllo dei servizi (SCP) e le policy degli endpoint VPC che si basano su queste chiavi globali o sull'identità AWS principale potrebbero bloccare queste

tre API quando i nodi ibridi tentano di registrarsi. Ciò può impedire ai nodi ibridi di completare la registrazione.

Per limitare l'accesso a queste API in base all'appartenenza all'account o all'organizzazione, utilizza le seguenti chiavi di condizione di Systems Manager, che si risolvono in modo coerente sia per le istanze di Amazon EC2 che per i nodi ibridi:

- `ssm:NodeAccountId`— Si risolve nell'account in cui esiste un'istanza Amazon EC2 o nell'account in cui è registrato un nodo ibrido.
- `ssm:NodeOrgId`— Si riferisce all'organizzazione proprietaria dell'account dell'istanza Amazon EC2 o all'organizzazione dell'account in cui è registrato un nodo ibrido.

### Ulteriori informazioni

Per ulteriori informazioni sui perimetri dei dati in AWS, consulta i seguenti argomenti:

- [Perimetri di dati attivi. AWS](#)
- [Stabilisci i guardrail delle autorizzazioni utilizzando i perimetri dei dati nella IAM User Guide](#)
- [Service-specific linee guida: AWS Systems Manager](#) e [Service-owned risorse](#) nel repository Samples su AWS GitHub

## Gestione delle identità e degli accessi per AWS Systems Manager

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 è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) a utilizzare risorse Systems Manager. IAM è un programma Servizio AWS che puoi utilizzare senza costi aggiuntivi.

### Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso tramite policy](#)
- [In che modo AWS Systems Manager funziona con IAM](#)
- [AWS Systems Manager esempi di politiche basate sull'identità](#)
- [AWS politiche gestite per AWS Systems Manager](#)

- [Risoluzione dei problemi di identità e accesso in AWS Systems Manager](#)

## Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta [Risoluzione dei problemi di identità e accesso in AWS Systems Manager](#))
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta [In che modo AWS Systems Manager funziona con IAM](#))
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta [AWS Systems Manager esempi di politiche basate sull'identità](#))

## Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali da una fonte di identità come Centro identità AWS IAM (IAM Identity Center), autenticazione Single Sign-on o credenziali. Google/Facebook Per ulteriori informazioni sull'accesso, consulta [Come accedere all' Account AWS](#) nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta [AWS Signature Version 4 per le richieste API](#) nella Guida per l'utente di IAM.

## Account AWS utente root

Quando ne crei uno Account AWS, inizi con un'identità di accesso chiamata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali come utente root, consulta [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente di IAM.

## Utenti e gruppi IAM

Un [utente IAM](#) è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali

a lungo termine. Per ulteriori informazioni, consulta [Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee](#) nella IAM User Guide.

Un [gruppo IAM](#) specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta [Casi d'uso per utenti IAM](#) nella Guida per l'utente di IAM.

## Ruoli IAM

Un [ruolo IAM](#) è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo [passando da un utente a un ruolo IAM \(console\)](#) o chiamando un'operazione AWS API AWS CLI or. Per ulteriori informazioni, consulta [Metodi per assumere un ruolo](#) nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

## Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un principale effettua una richiesta. La maggior parte delle policy sono archiviate AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

## Identity-based politiche

Identity-based le policy sono documenti relativi alle politiche di autorizzazione JSON che si allegano a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità,

nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente IAM.

Identity-based le politiche possono essere politiche in linea (incorporate direttamente in una singola identità) o politiche gestite (politiche autonome associate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scegliere tra policy gestite e policy in linea](#) nella Guida per l'utente di IAM.

Per informazioni sulle politiche AWS gestite per Systems Manager, vedere. [AWS Systems Manager policy gestite](#)

## Resource-based politiche

Resource-based le policy sono documenti di policy JSON che alleggi a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#).

Resource-based le policy sono policy in linea che si trovano in quel servizio. Non è possibile utilizzare le policy AWS gestite da IAM in una policy basata sulle risorse.

## Chiavi di condizione delle policy

Le operazioni che gli utenti e i ruoli eseguono e le risorse su cui intraprendono tali operazioni hanno la possibilità di essere ulteriormente limitate da condizioni specifiche.

Nel documento sulla policy JSON, l'elemento Condition (o blocco di Condition) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento Condition è facoltativo. È possibile compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio StringEquals o StringNotLike, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi Condition in un'istruzione o più chiavi in un singolo elemento Condition, questi vengono valutati da AWS tramite un'operazione AND logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. OR Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.



È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta [Elementi delle policy IAM: variabili e tag](#) nella Guida per l'utente IAM.

AWS supporta le chiavi di condizione globali e le chiavi di condizione specifiche del servizio. Per ulteriori informazioni, consultare [Chiavi di contesto delle condizioni globali AWS](#) nella Guida per l'utente IAM.

 Important

Se utilizzi Systems Manager Automation, ti consigliamo di non utilizzare la chiave di Sourcelp [condizione](#) `aws:` nelle tue policy. Il comportamento di questa chiave di condizione dipende da diversi fattori, tra cui l'eventuale fornitura di un ruolo IAM per l'esecuzione del runbook di Automazione e le azioni di Automazione utilizzate nel runbook. Di conseguenza, la chiave di condizione può produrre un comportamento imprevisto. Per questo motivo, ti consigliamo di non utilizzarlo.

Systems Manager supporta diverse chiavi di condizione proprie. Per ulteriori informazioni, consulta [Chiavi di condizione per AWS Systems Manager](#) nel Service Authorization Reference. Le azioni e le risorse con cui è possibile utilizzare una chiave di Manager-specific condizione Systems sono elencate nei tipi di [risorse definiti da AWS Systems Manager](#) nel Service Authorization Reference.

Quando la politica ha necessità di dipendere dal nome principale di un servizio di proprietà di Systems Manager, si consiglia di verificarne l'esistenza o l'inesistenza utilizzando la [chiave di condizione multivalore](#) `aws:PrincipalServiceNamesList`, anziché la chiave di condizione `aws:PrincipalServiceName`. La chiave di condizione `aws:PrincipalServiceName` contiene solo una voce dall'elenco dei nomi principali del servizio e potrebbe non essere sempre il nome principale del servizio previsto. Il seguente blocco di `Condition` mostra la verifica dell'esistenza di `ssm.amazonaws.com`.

```
{
 "Condition": {
 "ForAnyValue:StringEquals": {
 "aws:PrincipalServiceNamesList": "ssm.amazonaws.com"
 }
 }
}
```

Per visualizzare esempi di policy basate sull'identità di Systems Manager, consulta [AWS Systems Manager esempi di politiche basate sull'identità](#).

## Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali entità principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta [Panoramica delle liste di controllo degli accessi \(ACL\)](#) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

## Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.
- Policy di controllo dei servizi (SCP): specifica il numero massimo di autorizzazioni per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. Per ulteriori informazioni, consultare [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations .
- Policy di controllo delle risorse (RCP): imposta le autorizzazioni massime disponibili per le risorse degli account. Per ulteriori informazioni, consulta [Policy di controllo delle risorse \(RCP\)](#) nella Guida per l'utente di AWS Organizations .
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare [Policy di sessione](#) nella Guida per l'utente IAM.

## Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per sapere come AWS determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta la logica di valutazione delle [policy](#) nella IAM User Guide.

## In che modo AWS Systems Manager funziona con IAM

Prima di utilizzare AWS Identity and Access Management (IAM) per gestire l'accesso a AWS Systems Manager, è necessario comprendere con quali funzionalità IAM è possibile utilizzare Systems Manager. Per avere una panoramica generale di come Systems Manager e altri Servizi AWS funzionano con IAM, vedi [Servizi AWS come funziona con IAM](#) nella IAM User Guide.

### Argomenti

- [Systems Manager policy basate sull'identità](#)
- [Systems Manager policy basate sulle risorse](#)
- [Autorizzazione basata su Systems Manager tag](#)
- [Systems Manager Ruoli IAM](#)

### Systems Manager policy basate sull'identità

Con le policy basate su identità IAM è possibile specificare operazioni e risorse consentite o rifiutate, nonché le condizioni in base alle quali le operazioni sono consentite o rifiutate. Systems Manager supporta operazioni, risorse e chiavi di condizione specifiche. Per informazioni su tutti gli elementi utilizzati in una policy JSON, consulta [Documentazione di riferimento agli elementi delle policy JSON IAM](#) nella Guida per l'utente IAM.

### Azioni

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni di eseguire l'operazione associata.

Le operazioni delle policy in Systems Manager utilizzano il seguente prefisso prima dell'operazione: `ssm:`. Ad esempio, per concedere a qualcuno l'autorizzazione per creare un parametro Systems Manager (parametro SSM) mediante l'operazione API Systems Manager `PutParameter`, includere l'operazione `ssm:PutParameter` nella policy. Le istruzioni delle policy devono includere un elemento `Action` o `NotAction`. Systems Manager definisce una propria serie di operazioni che descrivono le attività eseguibili con questo servizio.

Per specificare più azioni in una sola istruzione, separa ciascuna di esse con una virgola come mostrato di seguito:

```
"Action": [
 "ssm:action1",
 "ssm:action2"
]
```

#### Note

I seguenti strumenti AWS Systems Manager utilizzano prefissi diversi prima delle azioni.

- AWS AppConfig utilizza il prefisso `appconfig:` delle azioni.
- Lo strumento di Gestione degli incidenti utilizza il prefisso `ssm-incidents:` o `ssm-contacts:` prima delle operazioni.
- Systems Manager GUI Connect utilizza il prefisso `ssm-guiconnect:` prima delle operazioni.
- Quick Setup utilizza il prefisso `ssm-quicksetup:` prima delle operazioni.

È possibile specificare più operazioni tramite caratteri jolly (\*). Ad esempio, per specificare tutte le operazioni che iniziano con la parola `Describe`, includi la seguente operazione:

```
"Action": "ssm:Describe*"
```

Per visualizzare un elenco di operazioni Systems Manager, consulta [Operazioni definite da AWS Systems Manager](#) in Riferimento per l'autorizzazione del servizio.

## Resources

Gli amministratori possono utilizzare le politiche AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (\*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Ad esempio, la risorsa finestra di manutenzione Systems Manager ha il seguente formato ARN.

```
arn:aws:ssm:region:account-id:maintenancewindow/window-id
```

Per specificare le finestre di manutenzione mw-0c50858d01EXAMPLE nell'istruzione nella regione Stati Uniti orientali (Ohio), utilizzare un ARN simile al seguente.

```
"Resource": "arn:aws:ssm:us-east-2:123456789012:maintenancewindow/mw-0c50858d01EXAMPLE"
```

Per specificare che tutte le finestre di manutenzione che appartengono ad un account specifico, utilizza il carattere jolly (\*).

```
"Resource": "arn:aws:ssm:region:123456789012:maintenancewindow/*"
```

Per le operazioni Parameter Store API, puoi fornire o limitare l'accesso a tutti i parametri in un livello di una gerarchia utilizzando i nomi gerarchici e le politiche AWS Identity and Access Management (IAM) come segue.

```
"Resource": "arn:aws:ssm:region:123456789012:parameter/Dev/ERP/Oracle/*"
```

Alcune operazioni Systems Manager, ad esempio quelle per la creazione di risorse, non possono essere eseguite su una risorsa specifica. In questi casi, è necessario utilizzare il carattere jolly (\*).

```
"Resource": "*"
```

Alcune operazioni API di Systems Manager accettano più risorse. Per specificare più risorse in una sola dichiarazione, separa i relativi ARN con una virgola come mostrato di seguito.

```
"Resource": [
 "resource1",
 "resource2"
```

#### Note

La maggior parte Servizi AWS considera i due punti (:) o una barra (/) come lo stesso carattere negli ARN. Tuttavia, Systems Manager richiede una corrispondenza esatta nei

modelli di risorse e nelle regole. Durante la creazione di modelli di eventi, assicurati di utilizzare i caratteri ARN corretti, facendo in modo che corrispondano all'ARN della risorsa.

Nella tabella seguente vengono descritti i formati ARN per i tipi di risorse supportati da Systems Manager.

#### Note

Notate le seguenti eccezioni ai formati ARN.

- I seguenti strumenti AWS Systems Manager utilizzano prefissi diversi prima delle azioni.
  - AWS AppConfig utilizza il prefisso `appconfig:` delle azioni.
  - Lo strumento di Gestione degli incidenti utilizza il prefisso `ssm-incidents:` o `ssm-contacts:` prima delle operazioni.
  - Systems Manager GUI Connect utilizza il prefisso `ssm-guiconnect` prima delle operazioni.
- I documenti e le risorse di definizione dell'automazione di proprietà di Amazon e i parametri pubblici forniti da Amazon e da fonti terze non includono gli ID degli account nei loro formati ARN. Ad esempio:
  - Il documento SSM AWS-RunPatchBaseline:

```
arn:aws:ssm:us-east-2::document/AWS-RunPatchBaseline
```

- Il runbook Automation AWS-ConfigureMaintenanceWindows:

```
arn:aws:ssm:us-east-2::automation-definition/AWS-ConfigureMaintenanceWindows
```

- I parametri pubblici `/aws/service/bottlerocket/aws-ecs-1-nvidia/x86_64/1.13.4/image_version`:

```
arn:aws:ssm:us-east-2::parameter/aws/service/bottlerocket/aws-ecs-1-nvidia/x86_64/1.13.4/image_version
```

Per ulteriori informazioni su questi tre tipi di risorse, consulta i seguenti argomenti:

- [Utilizzo dei documenti](#)
- [Esegui un'operazione automatizzata basata su Systems Manager Automation](#)
- [Utilizzo di parametri pubblici in Parameter Store](#)

- Quick Setup utilizza il prefisso `ssm-quicksetup:` prima delle operazioni.

Tipo di risorsa	Formato ARN
Applicazione (AWS AppConfig)	<code>arn:aws:appconfig: <i>region</i> :<i>account-id</i> :<i>application-id</i></code>
Associazione	<code>arn:aws:ssm: <i>region</i> :<i>account-id</i> :<i>association-id</i></code>
Esecuzione di automazione	<code>arn:aws:ssm: <i>region</i> :<i>account-id</i> :<i>automation-execution-id</i></code>
Definizione di automazione (con sottorisorsa della versione)	<code>arn:aws:ssm: <i>region</i> :<i>account-id</i> :<i>automation-definition-id</i> :<i>version-id</i></code>
Profilo di configurazione (AWS AppConfig)	<code>arn:aws:appconfig: <i>region</i> :<i>account-id</i> :<i>application-id</i> :<i>configurationprofile-id</i></code>
Contattare lo strumento di gestione degli incidenti	<code>arn:aws:ssm-contacts: <i>region</i> :<i>account-id</i> :<i>contact-alias</i></code>
Strategia di distribuzione (AWS AppConfig)	<code>arn:aws:appconfig: <i>region</i> :<i>account-id</i> :<i>deploymentstrategy-id</i></code>
Documento	<code>arn:aws:ssm: <i>region</i> :<i>account-id</i> :<i>document-name</i></code>
Ambiente (AWS AppConfig)	<code>arn:aws:appconfig: <i>region</i> :<i>account-id</i> :<i>application-id</i> :<i>environment-id</i></code>
Incidente	<code>arn:aws:ssm-incidents: <i>region</i> :<i>account-id</i> :<i>incident-record</i> :<i>response-plan-name</i> :<i>incident-id</i></code>
Finestra di manutenzione	<code>arn:aws:ssm: <i>region</i> :<i>account-id</i> :<i>window-id</i></code>

Tipo di risorsa	Formato ARN
Nodo gestito	arn:aws:ssm: <i>region</i> ::managed-instance/ <i>account-id</i> <i>managed-node-id</i>
Inventario nodi gestiti	arn:aws:ssm: <i>region</i> ::managed-instance-inventory/ <i>account-id</i> <i>managed-node-id</i>
OpsItem	arn:aws:ssm: <i>region</i> ::opsitem/ <i>account-id</i> <i>OpsItem-id</i>
Parametro	<p>Parametro a un livello:</p> <ul style="list-style-type: none"> <li>arn:aws:ssm: ::parametro/<i>region</i>/<i>account-id</i> <i>parameter-name</i></li> </ul> <p>Un parametro denominato con una struttura gerarchica:</p> <ul style="list-style-type: none"> <li>arn:aws:ssm: <i>region</i> ::parametro///// <i>account-id</i> /<i>parameter-name-root</i> <i>2</i> <i>level-2</i> <i>level-3</i> <i>level-4</i> <i>level-5</i></li> </ul>
baseline delle patch	arn:aws:ssm: <i>region</i> ::patchbaseline/ <i>account-id</i> <i>patch-baseline-id</i>
Piano di risposta	arn:aws:ssm-incidents: <i>region</i> ::response-plan/ <i>account-id</i> <i>response-plan-name</i>
Sessione	arn:aws:ssm: ::session/ <i>3 region account-id session-id</i>
Tutte le risorse Systems Manager	arn:aws:ssm:*
Tutte le risorse di proprietà di chi è specificato nello specificato Systems Manager Account AWS Regione AWS	arn:aws:ssm::: * <i>region account-id</i>



 Note

Le risorse per le definizioni di automazione sono obsolete. Aggiorna le politiche IAM per includere un'autorizzazione `ssm:StartAutomationExecution` o attivazione `document` e `ssm:StartChangeRequestExecution` automazione-execution risorse. Per visualizzare le best practice e gli esempi per l'impostazione delle autorizzazioni IAM, consulta la nostra guida [utente di esempio per la](#) configurazione di politiche basate sull'identità.

<sup>1</sup> Per le definizioni di automazione, Systems Manager supporta una risorsa di secondo livello, ID versione. In AWS, queste risorse di secondo livello sono note come risorse secondarie. Specificare una sottorisorsa della versione per una risorsa di definizione di automazione consente di fornire l'accesso ad alcune versioni di una definizione di automazione. Ad esempio, potresti voler assicurarti che nella gestione dei nodi venga utilizzata solo la versione più recente di una definizione di automazione.

<sup>2</sup> Per organizzare e gestire i parametri, puoi creare nomi per i parametri con una struttura gerarchica. Con tale struttura gerarchica, un nome di parametro può includere un percorso che definisci tramite l'utilizzo delle barre. È possibile assegnare un nome a una risorsa di parametro con un massimo di quindici livelli. Ti consigliamo di creare gerarchie che riflettano una struttura gerarchica esistente nel tuo ambiente. Per ulteriori informazioni, consulta [Creazione in corso Parameter Store parametri in Systems Manager](#).

<sup>3</sup> Nella maggior parte dei casi, l'ID sessione è costruito utilizzando l'ID dell'utente dell'account che ha iniziato la sessione, oltre a un suffisso alfanumerico. Ad esempio:

```
arn:aws:us-east-2:111122223333:session/JohnDoe-1a2b3c4sEXAMPLE
```

Tuttavia, se l'ID utente non è disponibile, l'ARN viene costruito in questo modo:

```
arn:aws:us-east-2:111122223333:session/session-1a2b3c4sEXAMPLE
```

Per ulteriori informazioni sul formato degli ARN, consulta [Amazon Resource Names \(ARN\)](#) nella Riferimenti generali di Amazon Web Services.

Per visualizzare un elenco di tipi di risorse Systems Manager e dei relativi ARN, consulta [Risorse definite da AWS Systems Manager](#) in Riferimento per l'autorizzazione del servizio. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta [Operazioni definite da AWS Systems Manager](#).

## Chiavi di condizione per Systems Manager

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per vedere tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni [AWS globali](#) nella IAM User Guide.

Per visualizzare un elenco di chiavi di condizione Systems Manager, consulta [Condition Keys \(Chiavi di condizione\) per per AWS Systems Manager](#) nel Service Authorization Reference (Riferimento per l'autorizzazione del servizio). Per informazioni su operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consulta [Operazioni definite da AWS Systems Manager](#).

Per informazioni sull'utilizzo della chiave di condizione `ssm:resourceTag/*`, consulta gli argomenti elencati di seguito:

- [Limitare l'accesso ai comandi a livello di root tramite SSM Agent](#)
- [Limitazione Run Command accesso basato su tag](#)
- [Limitazione dell'accesso alla sessione in base ai tag dell'istanza](#)

Per informazioni sull'uso delle chiavi di `ssm:Overwrite` condizione `ssm:Policies` e per indicazioni su come limitare l'accesso ai singoli parametri e ai percorsi dei parametri, consulta [Impedire l'accesso a Parameter Store operazioni API](#).

## Esempi

Per visualizzare esempi di policy basate su identità Systems Manager, consulta [AWS Systems Manager esempi di politiche basate sull'identità](#).

## Systems Manager policy basate sulle risorse

Altri Servizi AWS, come Amazon Simple Storage Service (Amazon S3), supportano politiche di autorizzazione basate sulle risorse. Ad esempio, è possibile allegare una policy di autorizzazione a un bucket S3 per gestire le autorizzazioni di accesso a quel bucket.

Systems Manager non supporta le policy basate su risorse.

## Autorizzazione basata su Systems Manager tag

È possibile collegare i tag alle risorse Systems Manager o passare i tag in una richiesta a Systems Manager. Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'[elemento condizione](#) di una policy utilizzando le chiavi di condizione `ssm:resourceTag/key-name`, `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`. È possibile aggiungere tag ai seguenti tipi di risorse quando vengono creati o aggiornati:

- Documento
- Nodo gestito
- Finestra di manutenzione
- Parametro
- baseline delle patch
- OpsItem

Per visualizzare una policy basata sulle identità di esempio per limitare l'accesso a una risorsa basata su tag su tale risorsa, consulta [Visualizzazione Systems Manager documenti basati su tag](#).

## Systems Manager Ruoli IAM

Un ruolo [IAM](#) è un'entità all'interno dell'utente Account AWS che dispone di autorizzazioni specifiche.

### Utilizzo di credenziali temporanee con Systems Manager

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. È possibile ottenere credenziali di sicurezza temporanee chiamando operazioni API Servizio di token di sicurezza AWS (AWS STS) come [AssumeRole](#) o [GetFederationToken](#).

Systems Manager supporta l'uso di credenziali temporanee.

### Service-linked ruoli

[Service-linked i ruoli](#) consentono Servizi AWS di accedere alle risorse di altri servizi per completare un'azione per conto dell'utente. Service-linked i ruoli sono elencati nel tuo account IAM e sono di

proprietà del servizio. Un amministratore può visualizzare, ma non modificare le autorizzazioni dei ruoli collegati ai servizi.

Systems Manager supporta i ruoli collegati ai servizi. Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi Systems Manager, consulta [Utilizzo di ruoli collegati ai servizi per Systems Manager](#).

## Ruoli dei servizi

Questa funzionalità consente a un servizio di assumere un [ruolo di servizio](#) per conto dell'utente. Questo ruolo consente al servizio di accedere alle risorse in altri servizi per completare un'azione per conto dell'utente. I ruoli dei servizi sono visualizzati nell'account IAM e sono di proprietà dell'account. Ciò significa che un amministratore può modificare le autorizzazioni per questo ruolo. Tuttavia, il farlo potrebbe pregiudicare la funzionalità del servizio.

Systems Manager supporta i ruoli dei servizi.

## Scelta di un ruolo IAM in Systems Manager

Affinché Systems Manager interagisca con i nodi gestiti, è necessario scegliere un ruolo per consentire l'accesso di Systems Manager alle istanze a tuo nodo. Se in precedenza hai creato un ruolo di servizio o un ruolo collegato al servizio, ti Systems Manager fornisce un elenco di ruoli tra cui scegliere. È importante scegliere un ruolo che consenta l'accesso per avviare e arrestare i nodi gestiti.

Per accedere alle istanze EC2, è necessario configurare le autorizzazioni dell'istanza. Per informazioni, consulta la pagina [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#).

Per accedere a nodi non EC2 in un ambiente [ibrido e multicloud](#), il ruolo di cui il tuo Account AWS ha bisogno è un ruolo di servizio IAM. Per informazioni, consulta [Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud](#).

I flussi di lavoro di automazione possono essere avviati nel contesto di un ruolo di servizio (o ruolo presunto). Ciò permette al servizio di eseguire operazioni per conto tuo. Se non specifichi un ruolo presunto, il servizio di automazione utilizza il contesto dell'utente che ha richiamato l'esecuzione. Tuttavia, i seguenti scenari richiedono di specificare un ruolo di servizio di automazione. Per ulteriori informazioni, consulta [Configurazione di un accesso al ruolo di servizio \(ruolo presunto\) per le automazioni](#).

## AWS Systems Manager policy gestite

AWS risolve molti casi d'uso comuni fornendo policy IAM autonome create e amministrate da AWS. Le policy gestite da AWS concedono le autorizzazioni necessarie per i casi di utilizzo comune in modo da non dover cercare quali sono le autorizzazioni richieste. (È inoltre possibile creare policy IAM personalizzate per concedere le autorizzazioni per operazioni e risorse Systems Manager).

Per ulteriori informazioni sulle policy gestite per Systems Manager, consulta [AWS politiche gestite per AWS Systems Manager](#)

Per informazioni generali sulle policy gestite, consulta [Policy gestite da AWS](#) nella Guida per l'utente IAM.

## AWS Systems Manager esempi di politiche basate sull'identità

Per impostazione predefinita, le entità AWS Identity and Access Management (IAM) (utenti e ruoli) non dispongono dell'autorizzazione per creare o modificare AWS Systems Manager risorse. Inoltre, non possono eseguire attività utilizzando la console di Systems Manager, AWS Command Line Interface (AWS CLI) o AWS l'API. È necessario un amministratore per creare politiche IAM che concedano a utenti e ruoli l'autorizzazione a eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi collegare queste policy a utenti o gruppi che richiedono tali autorizzazioni.

Di seguito è riportato un esempio di politica di autorizzazioni che consente a un utente di eliminare documenti con nomi che iniziano con **MyDocument** - Stati Uniti orientali (Ohio) (us-east-2). Regione AWS

JSON

```
{
 "Version": "2012-10-17",
 "Statement" : [
 {
 "Effect" : "Allow",
 "Action" : [
 "ssm:DeleteDocument"
],
 "Resource" : [
 "arn:aws:ssm:us-east-1:111122223333:document/MyDocument-*"
]
 }
]
}
```

```
}
]
}
```

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta [Creazione di policy](#) nella Guida per l'utente IAM.

## Argomenti

- [Best practice per le policy](#)
- [Esempio: autorizzazione all'uso di Systems Manager console](#)
- [Esempio: consentire agli utenti di visualizzare le loro autorizzazioni](#)
- [Esempio: autorizzazione per leggere e descrivere parametri individuali](#)
- [Cross-service prevenzione sostitutiva confusa](#)
- [Esempi di policy gestite dal cliente](#)
- [Visualizzazione Systems Manager documenti basati su tag](#)

## Best practice per le policy

Identity-based le politiche stabiliscono se qualcuno può creare, accedere o eliminare Systems Manager risorse nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere le autorizzazioni agli utenti e ai carichi di lavoro, utilizza le policy AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dal cliente specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente di IAM.

- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare [Convalida delle policy per il Sistema di analisi degli accessi IAM](#) nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root Account AWS, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare [Protezione dell'accesso API con MFA](#) nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta [Best practice di sicurezza in IAM](#) nella Guida per l'utente di IAM.

## Esempio: autorizzazione all'uso di Systems Manager console

Per accedere alla console di Systems Manager è necessario disporre di una serie di autorizzazioni minima. Queste autorizzazioni devono consentire di elencare e visualizzare i dettagli relativi alle risorse Systems Manager e ad altre risorse nel proprio Account AWS.

Se crei una policy basata su identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità IAM (utenti o ruoli) associate a tale policy.

Non è necessario consentire le autorizzazioni minime della console per gli utenti che effettuano chiamate solo all'API AWS CLI o all' AWS API. Al contrario, è possibile accedere solo alle operazioni che soddisfano l'operazione API che stai cercando di eseguire.

Per assicurarti che utenti e ruoli possano ancora utilizzare la console di Systems Manager, allega anche la policy [AmazonSSMFullAccess](#) or [AmazonSSMReadOnlyAccess](#) AWS managed alle entità. Per maggiori informazioni, consulta [Aggiunta di autorizzazioni a un utente](#) nella Guida per l'utente di IAM.

## Esempio: consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy in linea e quelle gestite che sono collegate alla relativa identità utente. Questa policy include le autorizzazioni per completare questa azione sulla console o a livello di programmazione utilizzando l' AWS CLI API or. AWS

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "ViewOwnUserInfo",
 "Effect": "Allow",
 "Action": [
 "iam:GetUserPolicy",
 "iam:ListGroupsForUser",
 "iam:ListAttachedUserPolicies",
 "iam:ListUserPolicies",
 "iam:GetUser"
],
 "Resource": ["arn:aws:iam::*:user/${aws:username}"]
 },
 {
 "Sid": "NavigateInConsole",
 "Effect": "Allow",
 "Action": [
 "iam:GetGroupPolicy",
 "iam:GetPolicyVersion",
 "iam:GetPolicy",
 "iam:ListAttachedGroupPolicies",
 "iam:ListGroupPolicies",
 "iam:ListPolicyVersions",
 "iam:ListPolicies",
 "iam:ListUsers"
],
 "Resource": "*"
 }
]
}
```



## Esempio: autorizzazione per leggere e descrivere parametri individuali

Example Leggi e descrivi un parametro

È possibile concedere l'accesso a un parametro allegando a un'identità la policy seguente.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:GetParameter",
 "ssm:DescribeParameters"
],
 "Resource": "arn:aws:ssm:us-east-1:111122223333:parameter/parameter-name"
 }
]
}
```

## Cross-service prevenzione sostitutiva 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. Nel AWS, l'impersonificazione tra servizi può portare al confuso problema del vice. Cross-service l'imitazione può avvenire quando un servizio (il servizio chiamante) chiama un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare che ciò accada, AWS fornisce strumenti che consentono di proteggere i dati per tutti i servizi ai quali è stato concesso l'accesso alle risorse del proprio account.

Ti consigliamo di utilizzare le chiavi di contesto delle condizioni globali [aws:SourceArn](#) e [aws:SourceAccount](#) nelle policy delle risorse per limitare le autorizzazioni con cui AWS Systems Manager fornisce un altro servizio alla risorsa. Se il valore `aws:SourceArn` non contiene l'ID account, ad esempio il nome della risorsa Amazon (ARN) di un bucket S3, è necessario utilizzare entrambe le chiavi di contesto delle condizioni globali per limitare le autorizzazioni. 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` deve utilizzare lo stesso ID account nella stessa dichiarazione di policy. Utilizzare `aws:SourceArn` se si desidera consentire l'associazione di una sola risorsa all'accesso tra servizi. Utilizzare `aws:SourceAccount` se si desidera consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi.

Nelle seguenti sezioni sono fornite le policy di esempio per gli strumenti AWS Systems Manager.

### Esempio di policy di attivazione ibrida

Per i ruoli di servizio utilizzati in un'[attivazione ibrida](#), il valore di `aws:SourceArn` deve essere l'ARN dell' Account AWS. Assicurati di specificare nell'ARN il luogo Regione AWS in cui hai creato l'attivazione ibrida. Se non si conosce l'ARN completo della risorsa o se si sta specificando più risorse, utilizzare la chiave di condizione del contesto globale `aws:SourceArn` con caratteri speciali (\*) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:ssm:*:region:123456789012:*`.

L'esempio seguente illustra l'utilizzo delle chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` per permettere all'automazione di prevenire il problema del “confused deputy” nella regione Stati Uniti orientali (Ohio) (us-east-2).

### JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "",
 "Effect": "Allow",
 "Principal": {
 "Service": "ssm.amazonaws.com"
 },
 "Action": "sts:AssumeRole",
 "Condition": {
 "StringEquals": {
 "aws:SourceAccount": "123456789012"
 },
 "ArnEquals": {
 "aws:SourceArn": "arn:aws:ssm:us-east-1:123456789012:*"
 }
 }
 }
]
}
```

```
}
```

## Esempio di policy di sincronizzazione dati risorsa

Systems Manager Inventory and Compliance ti consentono di creare una sincronizzazione dei dati delle risorse per centralizzare l'archiviazione dei dati operativi (OpsData) in un bucket centrale di Amazon Simple Storage Service. Explorer Per crittografare la sincronizzazione dei dati di una risorsa con AWS Key Management Service (AWS KMS), crea una nuova chiave che includa la seguente policy o aggiorna una chiave esistente per aggiungere questa policy. Le chiavi delle condizioni `aws:SourceArn` e `aws:SourceAccount` in questa policy impediscono il problema confused deputy.

## JSON

```
{
 "Version": "2012-10-17",
 "Id": "ssm-access-policy",
 "Statement": [
 {
 "Sid": "ssm-access-policy-statement",
 "Action": [
 "kms:GenerateDataKey"
],
 "Effect": "Allow",
 "Principal": {
 "Service": "ssm.amazonaws.com"
 },
 "Resource": "arn:aws:kms:us-east-1:123456789012:key/KMS_key_id",
 "Condition": {
 "StringLike": {
 "aws:SourceAccount": "123456789012"
 },
 "ArnLike": {
 "aws:SourceArn": "arn:aws:ssm:*:123456789012:role/aws-
service-role/ssm.amazonaws.com/AWSServiceRoleForAmazonSSM"
 }
 }
 }
]
}
```

 Note

L'ARN nell'esempio di policy consente al sistema di crittografare OpsData da tutte le fonti tranne AWS Security Hub CSPM. Se è necessario crittografare i dati CSPM di Security Hub, ad esempio se si utilizzano Explorer per raccogliere dati CSPM di Security Hub, è necessario allegare una policy aggiuntiva che specifichi il seguente ARN:

```
"aws:SourceArn": "arn:aws:ssm:*:account-id:role/
aws-service-role/opsdatasync.ssm.amazonaws.com/
AWSServiceRoleForSystemsManagerOpsDataSync"
```

## Esempi di policy gestite dal cliente

È possibile creare policy autonome amministrate nel proprio Account AWS. Facciamo riferimento a queste policy con il nome di policy gestite dal cliente. Puoi allegare queste politiche a più entità principali del tuo Account AWS. Quando si allega una policy a un'entità principale, è necessario fornire all'entità le autorizzazioni definite nella policy. Per ulteriori informazioni, consulta [Esempi di policy gestite dal cliente](#) nella [Guida per l'utente IAM](#).

I seguenti esempi di policy utente concedono le autorizzazioni per varie operazioni di Systems Manager. Utilizzale per limitare l'accesso a Systems Manager per le entità IAM (utenti e ruoli). Queste politiche funzionano quando si eseguono azioni nell'Systems Manager API, negli AWS SDK o nel AWS CLI. Per gli utenti che utilizzano la console, devi concedere autorizzazioni aggiuntive specifiche per la console. Per ulteriori informazioni, consulta [Esempio: autorizzazione all'uso di Systems Manager console](#).

 Note

Tutti gli esempi utilizzano la Regione Stati Uniti occidentali (Oregon) (us-west-2) e contengono ID account fittizi. L'ID dell'account non deve essere specificato nell'Amazon Resource Name (ARN) per i documenti AWS pubblici (documenti che iniziano con AWS- \*).

## Esempi

- [Esempio 1: consenti a un utente di eseguire Systems Manager operazioni in una singola regione](#)
- [Esempio 2: permettere a un utente di elencare i documenti per una sola Regione](#)

## Esempio 1: consenti a un utente di eseguire Systems Manager operazioni in una singola regione

Il seguente esempio concede le autorizzazioni per eseguire le operazioni Systems Manager solo nella Regione Stati Uniti orientali (Ohio) (us-east-2).

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:*"
],
 "Resource": [
 "arn:aws:ssm:us-east-1:111122223333:*"
]
 }
]
}
```

## Esempio 2: permettere a un utente di elencare i documenti per una sola Regione

Nell'esempio seguente vengono concesse autorizzazioni per elencare tutti i nomi dei documenti che iniziano con **Update** nella Regione Stati Uniti orientali (Ohio) (us-east-2).

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:ListDocuments"
],
 "Resource": [
 "arn:aws:ssm:us-east-1:111122223333:document/Update*"
]
 }
]
}
```

```
}
]
}
```

Esempio 3: permettere a un utente di utilizzare un documento SSM specifico per eseguire comandi su nodi specifici

L'esempio seguente di policy IAM consente all'utente di effettuare le seguenti operazioni nella Regione Stati Uniti orientali (Ohio) (us-east-2):

- Elencare documenti Systems Manager (documenti SSM) e versioni di tali documenti.
- Visualizzare i dettagli sui documenti.
- Inviare un comando utilizzando il documento specificato nella policy. Il nome del documento è determinato dalla seguente voce:

```
arn:aws:ssm:us-east-2:aws-account-ID:document/Systems-Manager-document-name
```

- Inviare un comando a tre nodi. I nodi sono determinati dalle seguenti voci nella seconda sezione Resource.

```
"arn:aws:ec2:us-east-2:aws-account-ID:instance/i-02573cafcfEXAMPLE",
"arn:aws:ec2:us-east-2:aws-account-ID:instance/i-0471e04240EXAMPLE",
"arn:aws:ec2:us-east-2:aws-account-ID:instance/i-07782c72faEXAMPLE"
```

- Visualizzare i dettagli di un comando dopo che è stato inviato.
- Avviare e arrestare i flussi di lavoro in Automazione, uno strumento di AWS Systems Manager.
- Informazioni sui flussi di lavoro di Automazione.

Per concedere a un utente il permesso di utilizzare questo documento per inviare comandi su qualsiasi nodo a cui ha accesso, specifica una voce simile alla seguente nella Resource sezione. Rimuovete le altre voci del nodo. Questo esempio utilizza la regione Stati Uniti orientali (Ohio) (us-east-2).

```
"arn:aws:ec2:us-east-2:*:instance/*"
```

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Action": [
 "ssm:ListDocuments",
 "ssm:ListDocumentVersions",
 "ssm:DescribeDocument",
 "ssm:GetDocument",
 "ssm:DescribeInstanceInformation",
 "ssm:DescribeDocumentParameters",
 "ssm:DescribeInstanceProperties"
],
 "Effect": "Allow",
 "Resource": "*"
 },
 {
 "Action": "ssm:SendCommand",
 "Effect": "Allow",
 "Resource": [
 "arn:aws:ec2:us-east-1:111122223333:instance/i-02573cafcfEXAMPLE",
 "arn:aws:ec2:us-east-1:111122223333:instance/i-0471e04240EXAMPLE",
 "arn:aws:ec2:us-east-1:111122223333:instance/i-07782c72faEXAMPLE",
 "arn:aws:ssm:us-east-1:111122223333:document/Systems-Manager-document-name"
]
 },
 {
 "Action": [
 "ssm:CancelCommand",
 "ssm:ListCommands",
 "ssm:ListCommandInvocations"
],
 "Effect": "Allow",
 "Resource": "*"
 },
 {
```

```

 "Action": "ec2:DescribeInstanceStatus",
 "Effect": "Allow",
 "Resource": "*"
 },
 {
 "Action": "ssm:StartAutomationExecution",
 "Effect": "Allow",
 "Resource": [
 "arn:aws:ssm:us-east-1:111122223333:document/*",
 "arn:aws:ssm:us-east-1:111122223333:automation-execution/*"
]
 },
 {
 "Action": "ssm:DescribeAutomationExecutions",
 "Effect": "Allow",
 "Resource": [
 "*"
]
 },
 {
 "Action": [
 "ssm:StopAutomationExecution",
 "ssm:GetAutomationExecution"
],
 "Effect": "Allow",
 "Resource": [
 "*"
]
 }
]
}

```

## Visualizzazione Systems Manager documenti basati su tag

È possibile utilizzare le condizioni nella policy basata sulle identità per controllare l'accesso alle risorse di Systems Manager in base ai tag. Questo esempio mostra come creare una policy che consente di visualizzare un documento SSM. Tuttavia, l'autorizzazione viene concessa solo se il valore del tag del documento Owner è quello del nome utente. Questa policy concede anche le autorizzazioni necessarie per completare questa azione nella console.



## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "ListDocumentsInConsole",
 "Effect": "Allow",
 "Action": "ssm:ListDocuments",
 "Resource": "*"
 },
 {
 "Sid": "ViewDocumentIfOwner",
 "Effect": "Allow",
 "Action": "ssm:GetDocument",
 "Resource": "arn:aws:ssm:*:*:document/*",
 "Condition": {
 "StringEquals": {"ssm:ResourceTag/Owner": "${aws:username}"}
 }
 }
]
}
```

È possibile collegare questa policy agli utenti nell'account. Se un utente denominato `richard-roe` tenta di visualizzare un documento Systems Manager, il documento deve essere contrassegnato con `Owner=richard-roe` o `owner=richard-roe`. In caso contrario, l'accesso viene negato. La chiave di tag di condizione `Owner` corrisponde a `Owner` e `owner` perché i nomi delle chiavi di condizione non effettuano la distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta la sezione [Elementi delle policy JSON IAM: condizione](#) nella Guida per l'utente IAM.

## AWS politiche gestite per AWS Systems Manager

Una policy AWS gestita è una policy autonoma creata e amministrata da AWS. AWS le policy gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché sono disponibili per tutti i clienti. AWS Si consiglia pertanto di

ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una policy AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui la policy è associata. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

## Argomenti

- [AWS politica gestita: AmazonSSMServiceRolePolicy](#)
- [AWS politica gestita: AmazonSSMAutomationRole](#)
- [AWS politica gestita: AmazonSSMReadOnlyAccess](#)
- [AWS politica gestita: AWSSystemsManagerOpsDataSyncServiceRolePolicy](#)
- [AWS politica gestita: AmazonSSMManagedEC2InstanceDefaultPolicy](#)
- [AWS politica gestita: SSMQuickSetupRolePolicy](#)
- [AWS politica gestita: AWSQuickSetupDeploymentRolePolicy](#)
- [AWS policy gestita: AWSQuickSetupPatchPolicyDeploymentRolePolicy](#)
- [AWS politica gestita: AWSQuickSetupPatchPolicyBaselineAccess](#)
- [AWS politica gestita: AWSQuickSetupPatchPolicyLambdaExecutionPolicy](#)
- [AWS politica gestita: AWSQuickSetupPatchPolicyTagManagementExecutionPolicy](#)
- [AWS politica gestita: AWSSystemsManagerEnableExplorerExecutionPolicy](#)
- [AWS politica gestita: AWSSystemsManagerEnableConfigRecordingExecutionPolicy](#)
- [AWS politica gestita: AWSQuickSetupDevOpsGuruPermissionsBoundary](#)
- [AWS politica gestita: AWSQuickSetupDistributorPermissionsBoundary](#)
- [AWS politica gestita: AWSQuickSetupSSMHostMgmtPermissionsBoundary](#)
- [AWS politica gestita: AWSQuickSetupPatchPolicyPermissionsBoundary](#)
- [AWS politica gestita: AWSQuickSetupSchedulerPermissionsBoundary](#)
- [AWS politica gestita: AWSQuickSetupCFGCPacksPermissionsBoundary](#)

- [AWS politica gestita: AWSQuickSetupStartStopInstancesExecutionPolicy](#)
- [AWS politica gestita: AWSQuickSetupStartSSMAssociationsExecutionPolicy](#)
- [AWS politica gestita: AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy](#)
- [AWS politica gestita: AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy](#)
- [AWS policy gestita: AWS-SSM-RemediationAutomation-AdministrationRolePolicy](#)
- [AWS politica gestita: AWS-SSM-RemediationAutomation-ExecutionRolePolicy](#)
- [AWS policy gestita: AWSQuickSetupSSMManageResourcesExecutionPolicy](#)
- [AWS politica gestita: AWSQuickSetupSSMLifecycleManagementExecutionPolicy](#)
- [AWS politica gestita: AWSQuickSetupSSMDeploymentRolePolicy](#)
- [AWS politica gestita: AWSQuickSetupSSMDeploymentS3BucketRolePolicy](#)
- [AWS politica gestita: AWSQuickSetupEnableDHMCEExecutionPolicy](#)
- [AWS politica gestita: AWSQuickSetupEnableAREXExecutionPolicy](#)
- [AWS politica gestita: AWSQuickSetupManagedInstanceProfileExecutionPolicy](#)
- [AWS politica gestita: AWSQuickSetupManageJITNAResourcesExecutionPolicy](#)
- [AWS politica gestita: AWSQuickSetupJITNADeploymentRolePolicy](#)
- [AWS politica gestita: AWSSystemsManagerJustInTimeAccessServicePolicy](#)
- [AWS politica gestita: AWSSystemsManagerJustInTimeAccessTokenPolicy](#)
- [AWS politica gestita: AWSSystemsManagerJustInTimeAccessTokenSessionPolicy](#)
- [AWS politica gestita: AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy](#)
- [AWS politica gestita: AWSSystemsManagerNotificationsServicePolicy](#)
- [AWS politica gestita: AWS-SSM-Automation-DiagnosisBucketPolicy](#)
- [AWS politica gestita: AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy](#)
- [AWS politica gestita: AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy](#)
- [Systems Manager aggiornamenti a AWS policy gestite](#)
- [Polity gestite aggiuntive per Systems Manager](#)

## AWS politica gestita: AmazonSSMServiceRolePolicy

Questa politica fornisce l'accesso a diverse AWS risorse gestite AWS Systems Manager o utilizzate nelle operazioni di Systems Manager.

Non puoi collegarti AmazonSSMServiceRolePolicy alle tue entità AWS Identity and Access Management (IAM). Questa policy è associata a un ruolo collegato al servizio che consente di AWS Systems Manager eseguire azioni per tuo conto. Per ulteriori informazioni, consulta [Utilizzo dei ruoli per raccogliere l'inventario e visualizzare OpsData](#).

## Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **ssm:** consente alle entità principali di avviare e gestire le esecuzioni sia per Run Command che per la funzione Automazione, nonché di recuperare informazioni su Run Command e sulle operazioni di Automazione, recuperare informazioni sui calendari Change Calendar dei parametri Parameter Store, aggiornare e recuperare informazioni sulle impostazioni del servizio Systems Manager per le risorse OpsCenter e leggere informazioni sui tag applicati alle risorse.
- **cloudformation:** consente alle entità principali di recuperare informazioni sulle operazioni e le istanze dello stackset, eliminando gli stackset sulla risorsa `arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*`. Consente alle entità principali di eliminare le istanze dello stack associate alle seguenti risorse:

```
arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*
arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-SSM*:*
arn:aws:cloudformation:*:*:type/resource/*
```

- **cloudwatch**— Consente ai committenti di recuperare informazioni sugli allarmi Amazon CloudWatch

### Note

AmazonSSMServiceRolePolicyInclude l'autorizzazione.

`cloudwatch:DescribeAlarms` Tuttavia, Automation non utilizza più il ruolo collegato al servizio per il monitoraggio degli CloudWatch allarmi. Questa operazione ora utilizza l'identità di esecuzione del runbook.

- **compute-optimizer**— Consente ai principali di recuperare lo stato di iscrizione (opt-in) di un account al AWS Compute Optimizer servizio e di recuperare i consigli per le istanze Amazon EC2 che soddisfano una serie specifica di requisiti dichiarati.
- **config**— Consente ai principali di recuperare le configurazioni di riparazione delle informazioni e i registratori di configurazione in AWS Config e di determinare se le regole e le risorse specificate sono conformi. AWS Config AWS

- **events**— Consente ai responsabili di recuperare informazioni sulle EventBridge regole, di creare EventBridge regole e destinazioni esclusivamente per il servizio Systems Manager (`ssm.amazonaws.com`) e di eliminare regole e destinazioni per la risorsa `arn:aws:events:*:*:rule/SSMExplorerManagedRule`.
- **ec2**: consente alle entità principali di recuperare informazioni sulle istanze Amazon EC2.
- **iam**: consente alle entità principali di assegnare le autorizzazioni ai ruoli per il servizio Systems Manager (`ssm.amazonaws.com`).
- **lambda**: consente alle entità principali di richiamare funzioni Lambda configurate specificamente per l'utilizzo da parte di Systems Manager.
- **resource-explorer-2**— Consente ai responsabili di recuperare i dati sulle istanze EC2 per determinare se ciascuna istanza è attualmente gestita da Systems Manager.

L'azione `resource-explorer-2:CreateManagedView` è consentita per la risorsa `arn:aws:resource-explorer-2:*:*:managed-view/AWSManagedViewForSSM*`.

- **resource-groups**— Consente ai principali di recuperare i gruppi di risorse dell'elenco e i relativi membri dalle risorse che appartengono a un gruppo AWS Resource Groups di risorse.
- **securityhub**— Consente ai principali di recuperare informazioni sulle risorse dell' AWS Security Hub CSPM hub nell'account corrente.
- **states**— Consente ai principali di avviare e recuperare informazioni configurate specificamente per AWS Step Functions l'uso da parte di Systems Manager.
- **support**: consente alle entità principali di recuperare informazioni su controlli e casi in AWS Trusted Advisor.
- **tag**: consente alle entità principali di recuperare informazioni su tutte le risorse contrassegnate o precedentemente contrassegnate che si trovano in una determinata Regione AWS su un account.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AmazonSSMServiceRolePolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AmazonSSMAutomationRole

È possibile allegare la policy `AmazonSSMAutomationRole` alle identità IAM. Questa policy fornisce le autorizzazioni per il servizio AWS Systems Manager Automation per eseguire le attività definite nei runbook di Automation.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **lambda**: consente alle entità principali di richiamare funzioni Lambda con nomi che iniziano con "Automazione". Ciò è necessario affinché i runbook di Automazione eseguano le funzioni Lambda come parte del loro flusso di lavoro.
- **ec2**: consente alle entità principali di eseguire varie operazioni di Amazon EC2, tra cui la creazione, la copia e l'annullamento della registrazione di immagini, la gestione delle istantanee, l'avvio, l'esecuzione, l'arresto e la chiusura delle istanze terminali, la gestione dello stato delle istanze e la creazione, l'eliminazione e la descrizione dei tag. Queste autorizzazioni consentono ai runbook di Automazione di gestire le risorse Amazon EC2 durante l'esecuzione.
- **cloudformation**— Consente ai principali di creare, descrivere, aggiornare ed eliminare gli stack. CloudFormation. Ciò consente ai runbook di Automazione di gestire l'infrastruttura tramite codice. CloudFormation
- **ssm**: consente alle entità principali di utilizzare tutte le operazioni di Systems Manager. Questo accesso completo è necessario per consentire ai runbook di Automazione di interagire con tutte le funzionalità di Systems Manager.
- **sns**: consente alle entità principali di pubblicare messaggi su argomenti di Amazon SNS con nomi che iniziano con "Automazione". Ciò consente ai runbook di Automazione di inviare notifiche durante l'esecuzione.
- **ssmmessages**: consente alle entità principali di aprire i canali di dati alle sessioni di Systems Manager. Ciò consente ai runbook di Automazione di stabilire canali di comunicazione per le operazioni basate sulle sessioni.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AmazonSSMAutomationRole](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AmazonSSMReadOnlyAccess

È possibile allegare la policy `AmazonSSMReadOnlyAccess` alle identità IAM. Questa politica garantisce l'accesso in sola lettura alle operazioni AWS Systems Manager `APIDescribe*`, tra cui, `eGet*.List*`

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AmazonSSMReadOnlyAccess](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSSystemsManagerOpsDataSyncServiceRolePolicy

Non è possibile collegare AWSSystemsManagerOpsDataSyncServiceRolePolicy alle entità IAM. Questa policy è associata a un ruolo collegato ai servizi che consente a Systems Manager di eseguire operazioni per tuo conto. Per ulteriori informazioni, consulta [Usare i ruoli per creare OpsData e OpsItems per Explorer](#).

AWSSystemsManagerOpsDataSyncServiceRolePolicy consente al ruolo AWSServiceRoleForSystemsManagerOpsDataSync collegato al servizio di creare OpsItems e OpsData aggiornare i risultati. AWS Security Hub CSPM

La policy consente a Systems Manager di eseguire le seguenti operazioni su tutte le risorse correlate ("Resource": "\*"), tranne dove indicato:

- ssm:GetOpsItem [1]
- ssm:UpdateOpsItem [1]
- ssm:CreateOpsItem
- ssm:AddTagsToResource [2]
- ssm:UpdateServiceSetting [3]
- ssm:GetServiceSetting [3]
- securityhub:GetFindings
- securityhub:GetFindings
- securityhub:BatchUpdateFindings [4]

[1] Le operazioni ssm:GetOpsItem e ssm:UpdateOpsItem sono autorizzazioni consentite dalla seguente condizione solo per il servizio Systems Manager.

```
"Condition": {
 "StringEquals": {
 "aws:ResourceTag/ExplorerSecurityHubOpsItem": "true"
 }
}
```

[2] L'operazione ssm:AddTagsToResource è un'autorizzazione consentita solo per la seguente risorsa.

```
arn:aws:ssm:*:*:opsitem/*
```

[3] Le operazioni `ssm:UpdateServiceSetting` e `ssm:GetServiceSetting` sono autorizzazioni consentite solo per le seguenti risorse.

```
arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*
arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*
```

[4] Gli `securityhub:BatchUpdateFindings` sono autorizzazioni concesse dalla seguente condizione solo per il servizio di Systems Manager.

```
{
 "Effect": "Deny",
 "Action": "securityhub:BatchUpdateFindings",
 "Resource": "*",
 "Condition": {
 "StringEquals": {
 "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
 }
 }
},
{
 "Effect": "Deny",
 "Action": "securityhub:BatchUpdateFindings",
 "Resource": "*",
 "Condition": {
 "Null": {
 "securityhub:ASFFSyntaxPath/Confidence": false
 }
 }
},
{
 "Effect": "Deny",
 "Action": "securityhub:BatchUpdateFindings",
 "Resource": "*",
 "Condition": {
 "Null": {
 "securityhub:ASFFSyntaxPath/Criticality": false
 }
 }
},
{
 "Effect": "Deny",
 "Action": "securityhub:BatchUpdateFindings",
 "Resource": "*",
```



```
"Condition": {
 "Null": {
 "securityhub:ASFFSyntaxPath/Note.Text": false
 }
},
{
 "Effect": "Deny",
 "Action": "securityhub:BatchUpdateFindings",
 "Resource": "*",
 "Condition": {
 "Null": {
 "securityhub:ASFFSyntaxPath/Note.UpdatedBy": false
 }
 }
},
{
 "Effect": "Deny",
 "Action": "securityhub:BatchUpdateFindings",
 "Resource": "*",
 "Condition": {
 "Null": {
 "securityhub:ASFFSyntaxPath/RelatedFindings": false
 }
 }
},
{
 "Effect": "Deny",
 "Action": "securityhub:BatchUpdateFindings",
 "Resource": "*",
 "Condition": {
 "Null": {
 "securityhub:ASFFSyntaxPath/Types": false
 }
 }
},
{
 "Effect": "Deny",
 "Action": "securityhub:BatchUpdateFindings",
 "Resource": "*",
 "Condition": {
 "Null": {
 "securityhub:ASFFSyntaxPath/UserDefinedFields.key": false
 }
 }
}
```

```
}
},
{
 "Effect": "Deny",
 "Action": "securityhub:BatchUpdateFindings",
 "Resource": "*",
 "Condition": {
 "Null": {
 "securityhub:ASFFSyntaxPath/UserDefinedFields.value": false
 }
 }
},
{
 "Effect": "Deny",
 "Action": "securityhub:BatchUpdateFindings",
 "Resource": "*",
 "Condition": {
 "Null": {
 "securityhub:ASFFSyntaxPath/VerificationState": false
 }
 }
}
```

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSSystemsManagerOpsDataSyncServiceRolePolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AmazonSSMManagedEC2InstanceDefaultPolicy

È necessario collegare AmazonSSMManagedEC2InstanceDefaultPolicy ai ruoli IAM solo per le istanze Amazon EC2 per le quali si ha l'autorizzazione per utilizzare le funzionalità Systems Manager. Non è consigliabile associare questo ruolo ad altre entità IAM, come utenti IAM e gruppi IAM, o a ruoli IAM che servono ad altri scopi. Per ulteriori informazioni, consulta [Gestione automatica delle istanze EC2 con la configurazione di gestione host predefinita](#).

Questa policy concede autorizzazioni che consentono SSM Agent alla tua istanza Amazon EC2 di comunicare con il servizio Systems Manager nel cloud per eseguire una serie di attività. Concede inoltre le autorizzazioni per i due servizi che forniscono token di autorizzazione per garantire che le operazioni vengano eseguite sull'istanza corretta.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **ssm**: consente alle entità principali di recuperare documenti, eseguire comandi utilizzando Run Command, stabilire sessioni con Session Manager, raccogliere un inventario d'istanza ed eseguire la scansione delle patch e della loro conformità tramite Patch Manager.
- **ssmmessages**: consente alle entità principali di accedere, per ogni istanza, a un token di autorizzazione personalizzato creato da [Amazon Message Gateway Service](#). Systems Manager convalida il token di autorizzazione personalizzato rispetto al nome della risorsa Amazon (ARN) dell'istanza che era stato fornito nell'operazione API. Questo accesso è necessario per assicurarsi che SSM Agent esegua le operazioni API sull'istanza corretta.
- **ec2messages**: consente alle entità principali di accedere, per ogni istanza, a un token di autorizzazione personalizzato creato da [Amazon Message Delivery Service](#). Systems Manager convalida il token di autorizzazione personalizzato rispetto al nome della risorsa Amazon (ARN) dell'istanza che era stato fornito nell'operazione API. Questo accesso è necessario per assicurarsi che SSM Agent esegua le operazioni API sull'istanza corretta.

Per informazioni correlate sugli endpoint **ssmmessages** e **ec2messages**, incluse le differenze tra i due, consulta [Agent-related Operazioni API \(endpoint ssmessages ed ec2messages\)](#).

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AmazonSSMManagedEC2InstanceDefaultPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: SSMQuickSetupRolePolicy

Non puoi collegarti SSMQuickSetupRolePolicy alle tue entità IAM. Questa policy è associata a un ruolo collegato ai servizi che consente a Systems Manager di eseguire operazioni per tuo conto. Per ulteriori informazioni, consulta [Utilizzo dei ruoli per mantenere l'integrità e la coerenza delle risorse fornite da Quick Setup](#).

Questa policy concede autorizzazioni di sola lettura che consentono a Systems Manager di verificare lo stato della configurazione, garantire l'uso coerente dei parametri e delle risorse assegnate e correggere le risorse quando viene rilevata una deviazione. Inoltre, concede autorizzazioni amministrative per creare un ruolo collegato ai servizi.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ssm`: consente alle entità principali di leggere le informazioni Resource Data Syncs e i documenti SSM in Systems Manager, inclusi gli account degli amministratori delegati. Questo viene richiesto in modo che Quick Setup determini lo stato in cui è necessario che si trovino le risorse configurate.
- `organizations`: consente alle entità responsabili di leggere le informazioni sugli account dei membri che appartengono a un'organizzazione, come configurato in AWS Organizations. Ciò è necessario per far sì che Quick Setup identifichi tutti gli account di un'organizzazione in cui vanno eseguiti i controlli sullo stato delle risorse.
- `cloudformation`— Consente ai presidi di leggere informazioni da CloudFormation. Ciò è necessario per Quick Setup raccogliere dati sugli CloudFormation stack utilizzati per gestire lo stato delle risorse e le operazioni degli CloudFormation stackset.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [SSMQuickSetupRolePolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSQuickSetupDeploymentRolePolicy

La policy gestita AWSQuickSetupDeploymentRolePolicy supporta diversi tipi di configurazione Quick Setup. Questi tipi di configurazione creano ruoli e automazioni IAM che configurano i servizi e le funzionalità di Amazon Web Services utilizzati di frequente con le best practice consigliate.

È possibile collegare AWSQuickSetupDeploymentRolePolicy alle entità IAM.

Questa policy concede le autorizzazioni amministrative necessarie per creare risorse associate alle seguenti configurazioni di Quick Setup:

- [Configura la gestione degli host di Amazon EC2 utilizzando Configurazione rapida](#)
- [Crea un AWS Config registratore di configurazione utilizzando Configurazione rapida](#)
- [Implementazione AWS Config pacchetto di conformità utilizzando Configurazione rapida](#)
- [Configura DevOps Guru usando Configurazione rapida](#)
- [Implementa i pacchetti Distributor tramite Quick Setup](#)
- [Arresta e avvia automaticamente le istanze EC2 in base a una pianificazione utilizzando Configurazione rapida](#)

## Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **ssm**— Consente ai committenti di leggere, creare, aggiornare ed eliminare documenti SSM con nomi che iniziano con "AWSQuickSetup-» o "AWSOperationsPack-» quando vengono richiamati CloudFormation; di leggere documenti di AWS proprietà specifici, tra cui "AWSQuickSetupType-ManagedInstanceProfile«, "AWSQuickSetupType-ConfigureDevOpsGuru e "AWSQuickSetupType-DeployConformancePack«; di creare, aggiornare ed eliminare associazioni per Quick Setup documenti e documenti di AWS proprietà quando vengono richiamati CloudFormation; e di ripulire le risorse precedenti contrassegnate con. QuickSetupID Ciò consente a Quick Setup di implementare e gestire flussi di lavoro e associazioni di automazione.
- **cloudformation**— Consente ai principali di leggere informazioni su CloudFormation stack e stack set e di creare, aggiornare ed eliminare CloudFormation stack e modificare set per le risorse i cui nomi iniziano con "StackSet-AWS-QuickSetup-». Ciò consente a Quick Setup di gestire le implementazioni dell'infrastruttura tra account e Regioni.
- **config**— AWS Config Consente ai direttori di leggere le informazioni sui pacchetti di conformità e sul loro stato e di creare ed eliminare i pacchetti di conformità i cui nomi iniziano con "-» quando vengono richiamati. AWS-QuickSetup CloudFormation Ciò consente a Quick Setup di implementare configurazioni di monitoraggio della conformità.
- **events**— Consente ai committenti di gestire EventBridge regole e destinazioni per le risorse i cui nomi contengono "-». QuickSetup Ciò consente a Quick Setup di creare flussi di lavoro di automazione pianificati.
- **iam**— Consente ai principali di creare ruoli collegati ai servizi per Systems Manager AWS Config e Systems Manager; di creare, gestire ed eliminare ruoli IAM con nomi che iniziano con "AWS-QuickSetup-» o "AWSOperationsPack-» quando vengono chiamati CloudFormation; di passare questi ruoli a Systems Manager e ai EventBridge servizi; di allegare policy AWS gestite specifiche a questi ruoli e di impostare i limiti delle autorizzazioni utilizzando politiche gestite specifiche. Quick Setup Ciò consente a Quick Setup di creare i ruoli di servizio necessari per le sue operazioni.
- **resource-groups**: consente alle entità principali di recuperare le query relative ai gruppi di risorse. Ciò consente a Quick Setup di indirizzare set specifici di risorse per la gestione della configurazione.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupDeploymentRolePolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS policy gestita: AWSQuickSetupPatchPolicyDeploymentRolePolicy

La policy gestita AWSQuickSetupPatchPolicyDeploymentRolePolicy supporta il tipo [Configurare l'applicazione di patch per le istanze in un'organizzazione utilizzando un Configurazione rapida politica sulle patch](#) di Quick Setup. Questo tipo di configurazione consente di automatizzare l'applicazione di patch alle applicazioni e ai nodi in un singolo account o in tutta l'organizzazione.

È anche possibile collegare AWSQuickSetupPatchPolicyDeploymentRolePolicy alle entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni per conto dell'utente.

Questa policy concede autorizzazioni amministrative che consentono a Quick Setup di creare risorse associate a una configurazione della policy di patch.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `iam`: consente alle entità principali di gestire ed eliminare i ruoli IAM necessari per le attività di configurazione dell'automazione e di gestire le politiche dei ruoli di automazione.
- `cloudformation`— Consente ai principali di leggere le informazioni sugli CloudFormation stack e di controllare CloudFormation gli stack creati Quick Setup utilizzando set di CloudFormation stack.
- `ssm`: consente alle entità principali di creare, aggiornare, leggere ed eliminare i runbook di Automazione necessari per le attività di configurazione, nonché di creare, aggiornare ed eliminare le associazioni di State Manager.
- `resource-groups`: consente alle entità principali di recuperare le query relative alle risorse associate ai gruppi di risorse destinate alle configurazioni di Quick Setup.
- `s3`: consente alle entità principali di elencare i bucket Amazon S3 e di gestire i bucket per l'archiviazione dei log di accesso alle policy di patch.
- `lambda`— Consente ai responsabili di gestire le funzioni di AWS Lambda riparazione che mantengono le configurazioni nello stato corretto.
- `logs`: consente alle entità principali di descrivere e gestire gruppi di log per le risorse di configurazione Lambda.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupPatchPolicyDeploymentRolePolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSQuickSetupPatchPolicyBaselineAccess

La policy gestita AWSQuickSetupPatchPolicyBaselineAccess supporta il tipo [Configurare l'applicazione di patch per le istanze in un'organizzazione utilizzando un Configurazione rapida politica sulle patch](#) di Quick Setup. Questo tipo di configurazione consente di automatizzare l'applicazione di patch alle applicazioni e ai nodi in un singolo account o in tutta l'organizzazione.

È anche possibile collegare AWSQuickSetupPatchPolicyBaselineAccess alle entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni per conto dell'utente.

Questa policy fornisce autorizzazioni di sola lettura per accedere alle baseline delle patch che sono state configurate da un amministratore nella versione corrente o nell'organizzazione che la utilizza. Account AWS Quick Setup Le baseline delle patch sono archiviate in un bucket Amazon S3 e vengono utilizzate per l'applicazione di patch a istanze in un singolo account o in un'intera organizzazione.

### Dettagli delle autorizzazioni

Questa policy include la seguente autorizzazione.

- s3: consente alle entità principali di leggere le sostituzioni alla baseline delle patch archiviata nei bucket di Amazon S3.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupPatchPolicyBaselineAccess](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSQuickSetupPatchPolicyLambdaExecutionPolicy

La policy gestita AWSQuickSetupPatchPolicyLambdaExecutionPolicy supporta il tipo [Configurare l'applicazione di patch per le istanze in un'organizzazione utilizzando un Configurazione rapida politica sulle patch](#) di Quick Setup. Questo tipo di configurazione consente di automatizzare l'applicazione di patch alle applicazioni e ai nodi in un singolo account o in tutta l'organizzazione.

È anche possibile collegare `AWSQuickSetupPatchPolicyLambdaExecutionPolicy` alle entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni per conto dell'utente.

Questa politica concede le autorizzazioni per gestire le associazioni di State Manager per le operazioni di pulizia automatiche quando le configurazioni Quick Setup vengono eliminate.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ssm`— Consente ai principali di interrogare e aggiornare le associazioni di State Manager in base all'ID durante le operazioni di pulizia automatiche. La policy concede le autorizzazioni per descrivere i dettagli dell'associazione, visualizzare la cronologia di esecuzione dell'associazione e aggiornare le configurazioni delle associazioni. Le risorse Wildcard sono necessarie perché gli ARN di associazione vengono generati dinamicamente.
- `iam`— Consente ai responsabili di passare i ruoli di automazione a Systems Manager per le operazioni di associazione. L'autorizzazione è limitata ai ruoli di automazione di Quick Setup con il modello `AWS-QuickSetup-AutomationRole-*` e include una condizione che limita il passaggio dei ruoli solo al servizio Systems Manager.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupPatchPolicyLambdaExecutionPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

### AWS politica gestita: `AWSQuickSetupPatchPolicyTagManagementExecutionPolicy`

La policy gestita `AWSQuickSetupPatchPolicyTagManagementExecutionPolicy` supporta il tipo [Configurare l'applicazione di patch per le istanze in un'organizzazione utilizzando un Configurazione rapida politica sulle patch](#) di Quick Setup. Questo tipo di configurazione consente di automatizzare l'applicazione di patch alle applicazioni e ai nodi in un singolo account o in tutta l'organizzazione.

È anche possibile collegare `AWSQuickSetupPatchPolicyTagManagementExecutionPolicy` alle entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni per conto dell'utente.

Questa policy concede le autorizzazioni per tenere traccia delle istanze gestite dalle configurazioni delle policy di Quick Setup patch tramite l'etichettatura automatica e la raccolta dell'inventario.



## Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **ssm**— Consente ai principali di recuperare le informazioni di inventario dalle istanze gestite e di aggiungere o rimuovere tag di tracciamento della configurazione sulle istanze gestite da SSM.
- **ec2**— Consente ai principali di aggiungere o rimuovere tag di tracciamento della configurazione sulle istanze Amazon EC2.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupPatchPolicyTagManagementExecutionPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: **AWSSystemsManagerEnableExplorerExecutionPolicy**

La policy gestita **AWSSystemsManagerEnableExplorerExecutionPolicy** supporta l'abilitazione Explorer, uno strumento in AWS Systems Manager.

È anche possibile collegare **AWSSystemsManagerEnableExplorerExecutionPolicy** alle entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni per conto dell'utente.

Questa policy concede autorizzazioni amministrative per l'attivazione di Explorer. Ciò include le autorizzazioni per aggiornare le impostazioni del relativo servizio di Systems Manager, creando un ruolo collegato al servizio per Systems Manager.

## Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **config**: consente alle entità principali di contribuire all'abilitazione di Explorer, fornendo un accesso in sola lettura ai dettagli del registratore di configurazione.
- **iam**: consente alle entità principali di aiutare ad abilitare Explorer.
- **ssm**: consente alle entità principali di avviare un flusso di lavoro di automazione che abiliti Explorer.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSSystemsManagerEnableExplorerExecutionPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

AWS politica gestita:

## **AWSSystemsManagerEnableConfigRecordingExecutionPolicy**

La policy gestita `AWSSystemsManagerEnableConfigRecordingExecutionPolicy` supporta il tipo di configurazione [Crea un AWS Config registratore di configurazione utilizzando Configurazione rapida](#) di Quick Setup . Questo tipo di configurazione Quick Setup consente di tenere traccia e registrare le modifiche ai tipi di AWS risorse scelti AWS Config. Consente inoltre a Quick Setup di configurare le opzioni di consegna e notifica per i dati registrati.

È anche possibile collegare `AWSSystemsManagerEnableConfigRecordingExecutionPolicy` alle entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni per conto dell'utente.

Questa politica concede autorizzazioni amministrative che consentono di abilitare e configurare Quick Setup la registrazione AWS Config della configurazione.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `s3`: consente alle entità principali di creare e configurare bucket Amazon S3 per la consegna delle registrazioni di configurazione.
- `sns`: consente alle entità principali di elencare e creare argomenti di Amazon SNS.
- `config`: consente alle entità principali di configurare e avviare il registratore di configurazione e di contribuire all'abilitazione di Explorer.
- `iam`— Consente ai responsabili di creare, ottenere e passare un ruolo collegato al servizio per AWS Config; di creare un ruolo collegato al servizio per Systems Manager; e di contribuire all'abilitazione. Explorer
- `ssm`: consente alle entità principali di avviare un flusso di lavoro di automazione che abiliti Explorer.
- `compute-optimizer`— Consente ai responsabili di agevolare l'abilitazione Explorer fornendo un accesso in sola lettura per determinare se una risorsa è iscritta. AWS Compute Optimizer
- `support`: consente alle entità principali di contribuire all'abilitazione di Explorer, fornendo un accesso in sola lettura per determinare se una risorsa è registrata a AWS Compute Optimizer.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSSystemsManagerEnableConfigRecordingExecutionPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSQuickSetupDevOpsGuruPermissionsBoundary

### Note

Questa politica rappresenta un limite delle autorizzazioni. Un limite delle autorizzazioni imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Non è necessario utilizzare e collegare autonomamente le policy relative al limite delle autorizzazioni di Quick Setup. Le policy relative al limite delle autorizzazioni di Quick Setup vanno allegate solo ai ruoli gestiti da Quick Setup. Per maggiori informazioni sui limiti delle autorizzazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.

La policy gestita AWSQuickSetupDevOpsGuruPermissionsBoundary supporta il tipo [Configura DevOps Guru usando Configurazione rapida](#). Il tipo di configurazione abilita Amazon Guru basato sull'apprendimento automatico. DevOps Il servizio DevOps Guru può contribuire a migliorare le prestazioni operative e la disponibilità di un'applicazione.

Quando crei una configurazione AWSQuickSetupDevOpsGuruPermissionsBoundary utilizzando Quick Setup, il sistema applica questo limite delle autorizzazioni ai ruoli IAM creati durante l'implementazione della configurazione. Il limite delle autorizzazioni limita l'ambito dei ruoli creati da Quick Setup.

Questa policy concede autorizzazioni amministrative che consentono di abilitare e configurare Quick Setup Amazon Guru. DevOps

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `iam`— Consente ai principali di creare ruoli collegati ai servizi per DevOps Guru e Systems Manager e di elencare i ruoli che aiutano ad abilitare. Explorer
- `cloudformation`: consente alle entità principali di elencare e descrivere gli stack CloudFormation .
- `sns`: consente alle entità principali di elencare e creare argomenti di Amazon SNS.
- `devops-guru`— Consente ai presidi di configurare DevOps Guru e di aggiungere un canale di notifica.

- `config`: consente alle entità principali di contribuire all'abilitazione di Explorer, fornendo un accesso in sola lettura ai dettagli del registratore di configurazione.
- `ssm`: consente alle entità principali di avviare un flusso di lavoro di automazione che abiliti Explorer, nonché di leggere e aggiornare le impostazioni del servizio Explorer.
- `compute-optimizer`— Consente ai principali di agevolare l'attivazione Explorer fornendo un accesso in sola lettura per determinare se una risorsa è iscritta. AWS Compute Optimizer
- `support`: consente alle entità principali di contribuire all'abilitazione di Explorer, fornendo un accesso in sola lettura per determinare se una risorsa è registrata a AWS Compute Optimizer.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupDevOpsGuruPermissionsBoundary](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSQuickSetupDistributorPermissionsBoundary

### Note

Questa politica rappresenta un limite delle autorizzazioni. Un limite delle autorizzazioni imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Non è necessario utilizzare e collegare autonomamente le policy relative al limite delle autorizzazioni di Quick Setup. Le policy relative al limite delle autorizzazioni di Quick Setup vanno allegate solo ai ruoli gestiti da Quick Setup. Per maggiori informazioni sui limiti delle autorizzazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.

La policy gestita AWSQuickSetupDistributorPermissionsBoundary supporta il tipo di configurazione [Implementa i pacchetti Distributor tramite Quick Setup](#) di Quick Setup . Il tipo di configurazione contribuisce ad abilitare la distribuzione di pacchetti software, ad esempio agenti, alle istanze Amazon Elastic Compute Cloud (Amazon EC2), utilizzando Distributor, uno strumento di AWS Systems Manager.

Quando crei una configurazione AWSQuickSetupDistributorPermissionsBoundary utilizzando Quick Setup, il sistema applica questo limite delle autorizzazioni ai ruoli IAM creati durante l'implementazione della configurazione. Il limite delle autorizzazioni limita l'ambito dei ruoli creati da Quick Setup.

Questa politica concede autorizzazioni amministrative che consentono a Quick Setup di abilitare la distribuzione di pacchetti software, come agenti, alle istanze Amazon EC2 utilizzando Distributor.

## Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `iam`: consente alle entità principali di ottenere e passare il ruolo di automazione del Distributore; di creare, leggere, aggiornare ed eliminare il ruolo dell'istanza predefinito; di passare il ruolo dell'istanza predefinito ad Amazon EC2 e Systems Manager; di associare policy di gestione delle istanze ai ruoli dell'istanza; di creare un ruolo collegato ai servizi per Systems Manager; di aggiungere il ruolo dell'istanza predefinito ai profili dell'istanza; di leggere informazioni sui ruoli IAM e sui profili dell'istanza, nonché di creare il profilo dell'istanza predefinito.
- `ec2`: consente alle entità principali di associare il profilo dell'istanza predefinito alle istanze EC2 e di contribuire all'abilitazione di Explorer.
- `ssm`: consente alle entità principali di avviare i flussi di lavoro di automazione, vale a dire quelli che configurano le istanze e installano i pacchetti, nonché di contribuire ad avviare il flusso di lavoro di automazione che abilita Explorer, leggendo e aggiornando le impostazioni del servizio Explorer.
- `config`: consente alle entità principali di contribuire all'abilitazione di Explorer, fornendo un accesso in sola lettura ai dettagli del registratore di configurazione.
- `compute-optimizer`— Consente ai principali di contribuire all'abilitazione Explorer fornendo un accesso in sola lettura per determinare se una risorsa è iscritta. AWS Compute Optimizer
- `support`: consente alle entità principali di contribuire all'abilitazione di Explorer, fornendo un accesso in sola lettura per determinare se una risorsa è registrata a AWS Compute Optimizer.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupDistributorPermissionsBoundary](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSQuickSetupSSMHostMgmtPermissionsBoundary

### Note

Questa politica rappresenta un limite delle autorizzazioni. Un limite delle autorizzazioni imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Non è necessario utilizzare e collegare autonomamente le policy relative al limite delle autorizzazioni di Quick Setup. Le policy relative al limite delle

autorizzazioni di Quick Setup vanno allegate solo ai ruoli gestiti da Quick Setup. Per maggiori informazioni sui limiti delle autorizzazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.

La policy gestita `AWSQuickSetupSSMHostMgmtPermissionsBoundary` supporta il tipo di configurazione [Configura la gestione degli host di Amazon EC2 utilizzando Configurazione rapida](#) di Quick Setup. Questo tipo di configurazione configura i ruoli IAM e abilita gli strumenti di Systems Manager di uso comune per gestire in modo sicuro le istanze Amazon EC2.

Quando crei una configurazione `AWSQuickSetupSSMHostMgmtPermissionsBoundary` utilizzando Quick Setup, il sistema applica questo limite delle autorizzazioni ai ruoli IAM creati durante l'implementazione della configurazione. Il limite delle autorizzazioni limita l'ambito dei ruoli creati da Quick Setup.

Questa policy concede autorizzazioni amministrative che consentono a Quick Setup di abilitare e configurare gli strumenti di Systems Manager necessari per la gestione sicura delle istanze EC2.

#### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `iam`: consente alle entità principali di ottenere e trasferire il ruolo di servizio all'automazione. Consente alle entità principali di creare, leggere, aggiornare ed eliminare il ruolo dell'istanza predefinito; di passare il ruolo dell'istanza predefinito ad Amazon EC2 e Systems Manager; di associare policy di gestione delle istanze ai ruoli dell'istanza; di creare un ruolo collegato ai servizi per Systems Manager; di aggiungere il ruolo dell'istanza predefinito ai profili dell'istanza; di leggere informazioni sui ruoli IAM e sui profili dell'istanza, nonché di creare il profilo dell'istanza predefinito.
- `ec2`: consente alle entità principali di associare e dissociare il profilo dell'istanza predefinito con le istanze EC2.
- `ssm`: consente alle entità principali di avviare flussi di lavoro di Automazione che attivano Explorer; di leggere e aggiornare le impostazioni del servizio Explorer; di configurare le istanze; di abilitare gli strumenti di Systems Manager sulle istanze.
- `compute-optimizer`— Consente ai principali di contribuire all'abilitazione Explorer fornendo un accesso in sola lettura per determinare se una risorsa è iscritta. AWS Compute Optimizer
- `support`: consente alle entità principali di contribuire all'abilitazione di Explorer, fornendo un accesso in sola lettura per determinare se una risorsa è registrata a AWS Compute Optimizer.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupSSMHostMgmtPermissionsBoundary](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSQuickSetupPatchPolicyPermissionsBoundary

### Note

Questa politica rappresenta un limite delle autorizzazioni. Un limite delle autorizzazioni imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Non è necessario utilizzare e collegare autonomamente le policy relative al limite delle autorizzazioni di Quick Setup. Le policy relative al limite delle autorizzazioni di Quick Setup vanno allegate solo ai ruoli gestiti da Quick Setup. Per maggiori informazioni sui limiti delle autorizzazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.

La policy gestita AWSQuickSetupPatchPolicyPermissionsBoundary supporta il tipo [Configurare l'applicazione di patch per le istanze in un'organizzazione utilizzando un Configurazione rapida politica sulle patch](#) di Quick Setup. Questo tipo di configurazione consente di automatizzare l'applicazione di patch alle applicazioni e ai nodi in un singolo account o in tutta l'organizzazione.

Quando crei una configurazione AWSQuickSetupPatchPolicyPermissionsBoundary utilizzando Quick Setup, il sistema applica questo limite delle autorizzazioni ai ruoli IAM creati durante l'implementazione della configurazione. Il limite delle autorizzazioni limita l'ambito dei ruoli creati da Quick Setup.

Questa policy concede autorizzazioni amministrative che consentono a Quick Setup di abilitare e configurare le policy di patch in Patch Manager, uno strumento di AWS Systems Manager.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **iam**— Consente ai principali di ottenere il ruolo di Patch Manager automazione; di passare i ruoli di automazione alle operazioni di Patch Manager patching; di creare il ruolo di istanza predefinito AmazonSSMRoleForInstancesQuickSetup; di passare il ruolo di istanza predefinito ad Amazon EC2 e Systems Manager; di allegare policy AWS gestite selezionate al ruolo di istanza; di creare un ruolo collegato ai servizi per Systems Manager; di aggiungere il ruolo di istanza

predefinito ai profili di istanza; di leggere informazioni sui profili e sui ruoli dell'istanza; di creare un profilo di istanza predefinito; e di etichettare i ruoli che hanno per missioni da leggere la baseline della patch sostituisce.

- **ssm**: consente alle entità principali di aggiornare il ruolo dell'istanza gestito da Systems Manager; di gestire le associazioni create da policy di patch di Patch Manager create in Quick Setup; di etichettare le istanze destinate a una configurazione di policy di patch; di leggere informazioni sulle istanze e sullo stato delle patch; di avviare flussi di lavoro di automazione che configurano, abilitano e correggono l'applicazione di patch alle istanze; di avviare flussi di lavoro di automazione che abilitino Explorer; di contribuire all'abilitazione di Explorer, nonché di leggere e aggiornare le impostazioni del servizio Explorer.
- **ec2**: consente alle entità principali di associare e dissociare il profilo dell'istanza predefinito con le istanze EC2, di etichettare le istanze destinate a una configurazione di policy di patch, di etichettare le istanze destinate a una configurazione di policy di patch e di contribuire all'abilitazione di Explorer.
- **s3**: consente alle entità principali di creare e configurare bucket S3 per archiviare le modifiche della baseline delle patch.
- **lambda**— Consente ai principali di richiamare AWS Lambda le funzioni che configurano l'applicazione delle patch e di eseguire operazioni di pulizia dopo l'eliminazione della configurazione di una policy sulle patch. Quick Setup
- **logs**— Consente ai responsabili di configurare la registrazione delle funzioni. Patch Manager Quick Setup AWS Lambda
- **config**: consente alle entità principali di contribuire all'abilitazione di Explorer, fornendo un accesso in sola lettura ai dettagli del registratore di configurazione.
- **compute-optimizer**— Consente ai principali di agevolare l'abilitazione Explorer fornendo un accesso di sola lettura per determinare se una risorsa è iscritta. AWS Compute Optimizer
- **support**: consente alle entità principali di contribuire all'abilitazione di Explorer, fornendo un accesso in sola lettura per determinare se una risorsa è registrata a AWS Compute Optimizer.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupPatchPolicyPermissionsBoundary](#) nella Guida di riferimento alle policy gestite da AWS .



## AWS politica gestita: AWSQuickSetupSchedulerPermissionsBoundary

### Note

Questa politica rappresenta un limite delle autorizzazioni. Un limite delle autorizzazioni imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Non è necessario utilizzare e collegare autonomamente le policy relative al limite delle autorizzazioni di Quick Setup. Le policy relative al limite delle autorizzazioni di Quick Setup vanno allegate solo ai ruoli gestiti da Quick Setup. Per maggiori informazioni sui limiti delle autorizzazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.

La policy gestita AWSQuickSetupSchedulerPermissionsBoundary supporta il tipo di configurazione [Arresta e avvia automaticamente le istanze EC2 in base a una pianificazione utilizzando Configurazione rapida](#) di Quick Setup . Questo tipo di configurazione consente di interrompere e avviare le istanze EC2 e altre risorse nei momenti specificati.

Quando crei una configurazione AWSQuickSetupSchedulerPermissionsBoundary utilizzando Quick Setup, il sistema applica questo limite delle autorizzazioni ai ruoli IAM creati durante l'implementazione della configurazione. Il limite delle autorizzazioni limita l'ambito dei ruoli creati da Quick Setup.

Questa policy concede autorizzazioni amministrative che consentono a Quick Setup di abilitare e configurare operazioni pianificate su istanze EC2 e altre risorse.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **iam:** consente alle entità principali di recuperare e trasferire ruoli per le operazioni di automazione della gestione delle istanze; di gestire, trasferire e associare ruoli di istanza predefiniti per la gestione delle istanze EC2; di creare profili di istanza predefiniti; di aggiungere ruoli di istanza predefiniti ai profili di istanza; di creare un ruolo collegato al servizio per Systems Manager; di leggere informazioni sui ruoli IAM e sui profili dell'istanza; di associare un profilo dell'istanza predefinito alle istanze EC2, nonché di avviare flussi di lavoro di Automazione per configurare le istanze e abilitare gli strumenti Systems Manager su questi.
- **ssm:** consente alle entità principali di avviare flussi di lavoro di automazione che abilitino Explorer, nonché di leggere e aggiornare le impostazioni del servizio Explorer.

- `ec2`: consente alle entità principali di individuare istanze destinate, avviandole e interrompendole secondo una pianificazione.
- `config`: consente alle entità principali di contribuire all'abilitazione di Explorer, fornendo un accesso in sola lettura ai dettagli del registratore di configurazione.
- `compute-optimizer`— Consente ai principali di contribuire all'abilitazione Explorer fornendo un accesso in sola lettura per determinare se una risorsa è iscritta. AWS Compute Optimizer
- `support`— Consente ai principali di agevolare l'abilitazione Explorer fornendo l'accesso in sola lettura agli assegni relativi a un account. AWS Trusted Advisor

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupSchedulerPermissionsBoundary](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSQuickSetupCFGCPacksPermissionsBoundary

### Note

Questa politica rappresenta un limite delle autorizzazioni. Un limite delle autorizzazioni imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Non è necessario utilizzare e collegare autonomamente le policy relative al limite delle autorizzazioni di Quick Setup. Le policy relative al limite delle autorizzazioni di Quick Setup vanno allegate solo ai ruoli gestiti da Quick Setup. Per maggiori informazioni sui limiti delle autorizzazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.

La policy gestita AWSQuickSetupCFGCPacksPermissionsBoundary supporta il tipo di configurazione [Implementazione AWS Config pacchetto di conformità utilizzando Configurazione rapida](#) di Quick Setup . Questo tipo di configurazione implementa pacchetti di AWS Config conformità. I pacchetti di conformità sono raccolte di AWS Config regole e azioni correttive che possono essere implementate come un'unica entità.

Quando crei una configurazione AWSQuickSetupCFGCPacksPermissionsBoundary utilizzando Quick Setup, il sistema applica questo limite delle autorizzazioni ai ruoli IAM creati durante l'implementazione della configurazione. Il limite delle autorizzazioni limita l'ambito dei ruoli creati da Quick Setup.

Questa policy concede autorizzazioni amministrative che consentono a Quick Setup di implementare i pacchetti di conformità AWS Config .

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `iam`— Consente ai responsabili di creare, ottenere e trasferire un ruolo collegato al servizio per. AWS Config
- `sns`: consente alle entità principali di elencare le applicazioni di piattaforma in Amazon SNS.
- `config`— AWS Config Consente ai responsabili di distribuire i pacchetti di conformità, di conoscere lo stato dei pacchetti di conformità e di ottenere informazioni sui registratori di configurazione.
- `ssm`: consente alle entità principali di ottenere informazioni sui documenti SSM e sui flussi di lavoro di automazione, di ottenere informazioni sui tag delle risorse e sulle le impostazioni del servizio, aggiornandole.
- `compute-optimizer`: consente alle entità principali di ottenere lo stato di consenso esplicito dell'account.
- `support`: consente alle entità principali di ottenere informazioni sui controlli AWS Trusted Advisor .

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupCFGCPacksPermissionsBoundary](#) nella Guida di riferimento alle policy gestite da AWS .

### AWS politica gestita: AWSQuickSetupStartStopInstancesExecutionPolicy

È possibile collegare AWSQuickSetupStartStopInstancesExecutionPolicy alle entità IAM. Questa policy fornisce le autorizzazioni di Quick Setup per la gestione dell'avvio e dell'interruzione delle istanze Amazon EC2 tramite l'automazione di Systems Manager.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ec2`— Consente ai committenti di descrivere le istanze Amazon EC2, il loro stato, le regioni e i tag. Consente inoltre di avviare e arrestare istanze Amazon EC2 specifiche.

- **ssm**— Consente ai committenti di ottenere lo stato del calendario Quick Setup modificando i calendari, avviando associazioni ed eseguendo documenti di automazione, ad esempio per la pianificazione.
- **iam**— Consente ai principali di passare i ruoli Quick Setup IAM a Systems Manager per l'esecuzione dell'automazione, con condizioni che limitano il servizio a `ssm.amazonaws.com` e agli ARN di risorse specifici.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupStartStopInstancesExecutionPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSQuickSetupStartSSMAssociationsExecutionPolicy

Questa politica concede le autorizzazioni che consentono a Quick Setup di eseguire il runbook Automation `AWSQuickSetupType-Scheduler-ChangeCalendarState`. Questo runbook viene utilizzato per gestire le modifiche agli stati del calendario per le operazioni pianificate nelle Quick Setup configurazioni.

È anche possibile collegare `AWSQuickSetupStartSSMAssociationsExecutionPolicy` alle entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni per conto dell'utente.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **ssm**: consente alle entità principali di avviare esecuzioni di automazione specifiche per il documento `AWSQuickSetupType-Scheduler-ChangeCalendarState`. Questo è necessario per gestire le modifiche Quick Setup agli stati del calendario per le operazioni pianificate.
- **iam**— Consente ai responsabili di passare ruoli con nomi che iniziano con "AWS-QuickSetup-" al servizio Systems Manager. Questa autorizzazione è limitata all'uso con documenti SSM specifici relativi alla gestione del calendario delle modifiche. Ciò è necessario per Quick Setup per passare il ruolo di esecuzione appropriato al processo di automazione.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupStartSSMAssociationsExecutionPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy

La policy `AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy` fornisce le autorizzazioni per diagnosticare i problemi con i nodi che interagiscono con i servizi Systems Manager, avviando i flussi di lavoro di automazione negli account e nelle regioni in cui vengono gestiti i nodi.

È anche possibile collegare `AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy` alle entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni di diagnosi per conto dell'utente.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ssm`: consente alle entità principali di eseguire i runbook di Automazione che diagnosticano i problemi dei nodi e accedono allo stato di esecuzione per i flussi di lavoro e recuperare i dettagli di esecuzione dell'automazione. La policy concede le autorizzazioni per descrivere le esecuzioni di automazione, descrivere le esecuzioni delle fasi di automazione, ottenere dettagli sull'esecuzione dell'automazione e avviare le esecuzioni di automazione per i documenti relativi alla diagnosi.
- `kms`: consente alle entità principali di utilizzare AWS Key Management Service chiavi specificate dal cliente per la decrittografia e la generazione di chiavi di dati durante l'accesso a oggetti crittografati nei bucket Amazon S3 utilizzati per le operazioni di diagnosi. Queste autorizzazioni sono limitate alle chiavi contrassegnate `SystemsManagerManaged` e utilizzate tramite il servizio Amazon S3 con requisiti di contesto di crittografia specifici.
- `sts`: consente alle entità principali di assumere ruoli di esecuzione della diagnosi per eseguire i runbook di Automazione sullo stesso account. Questa autorizzazione è limitata ai ruoli con lo schema di `AWS-SSM-DiagnosisExecutionRole` denominazione e include una condizione per assicurarsi che l'account della risorsa corrisponda all'account principale.
- `iam`: consente alle entità principali di passare il ruolo di amministrazione della diagnosi a Systems Manager per l'esecuzione dei runbook di Automazione. Questa autorizzazione è limitata ai ruoli con il modello di denominazione `AWS-SSM-DiagnosisAdminRole` e può essere passata solo al servizio di Systems Manager.
- `s3`: consente alle entità principali di accedere, leggere, scrivere ed eliminare oggetti nei bucket Amazon S3 utilizzati per le operazioni di diagnosi. Queste autorizzazioni sono limitate ai bucket con lo schema di `do-not-delete-ssm-diagnosis-` denominazione e includono condizioni per garantire che le operazioni vengano eseguite all'interno dello stesso account.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy

La policy gestita da AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy fornisce l'autorizzazione amministrativa per l'esecuzione dei runbook Automation in un Account AWS e Regione destinati, per diagnosticare i problemi con i nodi gestiti che interagiscono con i servizi Systems Manager.

È anche possibile collegare AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy alle entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni per conto dell'utente.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **ec2**— Consente ai committenti di descrivere le risorse Amazon EC2 e Amazon VPC e le relative configurazioni per diagnosticare problemi relativi ai servizi. Systems Manager Ciò include le autorizzazioni per descrivere VPC, attributi VPC, endpoint VPC, sottoreti, gruppi di sicurezza, istanze, stato delle istanze, ACL di rete e gateway Internet.
- **ssm**: consente alle entità principali di eseguire runbook di Automazione specifici per la diagnosi e di accedere allo stato del flusso di lavoro di automazione e ai metadati di esecuzione. Sono incluse le autorizzazioni per descrivere le esecuzioni delle fasi di automazione, descrivere le informazioni sulle istanze, descrivere le esecuzioni di automazione, descrivere le attivazioni, ottenere dettagli sull'esecuzione dell'automazione, ottenere le impostazioni del servizio e avviare le esecuzioni di automazione per specifici documenti di diagnosi EC2 non gestiti. AWS
- **kms**: consente alle entità principali di utilizzare AWS Key Management Service chiavi specificate dal cliente per la decrittografia e la generazione di chiavi di dati durante l'accesso a oggetti crittografati nei bucket Amazon S3 utilizzati per le operazioni di diagnosi. Queste autorizzazioni sono limitate alle chiavi contrassegnate SystemsManagerManaged e utilizzate tramite il servizio Amazon S3 con requisiti di contesto di crittografia specifici per i bucket di diagnosi.
- **iam**: consente alle entità principali di passare il ruolo di esecuzione della diagnosi a Systems Manager per l'esecuzione dei documenti di Automazione. Questa autorizzazione è limitata ai ruoli con il modello di denominazione AWS-SSM-DiagnosisExecutionRole e può essere passata solo al servizio di Systems Manager.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS policy gestita: AWS-SSM-RemediationAutomation-AdministrationRolePolicy

La policy AWS-SSM-RemediationAutomation-AdministrationRolePolicy fornisce le autorizzazioni per risolvere i problemi con i servizi di Systems Manager eseguendo le attività definite nei documenti di Automazione, utilizzate principalmente per eseguire i documenti di Automazione. Questa policy consente di avviare i flussi di lavoro di Automazione negli account e nelle Regioni in cui i nodi vengono gestiti per risolvere problemi di connettività e configurazione.

Puoi collegarti AWS-SSM-RemediationAutomation-AdministrationRolePolicy alle tue entità IAM. Systems Manager associa questa policy anche a un ruolo di servizio che consente di Systems Manager eseguire azioni correttive per tuo conto.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **ssm**: consente alle entità principali di eseguire i runbook di Automazione che riparano i problemi dei nodi e accedono allo stato di esecuzione di flussi di lavoro e recuperano i dettagli dell'esecuzione dell'automazione. La policy concede le autorizzazioni per descrivere le esecuzioni di automazione, le esecuzioni delle fasi di automazione, ottenere dettagli sull'esecuzione dell'automazione e avviare le esecuzioni di automazione per i documenti relativi alla riparazione.
- **kms**: consente alle entità principali di utilizzare AWS Key Management Service chiavi specificate dal cliente per la decrittografia e la generazione di chiavi di dati durante l'accesso a oggetti crittografati nei bucket Amazon S3 utilizzati per le operazioni di riparazione. Queste autorizzazioni sono limitate alle chiavi contrassegnate SystemsManagerManaged e utilizzate tramite il servizio Amazon S3 con requisiti di contesto di crittografia specifici.
- **sts**: consente alle entità principali di assumere ruoli di esecuzione della riparazione per eseguire i runbook di Automazione sullo stesso account. Questa autorizzazione è limitata ai ruoli con lo schema di AWS-SSM-RemediationExecutionRole denominazione e include una condizione per assicurarsi che l'account della risorsa corrisponda all'account principale.
- **iam**: consente alle entità principali di passare il ruolo di amministrazione della riparazione a Systems Manager per l'esecuzione dei runbook di Automazione. Questa autorizzazione è limitata ai ruoli con il modello di denominazione AWS-SSM-RemediationAdminRole e può essere passata solo al servizio di Systems Manager.



- `s3`: consente alle unità principali di accedere, leggere, scrivere ed eliminare oggetti nei bucket Amazon S3 utilizzati per le operazioni di riparazione. Queste autorizzazioni sono limitate ai bucket con lo schema di `do-not-delete-ssm-diagnosis-` denominazione e includono condizioni per garantire che le operazioni vengano eseguite all'interno dello stesso account.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWS-SSM-RemediationAutomation-AdministrationRolePolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWS-SSM-RemediationAutomation-ExecutionRolePolicy

La policy `AWS-SSM-RemediationAutomation-ExecutionRolePolicy` gestita concede le autorizzazioni per l'esecuzione di runbook di Automazione in un account e in una Regione di destinazione specifici per riparare gli errori di connessione della rete con i nodi gestiti che interagiscono con i servizi di Systems Manager. Questa policy consente attività di riparazione definite nei documenti di Automazione, utilizzate principalmente per l'esecuzione di documenti di Automazione e risolvere problemi di connettività e configurazione.

Puoi collegare la policy anche alle tue entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni di riparazione per conto dell'utente.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ssm`: consente alle entità principali di recuperare informazioni sulle esecuzioni di Automazione e sulle relative fasi e di avviare runbook di Automazione di riparazione specifici, inclusi documenti `AWS-OrchestrateUnmanagedEC2Actions` e `AWS-RemediateSSMAgent`. La policy concede le autorizzazioni per descrivere le esecuzioni di automazione, le esecuzioni delle fasi di automazione, ottenere dettagli sull'esecuzione dell'automazione e avviare le esecuzioni di automazione per i documenti relativi alla riparazione.
- `ec2`: consente alle entità principali di descrivere e modificare le risorse di rete Amazon VPC per riparare i problemi di connettività. Questo include:
  - Descrizione degli attributi e delle sottoreti di Amazon VPC, degli endpoint Amazon VPC e dei gruppi di sicurezza.
  - Creazione di endpoint Amazon VPC per i servizi di Systems Manager (`ssm`, `ssmmessages` e `ec2messages`) con i tag richiesti.



- Modifica degli attributi di Amazon VPC per abilitare il supporto DNS e i nomi host.
- Creazione e gestione di gruppi di sicurezza con tag specifici per l'accesso agli endpoint Amazon VPC.
- Autorizzazione e revoca delle regole dei gruppi di sicurezza per l'accesso HTTPS con tag appropriati.
- Creazione di tag su endpoint Amazon VPC, gruppi di sicurezza e regole dei gruppi di sicurezza durante la creazione delle risorse.
- kms: consente alle entità principali di utilizzare AWS Key Management Service chiavi specificate dal cliente per la decrittografia e la generazione di chiavi di dati durante l'accesso a oggetti crittografati nei bucket Amazon S3 utilizzati per le operazioni di riparazione. Queste autorizzazioni sono limitate alle chiavi contrassegnate SystemsManagerManaged e utilizzate tramite il servizio Amazon S3 con requisiti di contesto di crittografia specifici.
- iam: consente alle entità principali di passare il ruolo di esecuzione di riparazione a Systems Manager per l'esecuzione dei runbook di Automazione. Questa autorizzazione è limitata ai ruoli con il modello di denominazione AWS-SSM-RemediationExecutionRole e può essere passata solo al servizio di Systems Manager.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWS-SSM-RemediationAutomation-ExecutionRolePolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS policy gestita: AWSQuickSetupSSMManageResourcesExecutionPolicy

Questa politica concede le autorizzazioni che consentono a Quick Setup di eseguire il runbook Automation AWSQuickSetupType-SSM-SetupResources. Questo runbook crea ruoli IAM per le associazioni di Quick Setup, a loro volta create dall'implementazione AWSQuickSetupType-SSM. Concede inoltre le autorizzazioni per pulire un bucket Amazon S3 associato durante un'operazione di eliminazione di Quick Setup.

È anche possibile collegare questa policy alle entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni per conto dell'utente.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **iam**: consente alle entità principali di elencare e gestire i ruoli IAM da utilizzare con le operazioni di Systems Manager Explorer di Quick Setup, nonché di visualizzare, allegare e scollegare le policy IAM da utilizzare con Quick Setup e Systems Manager Explorer. Queste autorizzazioni sono necessarie in modo che Quick Setup crei i ruoli necessari per alcune delle sue operazioni di configurazione.
- **s3**: consente alle entità principali di recuperare informazioni sugli oggetti e di eliminare quelli dai bucket Amazon S3, nell'account principale, che vengono utilizzati specificamente nelle operazioni di configurazione in Quick Setup. Ciò è necessario per rimuovere gli oggetti S3 che non sono più necessari dopo la configurazione.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupSSMManageResourcesExecutionPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSQuickSetupSSMLifecycleManagementExecutionPolicy

La `AWSQuickSetupSSMLifecycleManagementExecutionPolicy` policy concede autorizzazioni amministrative che consentono di Quick Setup eseguire una risorsa CloudFormation personalizzata sugli eventi del ciclo di vita durante la distribuzione in. Quick Setup Systems Manager

È anche possibile collegare questa policy alle entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni per conto dell'utente.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **ssm**: consente alle entità principali di ottenere informazioni sulle esecuzioni di automazione e di avviare le esecuzioni di automazione per impostare determinate operazioni di Quick Setup.
- **iam**: consente alle entità principali di trasferire ruoli da IAM per la configurazione di determinate risorse di Quick Setup.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupSSMLifecycleManagementExecutionPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSQuickSetupSSMDeploymentRolePolicy

La policy gestita AWSQuickSetupSSMDeploymentRolePolicy concede autorizzazioni amministrative che consentono a Quick Setup di creare risorse da utilizzare durante il processo di onboarding di Systems Manager.

Sebbene sia possibile attribuire questa policy alle entità IAM, questa policy non è consigliata. Quick Setup crea entità che collegano questa policy a un ruolo di servizio che consente a Systems Manager di eseguire operazioni per tuo conto.

Questa policy non è correlata alla [policy SSMQuickSetupRolePolicy](#), utilizzata per fornire le autorizzazioni per il ruolo collegato al servizio AWSServiceRoleForSSMQuickSetup.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ssm`— Consente ai responsabili di gestire le associazioni per determinate risorse create utilizzando AWS CloudFormation modelli e un set specifico di documenti SSM; di gestire i ruoli e le politiche di ruolo utilizzando i CloudFormation modelli per la diagnosi e la correzione dei nodi gestiti; e di allegare ed eliminare le politiche per gli eventi del ciclo di vita Quick Setup
- `iam`: consente alle entità principali di aggiungere un tag ai ruoli, assegnare le autorizzazioni ai ruoli per il servizio di Systems Manager e il servizio Lambda e assegnare le autorizzazioni al ruolo per le operazioni di diagnosi.
- `lambda`— Consente ai principali di etichettare e gestire le funzioni per il Quick Setup ciclo di vita nell'account principale utilizzando modelli. CloudFormation
- `cloudformation`— Consente ai principali di leggere informazioni da. CloudFormation Ciò è necessario per Quick Setup raccogliere dati sugli CloudFormation stack utilizzati per gestire lo stato delle risorse e le operazioni degli CloudFormation stackset.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupSSMDeploymentRolePolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSQuickSetupSSMDeploymentS3BucketRolePolicy

La policy AWSQuickSetupSSMDeploymentS3BucketRolePolicy concede le autorizzazioni per elencare tutti i bucket S3 in un account e per gestire e recuperare informazioni su bucket specifici, gestiti tramite modelli CloudFormation , nell'account principale.

È anche possibile collegare `AWSQuickSetupSSMDeploymentS3BucketRolePolicy` alle entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni per conto dell'utente.

#### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `s3`— Consente ai principali di elencare tutti i bucket S3 in un account e di gestire e recuperare informazioni su bucket specifici nell'account principale gestiti tramite modelli. CloudFormation

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupSSMDeploymentS3BucketRolePolicy](#) nella Guida di riferimento alle policy gestite da AWS .

#### AWS politica gestita: `AWSQuickSetupEnableDHMCExecutionPolicy`

Questa policy concede autorizzazioni amministrative che consentono alle entità principali di eseguire il runbook di Automation `AWSQuickSetupType-EnableDHMC`, abilitando la configurazione di gestione host predefinita. La funzionalità Configurazione di gestione host predefinita consente a Systems Manager di gestire automaticamente le istanze Amazon EC2 come istanze gestite. Un'istanza gestita è un'istanza EC2 configurata per l'uso con Systems Manager. Questa policy concede anche le autorizzazioni per la creazione di ruoli IAM specificati nelle impostazioni del servizio Systems Manager come ruoli predefiniti per SSM Agent.

È anche possibile collegare `AWSQuickSetupEnableDHMCExecutionPolicy` alle entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni per conto dell'utente.

#### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ssm`: consente alle entità principali di aggiornare e ottenere informazioni sulle impostazioni del servizio di Systems Manager.
- `iam`: consente alle entità principali di creare e recuperare informazioni sui ruoli IAM per le operazioni di Quick Setup.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupEnableDHMCExecutionPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSQuickSetupEnableAREXExecutionPolicy

Questa policy concede autorizzazioni amministrative che consentono a Systems Manager di eseguire il runbook di `AWSQuickSetupType-EnableAREX Automation`, consentendo a Esploratore di risorse AWS l'utilizzo con Systems Manager. Resource Explorer consente di visualizzare le risorse dell'account con un'esperienza di ricerca simile a quella di un motore di ricerca Internet. La policy concede inoltre le autorizzazioni per la gestione degli indici e delle visualizzazioni di Resource Explorer.

È anche possibile collegare `AWSQuickSetupEnableAREXExecutionPolicy` alle entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni per conto dell'utente.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `iam`— Consente ai principali di creare un ruolo collegato al servizio nel servizio AWS Identity and Access Management (IAM).
- `resource-explorer-2`: consente alle entità principali di recuperare informazioni sulle visualizzazioni e sugli indici di Resource Explorer, di creare visualizzazioni e indici dello stesso, nonché di modificare la tipologia per gli indici visualizzati in Quick Setup.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupEnableAREXExecutionPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSQuickSetupManagedInstanceProfileExecutionPolicy

Questa policy concede autorizzazioni amministrative che consentono a Systems Manager di creare un profilo di istanza IAM predefinito per la Quick Setup funzionalità e di collegarlo alle istanze Amazon EC2 a cui non è già associato un profilo di istanza.

È possibile collegare `AWSQuickSetupManagedInstanceProfileExecutionPolicy` alle entità IAM. Systems Manager attribuisce inoltre questa policy a un ruolo di servizio che consente a Systems Manager di eseguire azioni per tuo conto.

## Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **ec2**— Consente ai principali di associare i profili delle istanze IAM alle istanze Amazon EC2 e di recuperare informazioni sulle associazioni e sulle istanze dei profili di istanza.
- **iam**— Consente ai principali di creare e gestire il ruolo e il profilo di istanza IAM predefiniti per Quick Setup, allegare policy gestite ai ruoli, etichettare i ruoli e passare ruoli ai servizi Amazon EC2 e Systems Manager.
- **ssm**— Consente ai principali di avviare e monitorare le esecuzioni di automazione, recuperare informazioni sulle istanze, aggiornare i ruoli delle istanze gestite e aggiungere tag alle risorse di automazione.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupManagedInstanceProfileExecutionPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSQuickSetupManageJITNAResourcesExecutionPolicy

La policy gestita da AWSQuickSetupManageJITNAResourcesExecutionPolicy consente a Quick Setup, uno strumento di Systems Manager, di configurare l'accesso ai nodi just-in-time.

È anche possibile collegare AWSQuickSetupManageJITNAResourcesExecutionPolicy alle entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni per conto dell'utente.

Questa policy concede autorizzazioni amministrative che consentono a Systems Manager di creare risorse associate all'accesso ai nodi just-in-time.

## Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **ssm**: consente alle entità principali di ottenere e aggiornare l'impostazione del servizio che specifica il provider di identità per l'accesso ai nodi just-in-time.
- **iam**: consente alle entità principali di creare, aggiungere tag e ottenere ruoli, allegare policy di ruolo per policy gestite di accesso ai nodi just-in-time e creare ruoli collegati ai servizi per l'accesso ai nodi e le notifiche just-in-time.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupManageJITNAResourcesExecutionPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSQuickSetupJITNADeploymentRolePolicy

La policy gestita da AWSQuickSetupJITNADeploymentRolePolicy consente a Quick Setup di implementare il tipo di configurazione richiesto per configurare l'accesso al nodo just-in-time.

È anche possibile collegare AWSQuickSetupJITNADeploymentRolePolicy alle entità IAM. Systems Manager collega questa policy anche a un ruolo di servizio che consente a Systems Manager di eseguire operazioni per conto dell'utente.

Questa policy concede autorizzazioni amministrative che consentono a Systems Manager di creare risorse associate all'accesso ai nodi just-in-time.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `cloudformation`— Consente ai principali di creare, aggiornare, eliminare e leggere gli CloudFormation stack.
- `ssm`— Consente ai principali di creare, eliminare, aggiornare e leggere State Manager le associazioni richiamate da. CloudFormation
- `iam`— Consente ai principali di creare, eliminare, leggere e contrassegnare i ruoli IAM chiamati da. CloudFormation

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSQuickSetupJITNADeploymentRolePolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSSystemsManagerJustInTimeAccessServicePolicy

La policy gestita AWSSystemsManagerJustInTimeAccessServicePolicy fornisce l'accesso alle AWS risorse gestite o utilizzate dal framework di accesso AWS Systems Manager just-in-time. Questo aggiornamento della policy aggiunge le autorizzazioni all'aggiunta di tag in modalità di esecuzione automatica, per consentire ai clienti di limitare le autorizzazioni degli operatori a tag specifici.

Non è possibile collegare `AWSSystemsManagerJustInTimeAccessServicePolicy` alle entità IAM. Questa policy è associata a un ruolo collegato ai servizi che consente a Systems Manager di eseguire operazioni per tuo conto. Per ulteriori informazioni, consulta [Utilizzo dei ruoli per abilitare l'accesso ai nodi just-in-time](#).

Questa policy concede autorizzazioni amministrative che consentono l'accesso alle risorse associate con accesso ai nodi just-in-time.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ssm`: consente alle unità principali di creare e gestire OpsItems, aggiungere tag a OpsItems e automatizzare le esecuzioni, ottenere e aggiornare OpsItems, recuperare e descrivere documenti, descrivere OpsItems e sessioni, elencare documenti e tag per le istanze gestite.
- `ssm-guiconnect`: consente alle entità principali di elencare le connessioni.
- `identitystore`: consente alle entità principali di ottenere ID utente e gruppo, descrivere gli utenti ed elencare l'appartenenza al gruppo.
- `sso-directory`: consente alle entità principali di descrivere gli utenti e determinare se un utente è membro di un gruppo.
- `sso`: consente alle entità principali di descrivere le Regioni registrate ed elencare le istanze e le associazioni di directory.
- `cloudwatch`: consente alle entità principali di inserire dati metrici per l'`AWS/SSM/JustInTimeAccess` namespace.
- `ec2`: consente alle entità principali di descrivere i tag.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSSystemsManagerJustInTimeAccessServicePolicy](#) nella Guida di riferimento alle policy gestite da AWS .

### AWS politica gestita: `AWSSystemsManagerJustInTimeAccessTokenPolicy`

La policy gestita `AWSSystemsManagerJustInTimeAccessTokenPolicy` fornisce agli utenti le autorizzazioni per stabilire connessioni sicure alle istanze Amazon EC2 e alle istanze gestite tramite Session Manager connessioni RDP Systems Manager GUI Connect come parte dei flussi di lavoro di accesso ai nodi just-in-time.



È possibile collegare `AWSSystemsManagerJustInTimeAccessTokenPolicy` alle entità IAM.

Questa policy concede ai collaboratori le autorizzazioni che consentono agli utenti di avviare e gestire sessioni sicure, stabilire connessioni RDP ed eseguire le operazioni crittografiche necessarie per l'accesso ai nodi just-in-time.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ssm`— Consente ai principali di avviare Session Manager sessioni su istanze Amazon EC2 e istanze gestite utilizzando il documento. `SSM-SessionManagerRunShell` Consente inoltre di terminare e riprendere le sessioni, recuperare i dettagli di richiamo dei comandi e inviare comandi alle istanze per la configurazione dell'utente SSO quando vengono richiamati tramite Systems Manager GUI Connect. Inoltre, consente di avviare sessioni di port forwarding per le connessioni RDP quando viene richiamata tramite Systems Manager GUI Connect.
- `ssmmessages`— Consente ai presidi di aprire canali di dati per comunicazioni sicure durante le sessioni. Session Manager
- `ssm-guiconnect`— Consente ai principali di avviare, ottenere dettagli e annullare le connessioni RDP di Systems Manager GUI Connect alle istanze.
- `kms`— Consente ai principali di generare chiavi di dati per la Session Manager crittografia e creare concessioni per le connessioni RDP. Queste autorizzazioni sono limitate alle chiavi contrassegnate con `AWS KMS SystemsManagerJustInTimeNodeAccessManaged=true` La creazione delle concessioni è ulteriormente limitata e può essere utilizzata solo tramite il servizio Systems Manager GUI Connect.
- `sso`— Consente ai principali di elencare le associazioni di directory quando vengono richiamate tramite Systems Manager GUI Connect. Ciò è necessario per la configurazione dell'utente RDP SSO.
- `identitystore`— Consente ai principali di descrivere gli utenti nell'archivio di identità quando vengono richiamati tramite Systems Manager GUI Connect. Ciò è necessario per la configurazione degli utenti RDP SSO.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSSystemsManagerJustInTimeAccessTokenPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSSystemsManagerJustInTimeAccessTokenSessionPolicy

La policy `AWSSystemsManagerJustInTimeAccessTokenSessionPolicy` gestita consente a Systems Manager di applicare autorizzazioni limitate a un token di accesso al nodo just-in-time.

È possibile collegare `AWSSystemsManagerJustInTimeAccessTokenSessionPolicy` alle entità IAM.

Questa policy concede autorizzazioni amministrative che consentono a Systems Manager di limitare le autorizzazioni per i token di accesso ai nodi just-in-time.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ssm`: consente alle entità principali di avviare sessioni Session Manager utilizzando il documento `SSM-SessionManagerRunShell`. Inoltre, quando viene chiamato per primo `ssm-guiconnect`, avvia le sessioni utilizzando il `AWS-StartPortForwardingSession` documento, elenca le chiamate ai comandi e invia i comandi utilizzando il `AWSSSO-CreateSSOUser` documento.
- `ssm-guiconnect`: consente alle entità principali di annullare, ottenere e avviare connessioni su tutte le risorse.
- `kms`— Consente ai committenti di creare concessioni e generare chiavi di dati per le chiavi contrassegnate `SystemsManagerJustInTimeNodeAccessManaged` quando vengono richiamate `ssm-guiconnect` da un servizio. AWS
- `sso`— Consente ai principali di elencare le associazioni di directory quando vengono richiamati. `ssm-guiconnect`
- `identitystore`— Consente ai principali di descrivere un utente quando viene chiamato. `ssm-guiconnect`

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSSystemsManagerJustInTimeAccessTokenSessionPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita:

### AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy

La policy gestita `AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy` consente a Systems Manager di condividere le policy di negazione dell'accesso dall'account amministratore delegato agli account membri e di replicare le policy su più Regioni AWS.

È possibile collegare `AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy` alle entità IAM.

Questa policy fornisce le autorizzazioni amministrative necessarie a Systems Manager per condividere e creare policy di negazione dell'accesso. Ciò garantisce che le politiche di negazione dell'accesso siano applicate a tutti gli account di un' AWS Organizations organizzazione e alle regioni configurate per l'accesso ai nodi just-in-time.

#### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ssm`: consente alle entità principali di gestire documenti SSM e policy delle risorse.
- `ssm-quicksetup`: consente alle entità principali di leggere i gestori di configurazione di Quick Setup.
- `organizations`: consente alle unità principali di elencare i dettagli su un'organizzazione AWS Organizations e sugli amministratori delegati.
- `ram`: consente alle entità principali di creare, assegnare tag e descrivere le condivisioni di risorse.
- `iam`: consente alle entità principali di descrivere un ruolo di servizio.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWSSystemsManagerNotificationsServicePolicy

La policy `AWSSystemsManagerNotificationsServicePolicy` gestita consente Systems Manager di inviare notifiche e-mail per le richieste di accesso ai nodi just-in-time agli approvatori delle richieste di accesso.

Non è possibile collegare `AWSSystemsManagerJustInTimeAccessServicePolicy` alle entità IAM. Questa policy è associata a un ruolo collegato ai servizi che consente a Systems Manager di

eseguire operazioni per tuo conto. Per ulteriori informazioni, consulta [Utilizzo dei ruoli per inviare notifiche di richiesta di accesso ai nodi just-in-time](#).

Questa policy concede autorizzazioni amministrative che consentono a Systems Manager di inviare notifiche e-mail per richieste di accesso ai nodi just-in-time agli approvatori delle richieste di accesso.

#### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `identitystore`: consente alle entità principali di elencare e descrivere gli utenti e l'appartenenza ai gruppi.
- `sso`: consente alle unità principali di elencare istanze, directory e descrivere le Regioni registrate.
- `sso-directory`: consente alle unità principali di descrivere utenti ed elencare membri in un gruppo.
- `iam`: consente alle entità principali di ottenere informazioni sui ruoli.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWSSystemsManagerNotificationsServicePolicy](#) nella Guida di riferimento alle policy gestite da AWS .

### AWS politica gestita: AWS-SSM-Automation-DiagnosisBucketPolicy

La policy gestita `AWS-SSM-Automation-DiagnosisBucketPolicy` fornisce le autorizzazioni per la diagnosi dei problemi con i nodi che interagiscono con AWS Systems Manager i servizi, consentendo l'accesso ai bucket S3 utilizzati per la diagnosi e la risoluzione dei problemi.

È possibile allegare la policy `AWS-SSM-Automation-DiagnosisBucketPolicy` alle identità IAM. Systems Manager collega questa policy anche a un ruolo IAM che consente a Systems Manager di eseguire operazioni di diagnosi per conto dell'utente.

#### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `s3`: consente alle entità principali l'accesso e la scrittura di oggetti in un bucket Amazon S3.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWS-SSM-Automation-DiagnosisBucketPolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy

La policy gestita AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy fornisce le autorizzazioni per consentire a un account operativo di diagnosticare problemi con i nodi fornendo autorizzazioni specifiche dell'organizzazione.

È possibile allegare la policy AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy alle identità IAM. Systems Manager collega questa policy anche a un ruolo IAM che consente a Systems Manager di eseguire operazioni di diagnosi per conto dell'utente.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **organizations**: consente alle entità principali di elencare i root dell'organizzazione e di ottenere gli account dei membri per determinare gli account di destinazione.
- **sts**: consente alle entità principali di assumere ruoli di esecuzione di correzione per eseguire i documenti di Automazione SSM su più account e Regioni, all'interno della stessa organizzazione.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## AWS politica gestita: AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy

La policy gestita AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy fornisce le autorizzazioni per consentire a un account operativo di diagnosticare problemi con i nodi fornendo autorizzazioni specifiche dell'organizzazione.

È possibile allegare la policy `AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy` alle identità IAM. Systems Manager collega questa policy anche a un ruolo IAM che consente a Systems Manager di eseguire operazioni di diagnosi per conto dell'utente.

### Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `organizations`: consente alle entità principali di elencare i root dell'organizzazione e di ottenere gli account membro per determinare gli account di destinazione.
- `sts`: consente alle entità principali di assumere ruoli di esecuzione di diagnosi per eseguire i documenti di automazione SSM su più account e Regioni, all'interno della stessa organizzazione.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta [AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy](#) nella Guida di riferimento alle policy gestite da AWS .

## Systems Manager aggiornamenti a AWS policy gestite

Nella tabella seguente, visualizza i dettagli sugli aggiornamenti alle policy AWS gestite da Systems Manager quando questo servizio ha iniziato a tracciare queste modifiche il 12 marzo 2021. Per informazioni su altre policy gestite per il servizio Systems Manager, consulta [Policy gestite aggiuntive per Systems Manager](#) più avanti. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivere il feed RSS nella pagina [Cronologia dei documenti](#) di Systems Manager.

Modifica	Descrizione	Data
<a href="#">AWSQuickSetupPatchPolicyLambdaExecutionPolicy</a> — Nuova politica gestita	Systems Manager ha aggiunto una nuova politica gestita <code>AWSQuickSetupPatchPolicyLambdaExecutionPolicy</code> che concede le autorizzazioni per gestire le associazioni di State	3 giugno 2026

Modifica	Descrizione	Data
	Manager per le operazioni di pulizia automatiche quando le configurazioni di Quick Setup vengono eliminate.	
<a href="#">AWSQuickSetupPatchPolicyTagManagementExecutionPolicy</a> — Nuova politica gestita	Systems Manager ha aggiunto una nuova policy gestita per consentire alle configurazioni delle policy di Quick Setup patch di tenere traccia delle istanze gestite tramite l'etichettatura automatica e la raccolta dell'inventario. La policy concede le autorizzazioni per aggiungere o rimuovere i tag QSConfigName -* sulle istanze Amazon EC2 e sulle istanze gestite da SSM, insieme alle funzionalità di recupero dell'inventario SSM.	3 giugno 2026

Modifica	Descrizione	Data
<a href="#">AWSQuickSetupManagedInstanceProfileExecutionPolicy</a> — Politica gestita aggiornata	<p>Systems Manager ha aggiornato la politica gestita per supportare Quick Setup Patch Policy la migrazione dalle politiche CloudFormation in linea alle politiche gestite. L'aggiornamento aggiunge funzionalità di esecuzione automatizzata, tra cui il rilevamento delle istanze, gli aggiornamenti dei ruoli, l'etichettatura dei ruoli e PassRole le autorizzazioni estese a Systems Manager. Un'istruzione protettiva Deny impedisce la modifica dei ruoli di automazione. Quick Setup</p>	<p>3 giugno 2026</p>
<a href="#">AmazonSSMAutomationRole</a> : aggiornamento di una policy esistente	<p>Systems Manager ha aggiunto le <code>cloudformation:UntagResource</code> autorizzazioni <code>cloudformation:TagResource</code> and. Queste autorizzazioni consentono ai runbook di Automation che creano CloudFormation stack di aggiungere e rimuovere tag dalle risorse.</p>	<p>20 marzo 2026</p>



Modifica	Descrizione	Data
<a href="#">AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy</a> — Politica gestita aggiornata	Systems Manager ha aggiornato la politica gestita per aggiungere ulteriori autorizzazioni EC2 e SSM per funzionalità di diagnosi avanzate. La policy ora include le autorizzazioni per descrivere lo stato dell'istanza EC2 e gli ACL di rete, nonché le attivazioni SSM e le impostazioni del servizio, fornendo informazioni diagnostiche più complete per la risoluzione dei problemi relativi ai nodi gestiti.	19 dicembre 2025
<a href="#">AWSQuickSetupDeploymentRolePolicy</a> — Politica gestita aggiornata	Systems Manager ha aggiornato la policy gestita <code>AWSQuickSetupDeploymentRolePolicy</code> per aggiungere il supporto per due documenti SSM aggiuntivi: <code>AWSQuickSetupType-ConfigureDevOpsGuru</code> e <code>AWSQuickSetupType-DeployConformancePack</code> . Queste aggiunte consentono di Quick Setup implementare le configurazioni DevOps Guru e i pacchetti di conformità tramite la policy.	15 dicembre 2025

Modifica	Descrizione	Data
<a href="#">AWSSystemsManagerJustInTimeAccessTokenPolicy</a> : aggiornamento di una policy esistente	Systems Manager ha aggiornato la politica <code>AWSSystemsManagerJustInTimeAccessTokenPolicy</code> gestita. L'istruzione <code>(SID) TerminateAndResumeSession</code> è stata rinominata a <code>TerminateAndResumeSessionAndOpenDataChannel</code> e ora include l' <code>ssmmessages:OpenDataChannel</code> azione, che combina la gestione delle sessioni e le autorizzazioni del canale dati in un'unica dichiarazione.	25 settembre 2025
Politiche gestite aggiornate: <ul style="list-style-type: none"> <li>• <a href="#">AWSQuickSetupSSMLifecycleManagementExecutionPolicy</a></li> <li>• <a href="#">AWSQuickSetupPatchPolicyPermissionsBoundary</a></li> <li>• <a href="#">AWSQuickSetupManagedInstanceProfileExecutionPolicy</a></li> </ul>	Systems Manager ha aggiornato tre policy gestite per aggiungere il supporto per l'avvio delle esecuzioni di Automation su risorse aggiuntive di Systems Manager, inclusi runbook di Automation specifici e documenti SSM Command.	12 settembre 2025

Modifica	Descrizione	Data
<a href="#">AWSQuickSetupStartStopInstancesExecutionPolicy</a> — Politica gestita aggiornata	Systems Manager ha aggiornato la politica gestita per perfezionare le autorizzazioni per la configurazione dello Quick Setup scheduler. La policy ora fornisce autorizzazioni più specifiche per l'avvio e l'arresto delle istanze Amazon EC2, l'accesso ai calendari delle modifiche e l'esecuzione di documenti di automazione con condizioni di sicurezza avanzate.	12 settembre 2025
<a href="#">AWSQuickSetupStartSSMAssociationsExecutionPolicy</a> — Politica gestita aggiornata	Systems Manager ha aggiornato la politica gestita per modificare il documento di automazione da <code>AWSQuickSetupType-StartSSMAssociations</code> a <code>AWSQuickSetupType-Scheduler-ChangeCalendarState</code> . Questo aggiornamento modifica lo scopo della politica, dall'avvio delle associazioni SSM alla gestione delle modifiche degli stati del calendario per le operazioni pianificate.	12 settembre 2025

Modifica	Descrizione	Data
<a href="#">AmazonSSMAutomationRole:</a> aggiornamento di una policy esistente	<p>Systems Manager ha aggiunto nuove autorizzazioni per consentire ai runbook di Automazione di stabilire canali di comunicazione per le operazioni basate sulla sessione.</p> <p>Autorizzazione <code>ssmmessages:OpenDataChannel</code> per la risorsa <code>arn:*:ssm:*:*:session/*</code> aggiunta.</p>	11 settembre 2025
<a href="#">AWSSystemsManagerJustInTimeAccessServicePolicy</a> — Politica gestita aggiornata	<p>Systems Manager ha aggiornato la policy gestita per aggiungere autorizzazioni di etichettatura di esecuzione e dell'automazione. Il servizio deve etichettare le esecuzioni di automazione con il tag <code>SystemsManagerJustInTimeNodeAccessManaged=true</code> per consentire ai clienti di limitare le autorizzazioni degli operatori a tag specifici.</p>	25 agosto 2025

Modifica	Descrizione	Data
<a href="#">AWSQuickSetupStartSSMAssociationsExecutionPolicy</a> : nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Quick Setup di eseguire il runbook di <code>AWSQuickSetupType-StartSSMAssociations</code> di Automazione. Questo runbook viene utilizzato per avviare le associazioni State Manager create dalle configurazioni Quick Setup.	12 agosto 2025
<a href="#">AWSQuickSetupStartStopInstancesExecutionPolicy</a> : nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Quick Setup l'avvio e l'interruzione delle istanze Amazon EC2 in base a una pianificazione. Questa policy fornisce le autorizzazioni necessarie per il tipo di configurazione del pianificatore di Quick Setup per gestire lo stato dell'istanza in base a pianificazioni definite.	12 agosto 2025

Modifica	Descrizione	Data
<a href="#">AWSQuickSetupDeploymentRolePolicy</a> — Aggiornamento della documentazione	Systems Manager ha aggiornato la policy di <code>AWSQuickSetupDeploymentRolePolicy</code> gestita per concedere autorizzazioni per risorse aggiuntive. Inoltre, la documentazione di <code>AWSQuickSetupDeploymentRolePolicy</code> è stata aggiornata con descrizioni più dettagliate delle autorizzazioni concesse da questa policy per le operazioni di gestione della configurazione di Quick Setup.	12 agosto 2025

Modifica	Descrizione	Data
<a href="#">AWS-SSM-RemediationAutomation-ExecutionRolePolicy</a> : aggiornamento di una policy esistente	Systems Manager ha aggiornato la policy gestita per migliorare lo stato di sicurezza dell'Star Automation Execution API ssm: richiedendo le autorizzazioni per i tipi di risorse «documento» e «esecuzione automatica». La policy aggiornata fornisce autorizzazioni più complete e dettagliate per l'esecuzione dell'automazione di riparazione, tra cui descrizioni migliorate delle funzionalità di riparazione della rete, autorizzazioni più specifiche per la creazione di endpoint Amazon VPC, autorizzazioni dettagliate per la gestione dei gruppi di sicurezza e controlli migliorati di etichettatura delle risorse per le operazioni di riparazione.	16 luglio 2025

Modifica	Descrizione	Data
<a href="#">AWS-SSM-RemediationAutomation-AdministrationRolePolicy</a> : aggiornamento di una policy esistente	Systems Manager ha aggiornato la policy gestita per supportare i miglioramenti delle autorizzazioni delle API per le operazioni di automazione della riparazione. La policy aggiornata migliora le autorizzazioni per l'esecuzione delle attività definite nei documenti di Automazione, con controlli di sicurezza e modelli di accesso alle risorse migliorati per i flussi di lavoro di riparazione.	16 luglio 2025
<a href="#">AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy</a> : aggiornamento di una policy esistente	Systems Manager ha aggiornato la policy gestita per fornire autorizzazioni più dettagliate e accurate per l'esecuzione dell'automazione della diagnosi. La policy aggiornata include descrizioni migliorate per l'accesso alle risorse di Amazon EC2 e Amazon VPC, autorizzazioni di automazione SSM più specifiche e descrizioni delle autorizzazioni migliorate e IAM con adeguate restrizioni sulle risorse. AWS KMS	16 luglio 2025



Modifica	Descrizione	Data
<a href="#">AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy</a> : aggiornamento di una policy esistente	<p>Systems Manager ha aggiornato la policy gestita per fornire autorizzazioni e condizioni di sicurezza più specifiche per le operazioni di automazione della diagnosi. La policy aggiornata fornisce controlli di sicurezza avanzati per l'utilizzo delle AWS KMS chiavi, l'accesso ai bucket Amazon S3 e l'assunzione dei ruoli, con condizioni basate sulle risorse e restrizioni a livello di account più rigorose.</p>	16 luglio 2025
<a href="#">AWSQuickSetupDeploymentRolePolicy</a> — Aggiornamento a una policy	<p>Systems Manager ha aggiunto le autorizzazioni alla policy gestita <code>AWSQuickSetupDeploymentRolePolicy</code> per l'accesso al <a href="#">AWSQuickSetupType-ManageInstanceProfile</a> runbook di proprietà di Amazon. Questa autorizzazione consente a Quick Setup di creare associazioni utilizzando la policy gestita anziché le policy in linea.</p>	14 luglio 2025

Modifica	Descrizione	Data
<a href="#">AmazonSSMAutomationRole</a> — Aggiornamento della documentazione	Systems Manager ha aggiunto una documentazione completa relativa alla policy AmazonSSMAutomationRole esistente, che fornisce le autorizzazioni per il servizio di Automazione di Systems Manager che esegue attività definite all'interno dei runbook di Automazione.	15 luglio 2025
<a href="#">AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy</a> — Aggiornamento di una politica	Systems Manager autorizzazioni aggiunte per consentire di Systems Manager etichettare una risorsa condivisa AWS Resource Access Manager per l'accesso al nodo just-in-time.	30 aprile 2025
<a href="#">AWSQuickSetupManagerJITNAResourcesExecutionPolicy</a> — Aggiornamento di una policy	Autorizzazioni aggiunte da Systems Manager per consentire Systems Manager di etichettare i ruoli IAM creati per l'accesso ai nodi just-in-time.	30 aprile 2025
<a href="#">AWSSystemsManagerJustInTimeAccessTokenSessionPolicy</a> : nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Systems Manager di applicare autorizzazioni limitate a un token di accesso al nodo just-in-time.	30 aprile 2025

Modifica	Descrizione	Data
<a href="#"><u>AWSSystemsManagerNotificationsServicePolicy:</u></a> nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Systems Manager di inviare le notifiche e-mail per le richieste di accesso ai nodi just-in-time agli approvatori delle richieste di accesso.	30 aprile 2025
<a href="#"><u>AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy:</u></a> nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Systems Manager di replicare le policy di approvazione in diverse Regioni.	30 aprile 2025
<a href="#"><u>AWSSystemsManagerJustInTimeAccessTokenPolicy:</u></a> nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Systems Manager di generare token di accesso utilizzati per l'accesso ai nodi just-in-time.	30 aprile 2025
<a href="#"><u>AWSSystemsManagerJustInTimeAccessServicePolicy:</u></a> nuova policy	Systems Manager ha aggiunto una nuova policy per fornire le autorizzazioni alle risorse gestite da AWS o utilizzate dalla funzionalità di accesso al nodo just-in-time di Systems Manager.	30 aprile 2025
<a href="#"><u>AWSQuickSetupManagerJITNAResourcesExecutionPolicy:</u></a> nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Quick Setup, in Systems Manager, di creare i ruoli IAM necessari per l'accesso just-in-time ai nodi.	30 aprile 2025

Modifica	Descrizione	Data
<a href="#">AWSQuickSetupJITNADeploymentRolePolicy</a> : nuova policy	Systems Manager ha aggiunto una nuova policy che fornisce le autorizzazioni a Quick Setup per implementare il tipo di configurazione richiesto per configurare l'accesso ai nodi just-in-time.	30 aprile 2025
<a href="#">AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy</a> — Aggiornamento di una policy	Systems Manager autorizzazioni aggiunte per consentire di Systems Manager etichettare una risorsa condivisa AWS Resource Access Manager per l'accesso al nodo just-in-time.	30 aprile 2025
<a href="#">AWSQuickSetupManagerJITNAResourcesExecutionPolicy</a> — Aggiornamento di una policy	Autorizzazioni aggiunte da Systems Manager per consentire Systems Manager di etichettare i ruoli IAM creati per l'accesso ai nodi just-in-time.	30 aprile 2025
<a href="#">AWSSystemsManagerJustInTimeAccessTokenSessionPolicy</a> : nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Systems Manager di applicare autorizzazioni limitate a un token di accesso al nodo just-in-time.	30 aprile 2025

Modifica	Descrizione	Data
<a href="#">AWSSystemsManagerNotificationsServicePolicy:</a> nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Systems Manager di inviare le notifiche e-mail per le richieste di accesso ai nodi just-in-time agli approvatori delle richieste di accesso.	30 aprile 2025
<a href="#">AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy:</a> nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Systems Manager di replicare le policy di approvazione in diverse Regioni.	30 aprile 2025
<a href="#">AWSSystemsManagerJustInTimeAccessTokenPolicy:</a> nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Systems Manager di generare token di accesso utilizzati per l'accesso ai nodi just-in-time.	30 aprile 2025
<a href="#">AWSSystemsManagerJustInTimeAccessServicePolicy:</a> nuova policy	Systems Manager ha aggiunto una nuova policy per fornire le autorizzazioni alle risorse gestite da AWS o utilizzate dalla funzionalità di accesso al nodo just-in-time di Systems Manager.	30 aprile 2025
<a href="#">AWSQuickSetupManagerJITNAResourcesExecutionPolicy:</a> nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Quick Setup, in Systems Manager, di creare i ruoli IAM necessari per l'accesso just-in-time ai nodi.	30 aprile 2025

Modifica	Descrizione	Data
<a href="#">AWSQuickSetupJITNADeploymentRolePolicy</a> : nuova policy	Systems Manager ha aggiunto una nuova policy che fornisce le autorizzazioni a Quick Setup per implementare il tipo di configurazione richiesto per configurare l'accesso ai nodi just-in-time.	30 aprile 2025
<a href="#">AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy</a> : nuova policy	Systems Manager ha aggiunto una nuova policy che autorizza un account operativo a diagnosticare problemi con i nodi, fornendo autorizzazioni specifiche dell'organizzazione.	21 novembre 2024
<a href="#">AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy</a> : nuova policy	Systems Manager ha aggiunto una nuova policy che autorizza un account operativo a diagnosticare problemi con i nodi, fornendo autorizzazioni specifiche dell'organizzazione.	21 novembre 2024
<a href="#">AWS-SSM-Automation-DiagnosisBucketPolicy</a> : nuova policy	Systems Manager ha aggiunto una nuova policy per supportare l'avvio di flussi di lavoro di automazione che diagnosticano i problemi con i nodi gestiti in account e Regioni specifici.	21 novembre 2024

Modifica	Descrizione	Data
<a href="#"><u>AmazonSSMServiceRolePolicy</u></a> : aggiornamento di una policy esistente	Systems Manager ha aggiunto nuove autorizzazioni per consentire di Esploratore di risorse AWS raccogliere dettagli sulle istanze Amazon EC2 e visualizzare i risultati nei widget nella nuova dashboard. Systems Manager	21 novembre 2024
<a href="#"><u>SSMQuickSetupRolePolicy</u></a> : aggiornamento di una policy esistente	Systems Manager ha aggiornato la policy gestita SSMQuickSetupRolePolicy. Questi aggiornamenti consentono al ruolo AWSServiceRoleForSSMQuickSetup associato al servizio di gestire le sincronizzazioni dei dati delle risorse.	21 novembre 2024
<a href="#"><u>AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy</u></a> : nuova policy	Systems Manager ha aggiunto una nuova policy per supportare l'avvio di flussi di lavoro di automazione che diagnosticano i problemi con i nodi gestiti in account e Regioni specifici.	21 novembre 2024
<a href="#"><u>AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy</u></a> : nuova policy	Systems Manager ha aggiunto una nuova policy per supportare l'avvio di flussi di lavoro di automazione che diagnosticano i problemi con i nodi gestiti in un account e in una Regione specifici.	21 novembre 2024

Modifica	Descrizione	Data
<a href="#"><u>AWS-SSM-RemediationAutomation-AdministrationRolePolicy</u></a> : nuova policy	Systems Manager ha aggiunto una nuova policy per supportare l'avvio di flussi di lavoro di automazione che risolvono i problemi nei nodi gestiti in account e Regioni specifici.	21 novembre 2024
<a href="#"><u>AWS-SSM-RemediationAutomation-ExecutionRolePolicy</u></a> : nuova policy	Systems Manager ha aggiunto una nuova policy per supportare l'avvio di flussi di lavoro di automazione che risolvono i problemi nei nodi gestiti in un account e in una Regione specifici.	21 novembre 2024
<a href="#"><u>AWSQuickSetupSSMDeploymentRolePolicy</u></a> — Aggiornamento di una policy	Systems Manager ha aggiunto le autorizzazioni per consentire a Systems Manager di etichettare i ruoli IAM e Lambda creati per la console unificata.	7 maggio 2025
<a href="#"><u>AWSQuickSetupSSMManagementResourcesExecutionPolicy</u></a> : nuova policy	Systems Manager ha aggiunto una nuova policy per supportare l'esecuzione di un'operazione in Quick Setup che crea ruoli IAM per le associazioni di Quick Setup, che a loro volta vengono creati da un'implementazione <code>AWSQuickSetupType-SSM</code> .	21 novembre 2024



Modifica	Descrizione	Data
<a href="#"><u>AWSQuickSetupSSMLifecycleManagementExecutionPolicy</u></a> : nuova policy	Systems Manager ha aggiunto una nuova policy per supportare l'Quick Setup esecuzione di una risorsa CloudFormation personalizzata sugli eventi del ciclo di vita durante una Quick Setup distribuzione.	21 novembre 2024
<a href="#"><u>AWSQuickSetupSSMDeploymentRolePolicy</u></a> : nuova policy	Systems Manager ha aggiunto una nuova policy per supportare la concessione di autorizzazioni amministrative che consentono a Quick Setup di creare risorse da utilizzare durante il processo di onboarding di Systems Manager.	21 novembre 2024
<a href="#"><u>AWSQuickSetupSSMDeploymentS3BucketRolePolicy</u></a> : nuova policy	Systems Manager ha aggiunto una nuova politica per supportare la gestione e il recupero di informazioni su bucket specifici nell'account principale gestiti tramite modelli CloudFormation	21 novembre 2024

Modifica	Descrizione	Data
<a href="#">AWSQuickSetupEnableDHMCExecutionPolicy</a> : nuova policy	Systems Manager sta introducendo una nuova policy per consentire a Quick Setup di creare un ruolo IAM che a sua volta utilizza quello esistente <a href="#">AmazonSSManagedEC2InstanceDefaultPolicy</a> . Questa policy contiene tutte le autorizzazioni necessarie all'SSM Agent per comunicare con il servizio Systems Manager. La nuova policy consente inoltre di modificare le impostazioni del servizio Systems Manager.	21 novembre 2024
<a href="#">AWSQuickSetupEnableAREXExecutionPolicy</a> : nuova policy	Systems Manager ha aggiunto una nuova policy per consentire la creazione di un ruolo collegato Quick Setup ai servizi per Esploratore di risorse AWS l'accesso alle viste di Resource Explorer e agli indici degli aggregatori.	21 novembre 2024

Modifica	Descrizione	Data
<a href="#"><u>AWSQuickSetupManagedInstanceProfileExecutionPolicy</u></a> : nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Quick Setup di creare un profilo dell'istanza predefinito in Quick Setup e di collegarlo a qualsiasi istanza Amazon EC2 priva di un profilo dell'istanza associato. Questa nuova politica consente inoltre di allegare autorizzazioni Quick Setup ai profili esistenti per assicurarsi che tutte le autorizzazioni richieste da Systems Manager siano state concesse.	21 novembre 2024
<a href="#"><u>SSMQuickSetupRolePolicy</u></a> : aggiornamento di una policy esistente	Systems Manager ha aggiunto nuove autorizzazioni per consentire Quick Setup di verificare lo stato degli AWS CloudFormation stack set aggiuntivi che ha creato.	13 agosto 2024
<a href="#"><u>AmazonSSMManagedEC2InstanceDefaultPolicy</u></a> : aggiornamento di una policy esistente	Systems Manager ha aggiunto gli ID di dichiarazione (Sid) alla policy JSON per AmazonSSMManagedEC2InstanceDefaultPolicy. Questi Sid forniscono descrizioni in linea dello scopo di ciascuna dichiarazione di policy.	18 luglio 2024

Modifica	Descrizione	Data
<a href="#">SSMQuickSetupRolePolicy</a> : nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Quick Setup di verificare lo stato delle risorse implementate e correggere le istanze con deviazioni dalla configurazione originale.	3 luglio 2024
<a href="#">AWSQuickSetupDeploymentRolePolicy</a> : nuova policy	Systems Manager ha aggiunto una nuova policy per supportare più tipi di Configurazione rapida che creano ruoli e automazioni IAM, che a loro volta configurano i servizi e le funzionalità di Amazon Web Services usati di frequente con le best practice consigliate.	3 luglio 2024
<a href="#">AWSQuickSetupPatchPolicyDeploymentRolePolicy</a> - Nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Quick Setup di creare risorse associate con le configurazioni in Quick Setup delle policy di patch di Patch Manager.	3 luglio 2024
<a href="#">AWSQuickSetupPatchPolicyBaselineAccess</a> : nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Quick Setup di accedere alle baseline delle patch in Patch Manager con autorizzazioni di sola lettura.	3 luglio 2024

Modifica	Descrizione	Data
<a href="#"><u>AWSSystemsManagerEnableExplorerExecutionPolicy</u></a> : nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Quick Setup di concedere le autorizzazioni amministrative per l'abilitazione di Explorer.	3 luglio 2024
<a href="#"><u>AWSSystemsManagerEnableConfigRecordingExecutionPolicy</u></a> : nuova policy	Systems Manager ha aggiunto una nuova politica per consentire di Quick Setup abilitare e configurare la registrazione delle AWS Config configurazioni.	3 luglio 2024
<a href="#"><u>AWSQuickSetupDevOpsGuruPermissionsBoundary</u></a> : nuova policy	Systems Manager ha aggiunto una nuova policy Quick Setup per consentire l'attivazione e la configurazione di Amazon DevOps Guru.	3 luglio 2024
<a href="#"><u>AWSQuickSetupDistributorPermissionsBoundary</u></a> : nuova policy	Systems Manager ha aggiunto una nuova policy per consentire di Quick Setup abilitare e configurare Distributor, uno strumento in AWS Systems Manager	3 luglio 2024
<a href="#"><u>AWSQuickSetupSSMHostMgmtPermissionsBoundary</u></a> : nuova policy	Systems Manager ha aggiunto una nuova policy per consentire di Quick Setup abilitare e configurare gli strumenti di Systems Manager per la gestione sicura delle istanze Amazon EC2.	3 luglio 2024

Modifica	Descrizione	Data
<a href="#"><u>AWSQuickSetupPatchPolicyPermissionsBoundary</u></a> : nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Quick Setup di abilitare e configurare le policy di patch in Patch Manager, uno strumento di AWS Systems Manager.	3 luglio 2024
<a href="#"><u>AWSQuickSetupSchedulerPermissionsBoundary</u></a> : nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Quick Setup di abilitare e configurare le operazioni pianificate su istanze Amazon EC2 e altre risorse.	3 luglio 2024
<a href="#"><u>AWSQuickSetupCFGCPacksPermissionsBoundary</u></a> : nuova policy	Systems Manager ha aggiunto una nuova policy per consentire a Quick Setup di implementare i pacchetti di conformità AWS Config .	3 luglio 2024
<a href="#"><u>AWSSystemsManagerOpsDataSyncServiceRolePolicy</u></a> : aggiornamento di una policy esistente	OpsCenter ha aggiornato la policy per migliorare la sicurezza del codice di servizio all'interno del ruolo collegato al servizio per la gestione delle operazioni. Explorer OpsData-related	3 luglio 2023
<a href="#"><u>AmazonSSMManagedEC2InstanceDefaultPolicy</u></a> : nuova policy	Systems Manager ha aggiunto una nuova policy per consentire la funzionalità Systems Manager nelle istanze Amazon EC2 senza l'uso di un profilo dell'istanza IAM.	18 agosto 2022

Modifica	Descrizione	Data
<a href="#">AmazonSSMServiceRolePolicy</a> : aggiornamento di una policy esistente	Systems Manager ha aggiunto nuove autorizzazioni per consentire la creazione Explorer di una regola gestita quando si attiva Security Hub CSPM da o. Explorer OpsCenter Sono state aggiunte nuove autorizzazioni per verificare che la configurazione e il compute-optimizer soddisfino i requisiti necessari prima di autorizzarli. OpsData	27 aprile 2021
<a href="#">AWSSystemsManagerOpsDataSyncServiceRolePolicy</a> : nuova policy	Systems Manager ha aggiunto una nuova policy per la creazione e l'aggiornamento e OpsData dai risultati del CSPM di Security Hub in OpsItems e. Explorer OpsCenter	27 aprile 2021
<a href="#">AmazonSSMServiceRolePolicy</a> : aggiornamento di una policy esistente	Systems Manager ha aggiunto nuove autorizzazioni per consentire la visualizzazione aggregata e dei OpsItems dettagli da più account OpsData e in. Regioni AWS Explorer	24 marzo 2021
Systems Manager Rilevamento delle modifiche	Systems Manager ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	12 marzo 2021

## Polity gestite aggiuntive per Systems Manager

Oltre alle politiche gestite descritte in precedenza in questo argomento, Systems Manager supporta anche le seguenti politiche.

- [AmazonSSMAutomationApproverAccess](#): policy gestita da AWS di attendibilità dell'utente che consente l'accesso per visualizzare le esecuzioni delle automazioni e inviare le decisioni di approvazione all'automazione in attesa di approvazione.
- [AmazonSSMDirectoryServiceAccess](#)— policy AWS gestita che consente di accedere SSM Agent per Directory Service conto dell'utente alle richieste di accesso al dominio da parte del nodo gestito.
- [AmazonSSMFullAccess](#)— policy AWS gestita che garantisce l'accesso completo all'Systems ManagerAPI e ai documenti.
- [AmazonSSMMaintenanceWindowRole](#): policy gestita da AWS che fornisce alle finestre di manutenzione le autorizzazioni per API di Systems Manager.
- [AmazonSSManagedInstanceCore](#): policy gestita da AWS che consente a un nodo di utilizzare la funzionalità principale del servizio di Systems Manager.
- [AmazonSSMPatchAssociation](#): policy gestita da AWS che fornisce l'accesso alle istanze secondarie per le operazioni di applicazione di patch.
- [AmazonSSMReadOnlyAccess](#): policy gestita da AWS che consente l'accesso alle operazioni API di Systems Manager in sola lettura, come `Get*` and `List*`.
- [AWSSSMOpsInsightsServiceRolePolicy](#)— policy AWS gestita che fornisce le autorizzazioni per la creazione e l'aggiornamento delle informazioni OpsItems operative in Systems Manager Utilizzata per fornire autorizzazioni tramite il ruolo collegato al servizio [AWSServiceRoleForAmazonSSM\\_OpsInsights](#).
- [AWSSystemsManagerAccountDiscoveryServicePolicy](#)— policy AWS gestita che concede a Systems Manager l'autorizzazione a scoprire Account AWS informazioni.
- [AmazonEC2RoleforSSM](#): questa policy non è più supportata e non deve essere utilizzata. Al suo posto, utilizza la policy [AmazonSSManagedInstanceCore](#) per consentire la funzionalità di base del servizio Systems Manager sulle istanze EC2. Per informazioni, consulta la pagina [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#).



# Risoluzione dei problemi di identità e accesso in AWS Systems Manager

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con AWS Systems Manager and AWS Identity and Access Management (IAM).

## Argomenti

- [Non sono autorizzato a eseguire un'operazione in Systems Manager](#)
- [Non sono autorizzato a eseguire iam: PassRole](#)
- [Voglio consentire a persone esterne a me di accedere Account AWS alle mie Systems Manager risorse](#)

## Non sono autorizzato a eseguire un'operazione in Systems Manager

Se ti Console di gestione AWS dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso.

L'errore di esempio seguente si verifica quando l'utente mateojackson tenta di utilizzare la console per visualizzare i dettagli relativi a un documento, ma non dispone delle autorizzazioni `ssm:GetDocument`.

```
User: arn:aws:ssm::123456789012:user/mateojackson isn't authorized to perform:
 ssm:GetDocument on resource: MyExampleDocument
```

In questo caso, Mateo chiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa `MyExampleDocument` mediante l'operazione `ssm:GetDocument`.

## Non sono autorizzato a eseguire iam: PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a Systems Manager.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in Systems Manager. Tuttavia, l'operazione richiede

che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

## Voglio consentire a persone esterne a me di accedere Account AWS alle mie Systems Manager risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizzare tali policy per concedere alle persone l'accesso alle proprie risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per capire se Systems Manager supporta queste funzionalità, consulta [In che modo AWS Systems Manager funziona con IAM](#).
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta [Fornire l'accesso a un utente IAM di un altro Account AWS utente di tua proprietà](#) nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a soggetti Account AWS di proprietà di terze parti](#) nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(federazione delle identità\)](#) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

## Utilizzo di ruoli collegati ai servizi per Systems Manager

AWS Systems Manager utilizza ruoli collegati ai [servizi AWS Identity and Access Management](#) (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. Systems

Manager Service-linked i ruoli sono predefiniti Systems Manager e includono tutte le autorizzazioni richieste dal servizio per chiamare altri Servizi AWS utenti per tuo conto.

#### Note

Un ruolo di servizio è diverso da un ruolo collegato al servizio. Un ruolo di servizio è un tipo di ruolo AWS Identity and Access Management (IAM) che concede le autorizzazioni a un utente in Servizio AWS modo che il servizio possa accedere alle risorse. AWS Solo alcuni scenari di Systems Manager richiedono un ruolo di servizio. Quando si crea un ruolo di servizio per Systems Manager, si scelgono le autorizzazioni da concedere, affinché questo possa accedere o interagire con altre risorse AWS .

Un ruolo collegato ai servizi semplifica la configurazione di Systems Manager perché non dovrai più aggiungere manualmente le autorizzazioni necessarie. Systems Manager definisce le autorizzazioni dei relativi ruoli associati ai servizi e, salvo diversamente definito, Systems Manager potrà assumere solo i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato al servizio solo dopo avere eliminato le risorse correlate. Questa procedura protegge le risorse Systems Manager poiché impedisce la rimozione involontaria dell'autorizzazione ad accedere alle risorse.

#### Note

Per i nodi non EC2 in un ambiente [ibrido e multicloud](#), è necessario disporre di un ruolo IAM aggiuntivo che consenta alle macchine di comunicare con il servizio Systems Manager. Questo è il ruolo di servizio IAM per Systems Manager. Questo ruolo concede Servizio di token di sicurezza AWS (AWS STS) AssumeRolefiducia al servizio. Systems Manager L'operazione AssumeRole restituisce un set di credenziali di sicurezza temporanee (ovvero l'ID chiave di accesso, una chiave di accesso segreta e un token di sicurezza). Utilizzate queste credenziali temporanee per accedere a AWS risorse a cui normalmente non potreste avere accesso. Per ulteriori informazioni, consulta [Creare il ruolo di servizio IAM richiesto per Systems Manager in ambienti ibridi e multicloud](#) e [AssumeRole](#) nel riferimento [Servizio di token di sicurezza AWS API](#).

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta [Servizi AWS quelli compatibili con IAM](#) e cerca i servizi con 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.

#### Note

Systems Manager Automation non utilizza più il ruolo collegato ai servizi per il monitoraggio degli CloudWatch allarmi. Questa operazione ora utilizza l'identità di esecuzione del runbook. Assicurati che la tua identità di esecuzione disponga delle autorizzazioni richieste. Per ulteriori informazioni, consulta [Configurazione delle automazioni per monitorare gli allarmi CloudWatch](#).

## Argomenti

- [Utilizzo dei ruoli per raccogliere l'inventario e visualizzare OpsData](#)
- [Usare i ruoli per raccogliere Account AWS informazioni per OpsCenter and Explorer](#)
- [Usare i ruoli per creare OpsData e OpsItems per Explorer](#)
- [Utilizzo dei ruoli per creare informazioni operative OpsItems in Systems Manager OpsCenter](#)
- [Utilizzo dei ruoli per mantenere l'integrità e la coerenza delle risorse fornite da Quick Setup](#)
- [Utilizzo dei ruoli per l'esportazione Explorer OpsData](#)
- [Utilizzo dei ruoli per abilitare l'accesso ai nodi just-in-time](#)
- [Utilizzo dei ruoli per inviare notifiche di richiesta di accesso ai nodi just-in-time](#)

## Utilizzo dei ruoli per raccogliere l'inventario e visualizzare OpsData

Systems Manager utilizza il ruolo collegato al servizio denominato.

**AWSServiceRoleForAmazonSSM** AWS Systems Manager utilizza questo ruolo del servizio IAM per gestire AWS le risorse per tuo conto.

### Service-linked autorizzazioni di ruolo per l'inventario OpsData e OpsItems

Il ruolo collegato ai servizi `AWSServiceRoleForAmazonSSM` considera attendibile solo `ssm.amazonaws.com` ai fini dell'assunzione del ruolo.

È possibile utilizzare il ruolo collegato ai servizi `AWSServiceRoleForAmazonSSM` di Systems Manager nei seguenti casi:

- Lo strumento inventario di Systems Manager usa il ruolo collegato a un servizio `AWSServiceRoleForAmazonSSM` per raccogliere i metadati dell'inventario da tag e gruppi di risorse.
- Lo Explorer strumento utilizza il ruolo collegato al servizio `AWSServiceRoleForAmazonSSM` per consentire la visualizzazione OpsData e OpsItems da più account. Questo ruolo collegato al servizio consente inoltre di Explorer creare una regola gestita quando si abilita Security Hub CSPM come origine dati da o. Explorer OpsCenter

 Important

In precedenza, la console di Systems Manager offriva la possibilità di scegliere il ruolo AWS gestito collegato ai servizi IAM `AWSServiceRoleForAmazonSSM` da utilizzare come ruolo di manutenzione per le attività. Non è più consigliato utilizzare questo ruolo e la relativa policy associata, `AmazonSSMServiceRolePolicy`, per le attività della finestra di manutenzione. Se stai ancora utilizzando questo ruolo per le attività della finestra di manutenzione, ti invitiamo a interromperne l'utilizzo. È invece possibile creare un ruolo IAM personalizzato che consenta la comunicazione tra Systems Manager e altri utenti Servizi AWS durante l'esecuzione delle attività della finestra di manutenzione.

Per ulteriori informazioni, consulta [Configurazione Intervallo di manutenzione](#).

La policy gestita utilizzata per fornire le autorizzazioni per il ruolo `AWSServiceRoleForAmazonSSM` è `AmazonSSMServiceRolePolicy`. Per informazioni dettagliate sulle autorizzazioni necessarie, consulta [AWS politica gestita: AmazonSSMServiceRolePolicy](#).

## Creazione del ruolo **AWSServiceRoleForAmazonSSM** collegato al servizio per Systems Manager

È possibile utilizzare la console IAM per creare un ruolo collegato ai servizi con il caso d'uso EC2. Utilizzando i comandi per IAM nella AWS Command Line Interface (AWS CLI) o utilizzando l'API IAM, crea un ruolo collegato ai servizi con il nome del servizio `ssm.amazonaws.com`. Per ulteriori informazioni, consulta [Creazione di un ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account.

## Modifica del ruolo collegato al **AWSServiceRoleForAmazonSSM** servizio per Systems Manager

Systems Manager non consente di modificare il ruolo collegato ai servizi **AWSServiceRoleForAmazonSSM**. Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

## Eliminazione del ruolo collegato al servizio per **AWSServiceRoleForAmazonSSM** Systems Manager

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare quel ruolo. In questo modo non hai un'entità non utilizzata che non viene monitorata o gestita attivamente. Puoi utilizzare la console IAM, l'API IAM o l'AWS CLI API IAM per eliminare manualmente il ruolo collegato al servizio. Per fare ciò, devi prima pulire manualmente le risorse per il tuo ruolo collegato al servizio. Quindi, puoi eliminarlo manualmente.

Poiché il ruolo **AWSServiceRoleForAmazonSSM** collegato al servizio può essere utilizzato da più strumenti, assicurati che nessuno stia utilizzando il ruolo prima di tentare di eliminarlo.

- **Inventario:** se si elimina il ruolo collegato ai servizi utilizzato dall'inventario, i dati dell'inventario per i tag e i gruppi di risorse non saranno più sincronizzati. È necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.
- **Explorer:** se elimini il ruolo collegato al servizio utilizzato dallo Explorer strumento, i ruoli interaccount e OpsData interregionale non sono più visualizzabili. **OpsItems**

### Note

Se il servizio Systems Manager utilizza tale ruolo quando tenti di eliminare i tag o i gruppi di risorse, è possibile che l'eliminazione non abbia esito positivo. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare Systems Manager risorse utilizzate da **AWSServiceRoleForAmazonSSM**

1. Per eliminare i tag, vedi [Aggiunta ed eliminazione di tag in una singola risorsa](#).
2. Per eliminare i gruppi di risorse, consulta [Eliminare i gruppi da AWS Resource Groups](#).

Per eliminare manualmente il ruolo collegato ai servizi **AWSServiceRoleForAmazonSSM** utilizzando IAM

Usa la console IAM AWS CLI, l'API IAM o l'API IAM per eliminare il ruolo **AWSServiceRoleForAmazonSSM** collegato al servizio. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

## Regioni supportate per Systems Manager Ruolo collegato ai servizi **AWSServiceRoleForAmazonSSM**

Systems Manager supporta l'utilizzo del ruolo **AWSServiceRoleForAmazonSSM** collegato al servizio in tutti i luoghi in Regioni AWS cui il servizio è disponibile. Per ulteriori informazioni, consulta [Endpoint e quote per AWS Systems Manager](#).

## Usare i ruoli per raccogliere Account AWS informazioni per OpsCenter and Explorer

Systems Manager utilizza il ruolo collegato al servizio denominato.

**AWSServiceRoleForAmazonSSM\_AccountDiscovery** AWS Systems Manager utilizza questo ruolo del servizio IAM per chiamare altri utenti Servizi AWS per scoprire Account AWS informazioni.

## Service-linked autorizzazioni di ruolo per Systems Manager individuazione dell'account

Ai fini dell'assunzione del ruolo, il ruolo collegato al servizio

**AWSServiceRoleForAmazonSSM\_AccountDiscovery** considera attendibili i seguenti servizi:

- `accountdiscovery.ssm.amazonaws.com`

La policy delle autorizzazioni del ruolo consente ad Systems Manager di eseguire le seguenti operazioni sulle risorse specificate:

- `organizations:DescribeAccount`
- `organizations:DescribeOrganizationalUnit`

- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListChildren`
- `organizations:ListParents`
- `organizations:ListDelegatedServicesForAccount`
- `organizations:ListDelegatedAdministrators`
- `organizations:ListRoots`

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 del ruolo **AWSServiceRoleForAmazonSSM \_ AccountDiscovery** service-linked per Systems Manager

Se vuoi utilizzare Explorer e OpsCenter, strumenti di Systems Manager su più Account AWS, devi creare un ruolo collegato ai servizi. Per quanto riguarda OpsCenter, crea manualmente il ruolo collegato ai servizi. Per ulteriori informazioni, consulta [\(Facoltativo\) Configurazione manuale OpsCenter per gestire centralmente OpsItems tra gli account](#).

ExplorerSe si crea una sincronizzazione dei dati delle risorse utilizzando Systems Manager in Console di gestione AWS, è possibile creare il ruolo collegato al servizio scegliendo il pulsante Crea ruolo. Se si desidera creare una sincronizzazione dei dati delle risorse a livello di programmazione, è necessario creare il ruolo prima di creare la sincronizzazione dei dati delle risorse. È possibile creare il ruolo utilizzando l'operazione [CreateServiceLinkedRole](#) API.

## Modifica del ruolo **AWSServiceRoleForAmazonSSM \_ AccountDiscovery** collegato al servizio per Systems Manager

Systems Manager non consente di modificare il ruolo collegato ai servizi `AWSServiceRoleForAmazonSSM_AccountDiscovery`. Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato al servizio](#) nella Guida per l'utente di IAM.



## Eliminazione del ruolo **AWSServiceRoleForAmazonSSM \_ collegato al servizio AccountDiscovery** per Systems Manager

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 hai un'entità non utilizzata che non viene monitorata o gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

### Pulizia del ruolo \_ collegato al **AWSServiceRoleForAmazonSSM servizio AccountDiscovery**

Prima di poter utilizzare IAM per eliminare un ruolo collegato ai servizi **AWSServiceRoleForAmazonSSM\_AccountDiscovery**, devi innanzitutto eliminare tutte le sincronizzazioni dei dati della risorsa Explorer.

#### Note

Se il servizio Systems 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.

### Eliminare manualmente il ruolo **AWSServiceRoleForAmazonSSM \_ collegato al servizio AccountDiscovery**

Usa la console IAM AWS CLI, l'API o l' AWS API per eliminare il ruolo collegato al **AWSServiceRoleForAmazonSSM\_AccountDiscovery** servizio. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

### Regioni supportate per Systems Manager **AWSServiceRoleForAmazonSSM\_ ruolo AccountDiscovery** collegato al servizio

Systems Manager supporta l'utilizzo di ruoli collegati al servizio in tutte le Regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta [Endpoint e quote per AWS Systems Manager](#).

### Aggiornamenti al ruolo **AWSServiceRoleForAmazonSSM \_ collegato al servizio AccountDiscovery**

Visualizza i dettagli sugli aggiornamenti del ruolo **AWSServiceRoleForAmazonSSM \_ AccountDiscovery** service-linked da quando questo servizio ha iniziato a tenere traccia di queste

modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivere il feed RSS nella pagina [Cronologia dei documenti](#) di Systems Manager.

Modifica	Descrizione	Data
Nuove autorizzazioni aggiunte	Questo ruolo collegato ai servizi include ora le autorizzazioni <code>organizations:DescribeOrganizationalUnit</code> e <code>organizations:ListRoots</code> . Queste autorizzazioni consentono a un account di AWS Organizations gestione o a un account amministratore delegato di Systems Manager di lavorare con più account. OpsItems Per ulteriori informazioni, consulta <a href="#">(Facoltativo) Configurazione manuale OpsCenter per gestire centralmente OpsItems tra gli account</a> .	17 ottobre 2022

## Usare i ruoli per creare OpsData e OpsItems per Explorer

Systems Manager utilizza il ruolo collegato al servizio denominato.

**AWSServiceRoleForSystemsManagerOpsDataSync** AWS Systems Manager utilizza questo ruolo di servizio IAM per Explorer creare OpsData e. OpsItems

### Service-linked autorizzazioni di ruolo per la sincronizzazione Systems Manager OpsData

Ai fini dell'assunzione del ruolo, il ruolo collegato al servizio

**AWSServiceRoleForSystemsManagerOpsDataSync** considera attendibili i seguenti servizi:

- `opsdatasync.ssm.amazonaws.com`

La policy delle autorizzazioni del ruolo consente ad Systems Manager di eseguire le seguenti operazioni sulle risorse specificate:

- Systems Manager Explorer richiede che un ruolo collegato al servizio conceda l'autorizzazione per aggiornare un risultato di sicurezza quando un OpsItem viene aggiornato, creare e aggiornare un'OpsItemorigine dati CSPM Security Hub e disattivare l'origine dati CSPM Security Hub quando una regola gestita SSM viene eliminata dai clienti.

La policy gestita utilizzata per fornire le autorizzazioni per il ruolo `AWSServiceRoleForSystemsManagerOpsDataSync` è `AWSSystemsManagerOpsDataSyncServiceRolePolicy`. Per informazioni dettagliate sulle autorizzazioni necessarie, consulta [AWS politica gestita: AWSSystemsManagerOpsDataSyncServiceRolePolicy](#).

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](#) Guida per l'utente IAM.

## Creazione del ruolo collegato ai servizi

### **AWSServiceRoleForSystemsManagerOpsDataSync** per Systems Manager

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando lo abiliti Explorer in Console di gestione AWS, Systems Manager crea automaticamente il ruolo collegato al servizio.

#### Important

Questo ruolo collegato al servizio può apparire nell'account, se è stata completata un'operazione in un altro servizio che utilizza le caratteristiche supportate da questo ruolo. Inoltre, se usavi il servizio Systems Manager prima del 1° gennaio 2017, data da cui è disponibile il supporto dei ruoli collegati ai servizi, Systems Manager ha creato il ruolo `AWSServiceRoleForSystemsManagerOpsDataSync` nel tuo account. Per ulteriori informazioni, consulta [Un nuovo ruolo è apparso nel mio account IAM](#).

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando lo abiliti Explorer in Console di gestione AWS, Systems Manager crea nuovamente il ruolo collegato al servizio per te.

Puoi anche utilizzare la console IAM per creare un ruolo collegato al servizio con il ruolo di AWS servizio che consente di creare OpsData e utilizzare Explorer case. OpsItems Nella AWS CLI o nell' AWS API, crea un ruolo collegato al servizio con il nome del servizio. `opsdatasync.ssm.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

### **AWSServiceRoleForSystemsManagerOpsDataSync** per Systems Manager

Systems Manager non consente di modificare il ruolo collegato ai servizi

`AWSServiceRoleForSystemsManagerOpsDataSync`. Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

## Eliminazione di un ruolo collegato ai servizi

### **AWSServiceRoleForSystemsManagerOpsDataSync** per Systems Manager

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 hai un'entità non utilizzata che non viene monitorata o gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

#### Note

Se il servizio Systems 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.

La procedura per eliminare Systems Manager le risorse utilizzate dal `AWSServiceRoleForSystemsManagerOpsDataSync` ruolo dipende dalla configurazione Explorer o OpsCenter dall'integrazione con Security Hub CSPM.

Per eliminare le risorse di Systems Manager utilizzate da

### **AWSServiceRoleForSystemsManagerOpsDataSync**

- Per interrompere la creazione Explorer di nuovi OpsItems risultati CSPM di Security Hub, vedere. [Come interrompere l'invio degli esiti](#)
- Per interrompere la creazione OpsCenter di nuovi OpsItems risultati CSPM di Security Hub, vedere

Per eliminare manualmente il ruolo collegato ai servizi

### **AWSServiceRoleForSystemsManagerOpsDataSync** utilizzando IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al **AWSServiceRoleForSystemsManagerOpsDataSync** servizio. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

Regioni supportate per il Systems Manager

### **AWSServiceRoleForSystemsManagerOpsDataSync** ruolo collegati ai servizi

Systems Manager supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta [Endpoint e quote per AWS Systems Manager](#).

Systems Manager non supporta l'utilizzo di ruoli collegati ai servizi in ogni regione nella quale è disponibile il servizio. Il ruolo **AWSServiceRoleForSystemsManagerOpsDataSync** può essere utilizzato nelle Regioni seguenti.

Regione AWS nome	Identità della Regione	Supporto in Systems 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
Asia Pacifico (Mumbai)	ap-south-1	Sì

Regione AWS nome	Identità della Regione	Supporto in Systems Manager
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
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
Europa (Parigi)	eu-west-3	Sì
Europa (Stoccolma)	eu-north-1	Sì
Sud America (San Paolo)	sa-east-1	Sì
AWS GovCloud (US)	us-gov-west-1	No

## Utilizzo dei ruoli per creare informazioni operative OpsItems in Systems Manager OpsCenter

Systems Manager utilizza il ruolo collegato al servizio denominato.

**AWSServiceRoleForAmazonSSM\_OpsInsights** AWS Systems Manager utilizza questo ruolo di servizio IAM per creare e aggiornare informazioni operative OpsItems in Systems Manager OpsCenter.

## **AWSServiceRoleForAmazonSSM\_OpsInsights** autorizzazioni relative ai ruoli collegati ai servizi per informazioni operative Systems Manager OpsItems

Ai fini dell'assunzione del ruolo, il ruolo collegato al servizio

AWSServiceRoleForAmazonSSM\_OpsInsights considera attendibili i seguenti servizi:

- `opsinsights.ssm.amazonaws.com`

La policy delle autorizzazioni del ruolo consente ad Systems Manager di eseguire le seguenti operazioni sulle risorse specificate:

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "AllowCreateOpsItem",
 "Effect": "Allow",
 "Action": [
 "ssm:CreateOpsItem",
 "ssm:AddTagsToResource"
],
 "Resource": "*"
 },
 {
 "Sid": "AllowAccessOpsItem",
 "Effect": "Allow",
 "Action": [
 "ssm:UpdateOpsItem",
 "ssm:GetOpsItem"
],
 "Resource": "*",
 "Condition": {
 "StringEquals": {
 "aws:ResourceTag/SsmOperationalInsight": "true"
 }
 }
 }
]
}
```

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 Guida](#) per l'utente IAM.

## Creazione del ruolo collegato ai servizi

### **AWSServiceRoleForAmazonSSM\_OpsInsights** per Systems Manager

È necessario creare un ruolo collegato ai servizi. Se abiliti gli approfondimenti operativi utilizzando Systems Manager in Console di gestione AWS, puoi creare il ruolo collegato al servizio scegliendo il pulsante Abilita.

## Modifica di un ruolo collegato ai servizi

### **AWSServiceRoleForAmazonSSM\_OpsInsights** per Systems Manager

Systems Manager non consente di modificare il ruolo collegato ai servizi **AWSServiceRoleForAmazonSSM\_OpsInsights**. 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 ai servizi](#) nella Guida per l'utente IAM.

## Eliminazione di un ruolo collegato ai servizi

### **AWSServiceRoleForAmazonSSM\_OpsInsights** per Systems Manager

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti 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.

### Pulizia del ruolo collegato ai servizi **AWSServiceRoleForAmazonSSM\_OpsInsights**

Per utilizzare IAM per eliminare il ruolo collegato ai servizi

**AWSServiceRoleForAmazonSSM\_OpsInsights**, prima occorre disattivare gli approfondimenti operativi in OpsCenter di Systems Manager. Per ulteriori informazioni, consulta [Analisi delle informazioni operative per ridurre OpsItems](#).



## Eliminazione manuale del ruolo collegato ai servizi

### **AWSServiceRoleForAmazonSSM\_OpsInsights**

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al **AWSServiceRoleForAmazonSSM\_OpsInsights** servizio. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

## Regioni supportate per il Systems Manager

### **AWSServiceRoleForAmazonSSM\_OpsInsights** ruolo collegati ai servizi

Systems Manager non supporta l'utilizzo di ruoli collegati ai servizi in ogni regione nella quale è disponibile il servizio. Puoi utilizzare il OpsInsights ruolo **AWSServiceRoleForAmazonSSM \_** nelle seguenti regioni.

Nome della Regione	Identità della Regione	Supporto in Systems 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
Asia Pacifico (Mumbai)	ap-south-1	Sì
Asia Pacifico (Tokyo)	ap-northeast-1	Sì
Asia Pacifico (Seoul)	ap-northeast-2	Sì
Asia Pacifico (Singapore)	ap-southeast-1	Sì
Asia Pacifico (Sydney)	ap-southeast-2	Sì
Asia Pacific (Hong Kong)	ap-east-1	Sì
Canada (Centrale)	ca-central-1	Sì

Nome della Regione	Identità della Regione	Supporto in Systems Manager
Europa (Francoforte)	eu-central-1	Sì
Europa (Irlanda)	eu-west-1	Sì
Europa (Londra)	eu-west-2	Sì
Europa (Parigi)	eu-west-3	Sì
Europa (Stoccolma)	eu-north-1	Sì
Europe (Milan)	eu-south-1	Sì
Sud America (San Paolo)	sa-east-1	Sì
Medio Oriente (Bahrein)	me-south-1	Sì
Africa (Città del Capo)	af-south-1	Sì
AWS GovCloud (US)	us-gov-west-1	Sì
AWS GovCloud (US)	us-gov-east-1	Sì

## Utilizzo dei ruoli per mantenere l'integrità e la coerenza delle risorse fornite da Quick Setup

Systems Manager usa il ruolo collegato ai servizi denominato **AWSServiceRoleForSSMQuickSetup**.

### Autorizzazioni del ruolo collegato ai servizi **AWSServiceRoleForSSMQuickSetup** per Systems Manager

Ai fini dell'assunzione del ruolo, il ruolo collegato al servizio **AWSServiceRoleForSSMQuickSetup** considera attendibili i seguenti servizi:

- `ssm-quicksetup.amazonaws.com`

AWS Systems Manager utilizza questo ruolo di servizio IAM per verificare lo stato della configurazione, garantire un uso coerente dei parametri e delle risorse assegnate e correggere le risorse quando viene rilevata una deriva.

La policy delle autorizzazioni del ruolo consente ad Systems Manager di eseguire le seguenti operazioni sulle risorse specificate:

- `ssm` (Systems Manager): legge le informazioni sullo stato in cui è necessario che si trovino le risorse configurate, inclusi gli account degli amministratori delegati.
- `iam` (AWS Identity and Access Management): è necessario affinché le sincronizzazioni dei dati sulle risorse siano accessibili in tutte le organizzazioni in AWS Organizations.
- `organizations` (AWS Organizations): legge le informazioni sugli account dei membri che appartengono a un'organizzazione come configurato in Organizations.
- `cloudformation`(CloudFormation) — Legge le informazioni sugli CloudFormation stack utilizzati per gestire lo stato delle risorse e le operazioni dello stackset. CloudFormation

La policy gestita utilizzata per fornire le autorizzazioni per il ruolo `AWSServiceRoleForSSMQuickSetup` è [SSMQuickSetupRolePolicy](#). Per informazioni dettagliate sulle autorizzazioni necessarie, consulta [AWS politica gestita: SSMQuickSetupRolePolicy](#).

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 Guida](#) per l'utente IAM.

## Creazione del ruolo collegato ai servizi **AWSServiceRoleForSSMQuickSetup** per Systems Manager

Non è necessario creare manualmente il ruolo collegato al `AWSServiceRoleForSSMQuickSetup` servizio. Quando esegui una configurazione Quick Setup nella Console di gestione AWS, Systems Manager crea automaticamente il ruolo collegato ai servizi.

## Modifica di un ruolo collegato ai servizi **AWSServiceRoleForSSMQuickSetup** per Systems Manager

Systems Manager non consente di modificare il ruolo collegato ai servizi `AWSServiceRoleForSSMQuickSetup`. 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 ai servizi](#) nella Guida per l'utente IAM.

## Eliminazione di un ruolo collegato ai servizi **AWSServiceRoleForSSMQuickSetup** per Systems Manager

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti 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.

### Pulizia del ruolo collegato ai servizi **AWSServiceRoleForSSMQuickSetup**

Prima di utilizzare IAM per eliminare il ruolo collegato al servizio **AWSServiceRoleForSSMQuickSetup**, è necessario prima rimuovere le configurazioni di Quick Setup che utilizzano il ruolo. Per ulteriori informazioni, consulta [Modifica ed eliminazione della configurazione](#).

### Eliminazione manuale del ruolo collegato ai servizi **AWSServiceRoleForSSMQuickSetup**

Utilizza la console IAM AWS CLI, l'API AWS per eliminare il ruolo collegato al **AWSServiceRoleForSSMQuickSetup** servizio. Per ulteriori informazioni, consulta i seguenti argomenti:

- [Eliminazione di un ruolo collegato ai servizi](#) nella Guida per l'utente IAM
- [delete-configuration-manager](#) nella sezione Quick Setup della Riferimenti AWS CLI
- [DeleteConfigurationManager](#) nel Documentazione di riferimento API di Quick Setup

## Regioni supportate per il Systems Manager **AWSServiceRoleForSSMQuickSetup** ruolo collegati ai servizi

Systems Manager non supporta l'utilizzo di ruoli collegati ai servizi in ogni regione nella quale è disponibile il servizio. Puoi utilizzare il **AWSServiceRoleForSSMQuickSetup** ruolo nelle seguenti regioni.

- Stati Uniti orientali (Ohio)
- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti occidentali (California settentrionale)

- Stati Uniti occidentali (Oregon)
- Asia Pacifico (Mumbai)
- Asia Pacifico (Seoul)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Tokyo)
- Canada (Centrale)
- Europa (Francoforte)
- Europa (Stoccolma)
- Europa (Irlanda)
- Europa (Londra)
- Europa (Parigi)
- Sud America (San Paolo)

## Utilizzo dei ruoli per l'esportazione Explorer OpsData

AWS Systems Manager Explorer utilizza il ruolo `AmazonSSMExplorerExportRole` di servizio per esportare i dati operativi (OpsData) utilizzando il runbook di automazione `AWS-ExportOpsDataToS3`.

### Service-linked autorizzazioni di ruolo per Explorer

Il ruolo collegato ai servizi `AmazonSSMExplorerExportRole` considera attendibile solo `ssm.amazonaws.com` ai fini dell'assunzione del ruolo.

È possibile utilizzare il ruolo `AmazonSSMExplorerExportRole` collegato al servizio per esportare i dati delle operazioni (OpsData) utilizzando il `AWS-ExportOpsDataToS3` runbook di automazione. Puoi esportare 5.000 OpsData articoli da un file con valori separati da virgole (Explorer virgole (.csv) a un bucket Amazon Simple Storage Service (Amazon S3).

La policy delle autorizzazioni del ruolo consente ad Systems Manager di eseguire le seguenti operazioni sulle risorse specificate:

- `s3:PutObject`
- `s3:GetBucketAc1`

- `s3:GetBucketLocation`
- `sns:Publish`
- `logs:DescribeLogGroups`
- `logs:DescribeLogStreams`
- `logs:CreateLogGroup`
- `logs:PutLogEvents`
- `logs:CreateLogStream`
- `ssm:GetOpsSummary`

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 del ruolo collegato al **AmazonSSMExplorerExportRole** servizio per Systems Manager

Systems Manager crea il ruolo `AmazonSSMExplorerExportRole` collegato al servizio quando si esporta OpsData utilizzando Explorer la console di Systems Manager. Per ulteriori informazioni, consulta [Esportazione OpsData da Systems Manager Explorer](#).

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account.

## Modifica del ruolo collegato al **AmazonSSMExplorerExportRole** servizio per Systems Manager

Systems Manager non consente di modificare il ruolo collegato ai servizi `AmazonSSMExplorerExportRole`. Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

## Eliminazione del ruolo collegato al servizio per **AmazonSSMExplorerExportRole** Systems Manager

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare quel ruolo. In questo modo non hai un'entità non utilizzata che non

viene monitorata o gestita attivamente. Puoi utilizzare la console IAM, l'API IAM o l'AWS CLI API IAM per eliminare manualmente il ruolo collegato al servizio. Per fare ciò, devi prima pulire manualmente le risorse per il tuo ruolo collegato al servizio. Quindi, puoi eliminarlo manualmente.

#### Note

Se il servizio Systems Manager utilizza tale ruolo quando tenti di eliminare i tag o i gruppi di risorse, è possibile che l'eliminazione non abbia esito positivo. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare Systems Manager risorse utilizzate da **AmazonSSMExplorerExportRole**

1. Per eliminare i tag, vedi [Aggiunta ed eliminazione di tag in una singola risorsa](#).
2. Per eliminare i gruppi di risorse, consulta [Eliminare i gruppi da AWS Resource Groups](#).

Per eliminare manualmente il ruolo collegato ai servizi **AmazonSSMExplorerExportRole** utilizzando IAM

Usa la console IAM AWS CLI, l'API IAM o l'API IAM per eliminare il ruolo **AmazonSSMExplorerExportRole** collegato al servizio. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

## Regioni supportate per Systems Manager Ruolo collegato ai servizi **AmazonSSMExplorerExportRole**

Systems Manager supporta l'utilizzo del ruolo **AmazonSSMExplorerExportRole** collegato al servizio in tutti i luoghi in Regioni AWS cui il servizio è disponibile. Per ulteriori informazioni, consulta [Endpoint e quote per AWS Systems Manager](#).

## Utilizzo dei ruoli per abilitare l'accesso ai nodi just-in-time

Systems Manager utilizza il ruolo collegato al servizio denominato.

**AWSServiceRoleForSystemsManagerJustInTimeAccess** AWS Systems Manager utilizza questo ruolo di servizio IAM per abilitare l'accesso al nodo just-in-time.

## Service-linked autorizzazioni di ruolo per Systems Manager l'accesso al nodo just-in-time

Ai fini dell'assunzione del ruolo, il ruolo collegato al servizio

`AWSServiceRoleForSystemsManagerJustInTimeAccess` considera attendibili i seguenti servizi:

- `ssm.amazonaws.com`

La policy delle autorizzazioni del ruolo consente ad Systems Manager di eseguire le seguenti operazioni sulle risorse specificate:

- `ssm:CreateOpsItem`
- `ssm:GetOpsItem`
- `ssm:UpdateOpsItem`
- `ssm:DescribeOpsItems`
- `ssm:DescribeSessions`
- `ssm:ListTagsForResource`
- `ssm-guiconnect:ListConnections`
- `identitystore:ListGroupMembershipsForMember`
- `identitystore:DescribeUser`
- `identitystore:GetGroupId`
- `identitystore:GetUserId`
- `sso-directory:DescribeUsers`
- `sso-directory:IsMemberInGroup`
- `sso:ListInstances`
- `sso:DescribeRegisteredRegions`
- `sso:ListDirectoryAssociations`
- `ec2:DescribeTags`

La policy gestita utilizzata per fornire le autorizzazioni per il ruolo

`AWSServiceRoleForSystemsManagerJustInTimeAccess` è

`AWSSystemsManagerEnableJustInTimeAccessPolicy`. Per informazioni



dettagliate sulle autorizzazioni necessarie, consulta [AWS politica gestita: AWSServiceRoleForSystemsManagerJustInTimeAccessServicePolicy](#).

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 Guida](#) per l'utente IAM.

## Creazione del ruolo collegato ai servizi

### **AWSServiceRoleForSystemsManagerJustInTimeAccess** per Systems Manager

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando abiliti l'accesso just-in-time al nodo in Console di gestione AWS, Systems Manager crea automaticamente il ruolo collegato al servizio.

#### Important

Questo ruolo collegato al servizio può apparire nell'account, se è stata completata un'operazione in un altro servizio che utilizza le funzionalità supportate da questo ruolo. Se inoltre usavi il servizio Systems Manager prima del 19 novembre 2024, data da cui è disponibile il supporto dei ruoli collegati ai servizi, Systems Manager ha creato il ruolo **AWSServiceRoleForSystemsManagerJustInTimeAccess** nel tuo account. Per ulteriori informazioni, consulta [Un nuovo ruolo è apparso nel mio account IAM](#).

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando abiliti l'accesso just-in-time al nodo in Console di gestione AWS, Systems Manager crea nuovamente il ruolo collegato al servizio.

È possibile utilizzare la console IAM anche per creare un ruolo collegato ai servizi con il ruolo di servizio AWS che consente a Systems Manager di abilitare l'accesso al nodo just-in-time. caso d'uso. Nella AWS CLI o nell' AWS API, crea un ruolo collegato al servizio con il nome del servizio. `ssm.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

### **AWSServiceRoleForSystemsManagerJustInTimeAccess** per Systems Manager

Systems Manager non consente di modificare il ruolo collegato ai servizi

**AWSServiceRoleForSystemsManagerJustInTimeAccess**. Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

## Eliminazione di un ruolo collegato ai servizi

### **AWSServiceRoleForSystemsManagerJustInTimeAccess** per Systems Manager

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 hai un'entità non utilizzata che non viene monitorata o gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

#### Note

Se il servizio Systems 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 eliminare manualmente il ruolo collegato ai servizi

**AWSServiceRoleForSystemsManagerJustInTimeAccess** utilizzando IAM

Utilizza la console IAM AWS CLI, l'AWS API per eliminare il ruolo collegato al **AWSServiceRoleForSystemsManagerJustInTimeAccess** servizio. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

## Regioni supportate per il ruolo collegato ai servizi Systems Manager

**AWSServiceRoleForSystemsManagerJustInTimeAccess**

Regione AWS nome	Identità della Regione	Supporto in Systems 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
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
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
Europa (Parigi)	eu-west-3	Sì
Europa (Stoccolma)	eu-north-1	Sì
Sud America (San Paolo)	sa-east-1	Sì

Regione AWS nome	Identità della Regione	Supporto in Systems Manager
AWS GovCloud (US)	us-gov-west-1	No

## Utilizzo dei ruoli per inviare notifiche di richiesta di accesso ai nodi just-in-time

Systems Manager utilizza il ruolo collegato al servizio denominato.

**AWSServiceRoleForSystemsManagerNotifications** AWS Systems Manager utilizza questo ruolo del servizio IAM per inviare notifiche agli approvatori delle richieste di accesso.

### Service-linked autorizzazioni di ruolo per le notifiche di accesso ai nodi Systems Manager just-in-time

Ai fini dell'assunzione del ruolo, il ruolo collegato al servizio

**AWSServiceRoleForSystemsManagerNotifications** considera attendibili i seguenti servizi:

- `ssm.amazonaws.com`

La policy delle autorizzazioni del ruolo consente ad Systems Manager di eseguire le seguenti operazioni sulle risorse specificate:

- `identitystore:ListGroupMembershipsForMember`
- `identitystore:ListGroupMemberships`
- `identitystore:DescribeUser`
- `sso:ListInstances`
- `sso:DescribeRegisteredRegions`
- `sso:ListDirectoryAssociations`
- `sso-directory:DescribeUser`
- `sso-directory:ListMembersInGroup`
- `iam:GetRole`

La policy gestita utilizzata per fornire le autorizzazioni per il ruolo `AWSServiceRoleForSystemsManagerNotifications` è `AWSSystemsManagerNotificationsServicePolicy`. Per informazioni dettagliate sulle autorizzazioni necessarie, consulta [AWS politica gestita: `AWSSystemsManagerNotificationsServicePolicy`](#).

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 Guida](#) per l'utente IAM.

## Creazione del ruolo collegato ai servizi

### **AWSServiceRoleForSystemsManagerNotifications** per Systems Manager

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando abiliti l'accesso just-in-time al nodo in Console di gestione AWS, Systems Manager crea automaticamente il ruolo collegato al servizio.

#### Important

Questo ruolo collegato al servizio può apparire nell'account, se è stata completata un'operazione in un altro servizio che utilizza le funzionalità supportate da questo ruolo. Se inoltre usavi il servizio Systems Manager prima del 19 novembre 2024, data da cui è disponibile il supporto dei ruoli collegati ai servizi, Systems Manager ha creato il ruolo `AWSServiceRoleForSystemsManagerNotifications` nel tuo account. Per ulteriori informazioni, consulta [Un nuovo ruolo è apparso nel mio account IAM](#).

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando abiliti l'accesso just-in-time al nodo in Console di gestione AWS, Systems Manager crea nuovamente il ruolo collegato al servizio per te.

È possibile utilizzare la console IAM anche per creare un ruolo collegato ai servizi con il ruolo di servizio AWS che consente a Systems Manager di inviare notifiche agli approvatori delle richieste di accesso. caso d'uso. Nella AWS CLI o nell' AWS API, crea un ruolo collegato al servizio con il nome del servizio. `ssm.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

### **AWSServiceRoleForSystemsManagerNotifications** per Systems Manager

Systems Manager non consente di modificare il ruolo collegato ai servizi

**AWSServiceRoleForSystemsManagerNotifications**. Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

## Eliminazione di un ruolo collegato ai servizi

### **AWSServiceRoleForSystemsManagerNotifications** per Systems Manager

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 hai un'entità non utilizzata che non viene monitorata o gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

#### Note

Se il servizio Systems 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 eliminare manualmente il ruolo collegato ai servizi

### **AWSServiceRoleForSystemsManagerNotifications** utilizzando IAM

Utilizza la console IAM AWS CLI, l'AWS API per eliminare il ruolo collegato al **AWSServiceRoleForSystemsManagerNotifications** servizio. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

## Regioni supportate per il ruolo collegato ai servizi Systems Manager

**AWSServiceRoleForSystemsManagerNotifications**

Regione AWS nome	Identità della Regione	Supporto in Systems 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
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
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
Europa (Parigi)	eu-west-3	Sì
Europa (Stoccolma)	eu-north-1	Sì
Sud America (San Paolo)	sa-east-1	Sì

Regione AWS nome	Identità della Regione	Supporto in Systems Manager
AWS GovCloud (US)	us-gov-west-1	No

## Registrazione e monitoraggio AWS Systems Manager

Il monitoraggio è una parte importante del mantenimento dell'affidabilità, della disponibilità AWS Systems Manager e delle prestazioni delle AWS soluzioni. È necessario raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire un maggiore debug di un eventuale errore multipunto. AWS fornisce diversi strumenti per monitorare le vostre Systems Manager e altre risorse e rispondere a potenziali incidenti.

### AWS CloudTrail registri

CloudTrail fornisce un registro delle azioni intraprese da un utente, da un ruolo o da un Servizio AWS in Systems Manager. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta a cui è stata effettuata Systems Manager, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi. Per ulteriori informazioni, consulta [Registrazione dei log AWS Systems Manager Chiamate API con AWS CloudTrail](#).

### CloudWatch Allarmi Amazon

Utilizzando gli CloudWatch allarmi Amazon, osservi una singola metrica per un periodo di tempo specificato per le tue istanze Amazon Elastic Compute Cloud (Amazon EC2) e altre risorse. Se la metrica supera una determinata soglia, viene inviata una notifica a un argomento o a una policy di Amazon Simple Notification Service (Amazon SNS). AWS Auto Scaling CloudWatch gli allarmi non richiamano azioni perché si trovano in uno stato particolare. È necessario invece cambiare lo stato e mantenerlo per un numero di periodi specificato. Per ulteriori informazioni, consulta [Usare gli CloudWatch allarmi di Amazon](#) nella Amazon CloudWatch User Guide.

### Dashboard Amazon CloudWatch

CloudWatch Le dashboard sono home page personalizzabili nella CloudWatch console che puoi utilizzare per monitorare le tue risorse in un'unica visualizzazione, anche quelle distribuite su più fronti. Regioni AWS Puoi utilizzare CloudWatch le dashboard per creare visualizzazioni personalizzate delle metriche e degli allarmi per le tue risorse. AWS Per ulteriori informazioni, consulta [Utilizzo delle CloudWatch dashboard Amazon ospitate da Systems Manager](#).



## Amazon EventBridge

Utilizzando Amazon EventBridge, puoi configurare regole per avvisarti dei cambiamenti nelle Systems Manager risorse e indirizzarti EventBridge a intraprendere azioni in base al contenuto di tali eventi. EventBridge fornisce supporto per diversi eventi emessi da vari Systems Manager strumenti. Per ulteriori informazioni, consulta [Monitoraggio degli eventi di Systems Manager con Amazon EventBridge](#).

## Amazon CloudWatch Logs e SSM Agent log

SSM Agent scrive informazioni su esecuzioni, operazioni pianificate, errori e stati di integrità in file di log per ogni nodo. È possibile visualizzare i file di log collegandosi manualmente a un nodo. Consigliamo di inviare automaticamente i dati di log degli agenti a un gruppo di CloudWatch log in Logs per l'analisi. Per ulteriori informazioni, consultare [Invio dei log dei nodi a CloudWatch registri unificati \(CloudWatch agente\)](#) e [Visualizzazione Agente SSM log](#).

## Conformità AWS Systems Manager

Puoi utilizzare Compliance per scansionare la tua flotta di nodi gestiti per verificare la conformità delle patch e le incoerenze di configurazione. Puoi raccogliere e aggregare dati da più Account AWS e Regioni AWS quindi approfondire le risorse specifiche che non sono conformi. Per impostazione predefinita, Compliance mostra i dati di conformità correnti relativi all'applicazione di patch e alle associazioni in State Manager uno strumento. Patch Manager AWS Systems Manager Per ulteriori informazioni, consulta [AWS Systems Manager Conformità](#).

## AWS Systems Manager Explorer

Explorer è una dashboard operativa personalizzabile che riporta informazioni sulle tue AWS risorse. Explorer mostra una vista aggregata dei dati operativi (OpsData) per te Account AWS e per tutti Regioni AWS. In Explorer, OpsData include metadati sulle istanze EC2, dettagli sulla conformità delle patch e elementi di lavoro operativi (). OpsItems Explorer fornisce un contesto su come OpsItems sono distribuite tra le unità aziendali o le applicazioni, come si evolvono nel tempo e come variano in base alla categoria. È possibile raggruppare e filtrare le informazioni Explorer per concentrarti sugli elementi rilevanti e per cui è necessario prendere misure. Per ulteriori informazioni, consulta [AWS Systems Manager Explorer](#).

## AWS Systems Manager OpsCenter

OpsCenter fornisce una posizione centrale in cui gli ingegneri operativi e i professionisti IT possono visualizzare, esaminare e risolvere gli elementi di lavoro operativi (OpsItems) relativi alle AWS risorse. OpsCenter aggrega e standardizza OpsItems tutti i servizi fornendo al contempo dati di indagine contestuali su ciascuna risorsa OpsItem correlata e OpsItems

correlata. OpsCenter fornisce anche runbook in Automation, che puoi utilizzare per risolvere rapidamente i problemi. OpsCenter è integrato con Amazon EventBridge. Ciò significa che puoi creare EventBridge regole che vengono create automaticamente OpsItems per chiunque Servizio AWS pubblici eventi su EventBridge. Per ulteriori informazioni, consulta [AWS Systems Manager OpsCenter](#).

## Amazon Simple Notification Service

Puoi configurare Amazon Simple Notification Service (Amazon SNS) per inviare notifiche sullo stato dei comandi inviati utilizzando Run Command o Maintenance Windows, uno strumento di AWS Systems Manager. Amazon SNS coordina e gestisce l'invio e la consegna delle notifiche ai clienti o agli endpoint che sono iscritti agli argomenti di Amazon SNS. Ogni volta che un comando cambia di stato o passa a uno stato specifico, ad esempio Failed o Timed Out, è possibile decidere di ricevere una notifica. Quando si invia un comando a più nodi, è possibile ricevere una notifica per ciascuna copia del comando inviato a un determinato nodo. Per ulteriori informazioni, consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

## AWS Trusted Advisor e Dashboard AWS Health

Trusted Advisor si basa sulle migliori pratiche apprese servendo centinaia di migliaia di AWS clienti. Trusted Advisor esamina l'AWS ambiente e quindi formula raccomandazioni laddove esistono opportunità per risparmiare denaro, migliorare la disponibilità e le prestazioni del sistema o contribuire a colmare le lacune di sicurezza. Tutti i AWS clienti hanno accesso a cinque Trusted Advisor controlli. I clienti con un piano Supporto AWS Business o Enterprise possono visualizzare tutti gli Trusted Advisor assegni. Per ulteriori informazioni, consulta la sezione [AWS Trusted Advisor](#) nella Guida per l'utente di Supporto AWS e la [Guida per l'utente di AWS Health](#).

Ulteriori informazioni

- [Registrazione e monitoraggio AWS Systems Manager](#)

## Convalida della conformità per AWS Systems Manager

Questo argomento affronta la conformità di AWS Systems Manager ai programmi di garanzia di terze parti. Per informazioni sulla visualizzazione dei dati di conformità per le istanze gestite, consulta [AWS Systems Manager Conformità](#).

Third-party gli auditor valutano la sicurezza e la conformità di Systems Manager come parte di più programmi di AWS conformità. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per un elenco dei programmi di conformità specifici, vedere [AWS Servizi Servizi AWS nell'ambito del programma di conformità in Ambito di applicazione del programma di conformità Servizi AWS](#) . Per informazioni generali, vedere Programmi di [AWS conformità Programmi](#) di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Scaricamento dei report in AWS Artifact](#) .

La vostra responsabilità di conformità durante l'utilizzo Systems Manager è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- [Le guide rapide per la sicurezza e la conformità](#): queste guide all'implementazione illustrano considerazioni architettoniche e forniscono i passaggi per l'implementazione di ambienti di base incentrati sulla sicurezza e sulla conformità su AWS.
- [Whitepaper sull'architettura per la sicurezza e la conformità HIPAA](#): questo white paper descrive come le aziende possono utilizzare per creare applicazioni. AWS HIPAA-compliant
- [AWS Risorse per la conformità Risorse](#) per : questa raccolta di cartelle di lavoro e guide potrebbe riguardare il settore e la località in cui operi.
- [Valutazione delle risorse con le regole](#) nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- [AWS Security Hub CSPM](#)— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza dell'utente, AWS che consente di verificare la conformità agli standard e alle best practice del settore della sicurezza.

## Resilienza nell' AWS Systems Manager

L'infrastruttura AWS globale è costruita attorno a zone Regioni AWS di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità è possibile progettare e gestire applicazioni e database che eseguono automaticamente il failover 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 tradizionali.

[Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS](#)

# Sicurezza dell'infrastruttura nell' AWS Systems Manager

In quanto servizio gestito, AWS Systems Manager è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di 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.

Utilizzate chiamate API AWS pubblicate per accedere Systems Manager 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.

## Analisi della configurazione e delle vulnerabilità in AWS Systems Manager

AWS gestisce le attività di sicurezza di base come la configurazione del firewall e il disaster recovery. Queste procedure sono state riviste e certificate dalle terze parti appropriate. Per ulteriori dettagli, consulta le seguenti risorse :

- [Convalida della conformità per AWS Systems Manager](#)
- [Modello di responsabilità condivisa](#)
- [Best practice per sicurezza, identità e conformità.](#)

## Le migliori pratiche di sicurezza per Systems Manager

AWS Systems Manager offre diverse funzionalità di sicurezza da considerare durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, sono da considerare come considerazioni utili anziché prescrizioni.

### Argomenti

- [Systems Manager best practice di sicurezza preventiva](#)

- [Agente SSM best practice di installazione](#)
- [Systems Manager best practice di monitoraggio e verifica](#)

## Systems Manager best practice di sicurezza preventiva

Le seguenti best practice per Systems Manager consentono di evitare incidenti di sicurezza.

### Applicazione dell'accesso con privilegio minimo

Attribuite le autorizzazioni, si può decidere chi ottiene tali autorizzazioni e verso quali Systems Manager risorse. È possibile abilitare operazioni specifiche che desideri consentire su tali risorse. Pertanto è necessario concedere solo le autorizzazioni necessarie per eseguire un'attività. L'implementazione dell'accesso con privilegi minimi è fondamentale per ridurre i rischi di sicurezza e l'impatto risultante da errori o intenzioni dannose.

Gli strumenti seguenti sono disponibili per implementare l'accesso con privilegi minimi:

- [Policy IAM](#) e [Limiti delle autorizzazioni per le entità IAM](#)
- [Policy di controllo dei servizi](#)

Utilizza le impostazioni consigliate per SSM Agent quando è configurato per utilizzare un proxy

Se si configura SSM Agent l'uso di un proxy, utilizzare la `no_proxy` variabile con l'indirizzo IP del servizio di metadati delle istanze di Systems Manager per assicurarsi che le chiamate a Systems Manager non assumano l'identità del servizio proxy.

Per ulteriori informazioni, consulta [Configurazione Agente SSM usare un proxy su nodi Linux](#) e [Configurazione di SSM Agent per utilizzare un proxy per le istanze Windows Server](#).

Utilizza SecureString i parametri per crittografare e proteggere i dati segreti

InParameter Store, un SecureString parametro è qualsiasi dato sensibile che deve essere archiviato e referenziato in modo sicuro. Se disponi di dati a cui non desideri che gli utenti alterino o facciano riferimento in testo normale, come password o chiavi di licenza, crea tali parametri utilizzando il SecureString tipo di dati. Parameter Store utilizza un AWS KMS key in AWS Key Management Service (AWS KMS) per crittografare il valore del parametro. AWS KMS utilizza una chiave gestita dal cliente o una per crittografare Chiave gestita da AWS il valore del parametro. Per la massima sicurezza, si consiglia di utilizzare il proprio CMK. Se utilizzi il Chiave gestita da AWS, qualsiasi utente autorizzato a eseguire le [GetParameters](#) azioni [GetParameter](#) and nel tuo account può visualizzare o recuperare il contenuto di tutti i SecureString parametri. Se

si utilizzano CMK gestiti dal cliente per crittografare i valori SecureString protetti, è possibile utilizzare le policy IAM e le policy chiave per gestire le autorizzazioni per la crittografia e la decrittografia dei parametri.

È molto difficile stabilire le policy di controllo degli accessi per queste operazioni utilizzando una Chiave gestita da AWS. Ad esempio, se utilizzi an per Chiave gestita da AWS crittografare SecureString i parametri e non vuoi che gli utenti lavorino con SecureString i parametri, le politiche IAM dell'utente devono negare esplicitamente l'accesso alla chiave predefinita.

Per ulteriori informazioni, consulta [Gestire l'accesso a Parameter Store parametri che utilizzano le politiche IAM](#) e [Come AWS Systems Manager Parameter Store Usa Usa AWS KMS nella AWS Key Management Service Guida per gli sviluppatori](#).

### Definire allowedValues e allowedPattern per parametri del documento

È possibile convalidare l'input dell'utente per i parametri del documento Systems Manager (documenti SSM) definendo allowedValues e allowedPattern. Per allowedValues, definire una matrice di valori consentiti per il parametro. Se un utente inserisce un valore non consentito, l'esecuzione non viene avviata. Per allowedPattern, definire un'espressione regolare che convalida se l'input dell'utente corrisponde al modello definito per il parametro. Se l'input dell'utente non corrisponde al modello consentito, l'esecuzione non viene avviata.

Per ulteriori informazioni su allowedValues e allowedPattern, consulta [Elementi di dati e parametri](#).

### Blocca la condivisione pubblica per i documenti

A meno che il caso d'uso non richieda l'autorizzazione della condivisione pubblica, si consiglia di attivare l'impostazione Blocca condivisione pubblica per i documenti SSM nella sezione Preferenze della console Documenti di Systems Manager.

### Utilizzare un Amazon Virtual Private Cloud (Amazon VPC) e gli endpoint VPC

Puoi usare Amazon VPC per lanciare AWS risorse in una rete virtuale che hai definito. Questa rete virtuale è simile a una comune rete da gestire all'interno del proprio data center, ma con i vantaggi dell'infrastruttura scalabile di AWS.

Implementando un endpoint VPC, puoi connettere privatamente il tuo VPC a servizi endpoint VPC supportati Servizi AWS e alimentati da, AWS PrivateLink senza richiedere un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze nel VPC non richiedono indirizzi IP pubblici per comunicare con risorse nel servizio. Il traffico tra il VPC e gli altri servizi non lascia la rete Amazon.

Per ulteriori informazioni sulla sicurezza di Amazon VPC, consulta [Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager](#) e [Riservatezza del traffico Internet in Amazon VPC](#) nella Guida per l'utente di Amazon VPC.

Limitare gli utenti Session Manager alle sessioni che utilizzano comandi interattivi e documenti di sessione SSM specifici

Session Manager fornisce [diversi metodi per avviare sessioni sui nodi gestiti](#). Per le connessioni più sicure, è possibile richiedere agli utenti di connettersi utilizzando il metodo dei comandi interattivi per limitare l'interazione dell'utente a uno specifico comando o a una sequenza di comandi. Ciò consente di gestire le operazioni interattive che un utente può intraprendere. Per ulteriori informazioni, consulta [Avvio di una sessione \(comandi interattivi e non interattivi\)](#).

Per una maggiore sicurezza, è possibile limitare l'accesso Session Manager a istanze Amazon EC2 specifiche e a documenti di sessione Session Manager specifici. L'accesso Session Manager viene concesso o revocato in questo modo utilizzando le policy AWS Identity and Access Management (IAM). Per ulteriori informazioni, consulta [Fase 3: Controlla l'accesso della sessione ai nodi gestiti](#).

Fornire autorizzazioni di nodo temporanee per flussi di lavoro di automazione

Durante un flusso di lavoro in Automazione, uno strumento di AWS Systems Manager, i nodi potrebbero aver bisogno delle autorizzazioni necessarie solo per tale esecuzione, ma non per altre operazioni Systems Manager. Ad esempio, un flusso di lavoro di automazione potrebbe richiedere che un nodo chiami una particolare operazione API o acceda a una AWS risorsa specificamente durante il flusso di lavoro. Se queste chiamate o risorse sono quelle a cui si desidera limitare l'accesso, è possibile fornire autorizzazioni temporanee e supplementari per i nodi all'interno del runbook di Automazione stesso invece di aggiungere le autorizzazioni al profilo dell'istanza IAM. Al termine dell'esecuzione di automazione, le autorizzazioni temporanee vengono rimosse. Per ulteriori informazioni, consulta [Fornire autorizzazioni di istanza temporanee con le automazioni AWS Systems Manager](#) nel Blog di Gestione e Controllo AWS .

AWS Mantieni i tuoi Systems Manager strumenti aggiornati

AWS rilascia regolarmente versioni aggiornate di strumenti e plug-in che puoi utilizzare nelle tue AWS Systems Manager operazioni. Mantenere aggiornate queste risorse garantisce che gli utenti e i nodi dell'account abbiano accesso alle funzionalità e alle funzioni di sicurezza più recenti di questi strumenti.

- SSM Agent – AWS Systems Manager Agent (SSM Agent) è un software Amazon che può essere installato e configurato su un'istanza Amazon Elastic Compute Cloud (Amazon EC2), un



server on-premises o una macchina virtuale (VM). SSM Agent consente a Systems Manager di aggiornare, gestire e configurare tali risorse. Si consiglia di verificare la presenza di nuove versioni o di automatizzare gli aggiornamenti dell'agente almeno ogni due settimane. Per informazioni, consulta [Automatizzazione degli aggiornamenti a Agente SSM](#). Ti consigliamo inoltre di verificare la firma di SSM Agent nell'ambito del processo di aggiornamento. Per informazioni, consulta [Verifica della firma di Agente SSM](#).

- **AWS CLI** — The AWS Command Line Interface (AWS CLI) è uno strumento open source che consente di interagire Servizi AWS utilizzando i comandi nella shell della riga di comando. Per aggiornare il AWS CLI, si esegue lo stesso comando utilizzato per installare. AWS CLI Si consiglia di creare un'attività pianificata sul computer locale per eseguire il comando appropriato al sistema operativo almeno una volta ogni due settimane. Per informazioni sui comandi di installazione, vedere [Installazione della AWS CLI versione 2](#) nella Guida per l'AWS Command Line Interface utente.
- **AWS Tools for Windows PowerShell** — Gli strumenti per Windows PowerShell sono un insieme di PowerShell moduli basati sulle funzionalità esposte dall' AWS SDK for .NET. Ti AWS Tools for Windows PowerShell consentono di creare script per le operazioni sulle tue AWS risorse dalla PowerShell riga di comando. Periodicamente, man mano che PowerShell vengono rilasciate versioni aggiornate degli Strumenti per Windows, è necessario aggiornare la versione in esecuzione localmente. Per informazioni, consulta [Aggiornamento di Windows](#) o [Aggiornamento di AWS Tools for Windows PowerShell](#) su [Linux o macOS](#) nella Guida per l'utente di IAM Policy Simulator.
- **Plug-in di Session Manager** - Se gli utenti dell'organizzazione con autorizzazioni a utilizzare Session Manager desiderano connettersi a un nodo utilizzando l' AWS CLI, devono prima installare il plug-in Session Manager sui computer locali. Per aggiornare il plugin, si esegue lo stesso comando utilizzato per installare il plugin. Si consiglia di creare un'attività pianificata sul computer locale per eseguire il comando appropriato al sistema operativo almeno una volta ogni due settimane. Per informazioni, consulta [Installa il Session Manager plugin per AWS CLI](#).
- **CloudWatch agente** — È possibile configurare e utilizzare l' CloudWatch agente per raccogliere metriche e log dalle istanze EC2, dalle istanze locali e dalle macchine virtuali (VM). Questi log possono essere inviati ad Amazon Logs per il monitoraggio e l'analisi CloudWatch . Si consiglia di verificare la presenza di nuove versioni o di automatizzare gli aggiornamenti dell'agente almeno ogni due settimane. Per gli aggiornamenti più semplici, utilizza la configurazione rapida di AWS Systems Manager. Per informazioni, consulta [AWS Systems Manager Configurazione rapida](#).



## Agente SSM best practice di installazione

Durante l'installazione dell'SSM Agent, utilizza il metodo di installazione appropriato per il tipo di macchina in uso. In particolare, utilizza lo strumento `ssm-setup-cli` per tutte le installazioni non EC2 in un ambiente [ibrido e multicloud](#). Questo strumento fornisce protezioni di sicurezza aggiuntive per macchine non EC2.

Per installare l'agente sui server on-premises e sulle macchine virtuali, utilizzare lo strumento `ssm-setup-cli` come descritto nei seguenti argomenti:

- [the section called “Installa Agente SSM su nodi Linux ibridi”](#)
- [the section called “Installa Agente SSM su ibrido Windows Server nodi”](#)

Per installare l'agente sulle istanze EC2, utilizza la procedura di installazione appropriata per il tipo di sistema operativo:

- [the section called “Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux”](#)
- [the section called “Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per macOS”](#)
- [the section called “Installazione e disinstallazione manuali Agente SSM su istanze EC2 per Windows Server”](#)

## Systems Manager best practice di monitoraggio e verifica

Le best practice seguenti per Systems Manager consentono di rilevare potenziali debolezze e incidenti di sicurezza.

Identificare e controllare tutte le risorse di Systems Manager

L'identificazione degli asset IT è un aspetto essenziale di governance e sicurezza. È richiesta identificare tutte le risorse Systems Manager per valutare il loro assetto di sicurezza e intervenire su aree di debolezza potenziali.

Utilizza Tag Editor per identificare risorse sensibili alla sicurezza e risorse sensibili al controllo, quindi utilizza questi tag quando occorre cercare le risorse. Per ulteriori informazioni, consulta [Ricerca di risorse per i tag](#) nella Guida per l'utente AWS Resource Groups .

Crea gruppi di risorse per le risorse Systems Manager. Per ulteriori informazioni, consulta [Che cos'è Resource Groups?](#).

Implementa il monitoraggio utilizzando gli strumenti di CloudWatch monitoraggio di Amazon

Il monitoraggio è importante per garantire l'affidabilità, la disponibilità e le prestazioni di Systems Manager e delle soluzioni AWS . Amazon CloudWatch fornisce diversi strumenti e servizi per aiutare te Systems Manager e gli altri Servizi AWS. Per ulteriori informazioni, consulta [Invio dei log dei nodi a CloudWatch registri unificati \(CloudWatch agente\)](#) e [Monitoraggio degli eventi di Systems Manager con Amazon EventBridge](#).

Usa CloudTrail

AWS CloudTrail fornisce un registro delle azioni intraprese da un utente, da un ruolo o da un Servizio AWS utente Systems Manager. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta a cui è stata effettuata Systems Manager, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi. Per ulteriori informazioni, consulta [Registrazione dei log AWS Systems Manager Chiamate API con AWS CloudTrail](#).

Attiva AWS Config

AWS Config consente di valutare, controllare e valutare le configurazioni delle AWS risorse. AWS Config monitora le configurazioni delle risorse, consentendo di valutare le configurazioni registrate rispetto alle configurazioni sicure richieste. Utilizzando AWS Config, è possibile esaminare le modifiche nelle configurazioni e nelle relazioni tra le AWS risorse, esaminare le cronologie dettagliate delle configurazioni delle risorse e determinare la conformità generale rispetto alle configurazioni specificate nelle linee guida interne. Questo semplifica il controllo della conformità, l'analisi della sicurezza, la gestione delle modifiche e la risoluzione dei problemi operativi. Per ulteriori informazioni, consulta la sezione [Configurazione di AWS Config con la console](#) nella Guida per gli sviluppatori di AWS Config . Quando specificate i tipi di risorse da registrare, assicuratevi di includere le risorse. Systems Manager

Monitora gli avvisi AWS di sicurezza

Dovresti controllare regolarmente gli avvisi di sicurezza pubblicati Trusted Advisor per il tuo Account AWS. È possibile eseguire questa operazione in modo programmatico utilizzando [describe-trusted-advisor-checks](#).

Inoltre, monitora attivamente l'indirizzo email principale registrato da ciascuno dei tuoi Account AWS. AWS ti contatterà, utilizzando questo indirizzo email, in merito a problemi di sicurezza emergenti che potrebbero interessarti.

AWS i problemi operativi di ampio impatto sono pubblicati nel [AWS Service Health Dashboard](#). Problemi operativi sono anche pubblicati su singoli account tramite il Personal Health Dashboard. Per ulteriori informazioni, consulta la [Documentazione AWS Health](#).

#### Ulteriori informazioni

- [Best practice per sicurezza, identità e conformità](#).
- [Guida introduttiva: segui le best practice di sicurezza durante la configurazione AWS delle risorse](#) (AWS Security Blog)
- [Best practice per la sicurezza in IAM](#)
- [Le migliori pratiche di sicurezza in AWS CloudTrail](#)
- [Best practice di sicurezza per Amazon S3](#)
- [Le migliori pratiche di sicurezza per AWS Key Management Service](#)

# Esempi di codice per Systems Manager utilizzando AWS SDK

I seguenti esempi di codice mostrano come utilizzare Systems Manager con un kit di sviluppo AWS software (SDK).

Nozioni di base: esempi di codice che mostrano come eseguire le operazioni essenziali all'interno di un servizio.

Le azioni sono estratti di codice da programmi più grandi e devono essere eseguite nel contesto. Sebbene le azioni mostrino come richiamare le singole funzioni del servizio, è possibile visualizzarle contestualizzate negli scenari correlati.

Scenari: esempi di codice che mostrano come eseguire un'attività specifica chiamando più funzioni all'interno dello stesso servizio o combinate con altri Servizi AWS.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Esempi di codice

- [Esempi di base per l'utilizzo di Systems Manager AWS SDK](#)
  - [Salve Systems Manager](#)
  - [Impara le basi di Systems Manager con un AWS SDK](#)
  - [Azioni per Systems Manager utilizzando AWS SDK](#)
    - [Utilizzo di AddTagsToResource con una CLI](#)
    - [Utilizzo di CancelCommand con una CLI](#)
    - [Utilizzo di CreateActivation con una CLI](#)
    - [Utilizzo di CreateAssociation con una CLI](#)
    - [Utilizzo di CreateAssociationBatch con una CLI](#)
    - [Usare CreateDocument con un AWS SDK o CLI](#)
    - [Usare CreateMaintenanceWindow con un AWS SDK o CLI](#)
    - [Usare CreateOpsItem con un AWS SDK o CLI](#)
    - [Utilizzo di CreatePatchBaseline con una CLI](#)
    - [Utilizzo di DeleteActivation con una CLI](#)

- [Utilizzo di DeleteAssociation con una CLI](#)
- [Usare DeleteDocument con un AWS SDK o CLI](#)
- [Usare DeleteMaintenanceWindow con un AWS SDK o CLI](#)
- [Usare DeleteOpsItem con un AWS SDK](#)
- [Utilizzo di DeleteParameter con una CLI](#)
- [Utilizzo di DeletePatchBaseline con una CLI](#)
- [Utilizzo di DeregisterManagedInstance con una CLI](#)
- [Utilizzo di DeregisterPatchBaselineForPatchGroup con una CLI](#)
- [Utilizzo di DeregisterTargetFromMaintenanceWindow con una CLI](#)
- [Utilizzo di DeregisterTaskFromMaintenanceWindow con una CLI](#)
- [Utilizzo di DescribeActivations con una CLI](#)
- [Utilizzo di DescribeAssociation con una CLI](#)
- [Utilizzo di DescribeAssociationExecutionTargets con una CLI](#)
- [Utilizzo di DescribeAssociationExecutions con una CLI](#)
- [Utilizzo di DescribeAutomationExecutions con una CLI](#)
- [Utilizzo di DescribeAutomationStepExecutions con una CLI](#)
- [Utilizzo di DescribeAvailablePatches con una CLI](#)
- [Usare DescribeDocument con un AWS SDK o CLI](#)
- [Utilizzo di DescribeDocumentPermission con una CLI](#)
- [Utilizzo di DescribeEffectiveInstanceAssociations con una CLI](#)
- [Utilizzo di DescribeEffectivePatchesForPatchBaseline con una CLI](#)
- [Utilizzo di DescribeInstanceAssociationsStatus con una CLI](#)
- [Utilizzo di DescribeInstanceInformation con una CLI](#)
- [Utilizzo di DescribeInstancePatchStates con una CLI](#)
- [Utilizzo di DescribeInstancePatchStatesForPatchGroup con una CLI](#)
- [Utilizzo di DescribeInstancePatches con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindowExecutionTaskInvocations con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindowExecutionTasks con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindowExecutions con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindowTargets con una CLI](#)

- [Utilizzo di DescribeMaintenanceWindowTasks con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindows con una CLI](#)
- [Usare DescribeOpsItems con un AWS SDK o CLI](#)
- [Usare DescribeParameters con un AWS SDK o CLI](#)
- [Utilizzo di DescribePatchBaselines con una CLI](#)
- [Utilizzo di DescribePatchGroupState con una CLI](#)
- [Utilizzo di DescribePatchGroups con una CLI](#)
- [Utilizzo di GetAutomationExecution con una CLI](#)
- [Utilizzo di GetCommandInvocation con una CLI](#)
- [Utilizzo di GetConnectionStatus con una CLI](#)
- [Utilizzo di GetDefaultPatchBaseline con una CLI](#)
- [Utilizzo di GetDeployablePatchSnapshotForInstance con una CLI](#)
- [Utilizzo di GetDocument con una CLI](#)
- [Utilizzo di GetInventory con una CLI](#)
- [Utilizzo di GetInventorySchema con una CLI](#)
- [Utilizzo di GetMaintenanceWindow con una CLI](#)
- [Utilizzo di GetMaintenanceWindowExecution con una CLI](#)
- [Utilizzo di GetMaintenanceWindowExecutionTask con una CLI](#)
- [Usare GetParameter con un AWS SDK o CLI](#)
- [Utilizzo di GetParameterHistory con una CLI](#)
- [Utilizzo di GetParameters con una CLI](#)
- [Utilizzo di GetPatchBaseline con una CLI](#)
- [Utilizzo di GetPatchBaselineForPatchGroup con una CLI](#)
- [Utilizzo di ListAssociationVersions con una CLI](#)
- [Utilizzo di ListAssociations con una CLI](#)
- [Usare ListCommandInvocations con un AWS SDK o CLI](#)
- [Utilizzo di ListCommands con una CLI](#)
- [Utilizzo di ListComplianceItems con una CLI](#)
- [Utilizzo di ListComplianceSummaries con una CLI](#)
- [Utilizzo di ListDocumentVersions con una CLI](#)

- [Utilizzo di ListDocuments con una CLI](#)
- [Utilizzo di ListInventoryEntries con una CLI](#)
- [Utilizzo di ListResourceComplianceSummaries con una CLI](#)
- [Utilizzo di ListTagsForResource con una CLI](#)
- [Utilizzo di ModifyDocumentPermission con una CLI](#)
- [Utilizzo di PutComplianceItems con una CLI](#)
- [Utilizzo di PutInventory con una CLI](#)
- [Usare PutParameter con un AWS SDK o CLI](#)
- [Utilizzo di RegisterDefaultPatchBaseline con una CLI](#)
- [Utilizzo di RegisterPatchBaselineForPatchGroup con una CLI](#)
- [Utilizzo di RegisterTargetWithMaintenanceWindow con una CLI](#)
- [Utilizzo di RegisterTaskWithMaintenanceWindow con una CLI](#)
- [Utilizzo di RemoveTagsFromResource con una CLI](#)
- [Usare SendCommand con un AWS SDK o CLI](#)
- [Utilizzo di StartAutomationExecution con una CLI](#)
- [Utilizzo di StartSession con una CLI](#)
- [Utilizzo di StopAutomationExecution con una CLI](#)
- [Utilizzo di UpdateAssociation con una CLI](#)
- [Utilizzo di UpdateAssociationStatus con una CLI](#)
- [Utilizzo di UpdateDocument con una CLI](#)
- [Utilizzo di UpdateDocumentDefaultVersion con una CLI](#)
- [Usare UpdateMaintenanceWindow con un AWS SDK o CLI](#)
- [Utilizzo di UpdateManagedInstanceRole con una CLI](#)
- [Usare UpdateOpsItem con un AWS SDK o CLI](#)
- [Utilizzo di UpdatePatchBaseline con una CLI](#)
- [Scenari per l'utilizzo di Systems Manager AWS SDK](#)
  - [Creazione di un servizio contenitore per istanze di macchine virtuali](#)
  - [Guida introduttiva alle macchine virtuali](#)
  - [Configurazione della gestione dei sistemi](#)

# Esempi di base per l'utilizzo di Systems Manager AWS SDK

I seguenti esempi di codice mostrano come utilizzare le nozioni di base di AWS Systems Manager con gli SDK. AWS

## Esempi

- [Salve Systems Manager](#)
- [Impara le basi di Systems Manager con un AWS SDK](#)
- [Azioni per Systems Manager utilizzando AWS SDK](#)
  - [Utilizzo di AddTagsToResource con una CLI](#)
  - [Utilizzo di CancelCommand con una CLI](#)
  - [Utilizzo di CreateActivation con una CLI](#)
  - [Utilizzo di CreateAssociation con una CLI](#)
  - [Utilizzo di CreateAssociationBatch con una CLI](#)
  - [Usare CreateDocument con un AWS SDK o CLI](#)
  - [Usare CreateMaintenanceWindow con un AWS SDK o CLI](#)
  - [Usare CreateOpsItem con un AWS SDK o CLI](#)
  - [Utilizzo di CreatePatchBaseline con una CLI](#)
  - [Utilizzo di DeleteActivation con una CLI](#)
  - [Utilizzo di DeleteAssociation con una CLI](#)
  - [Usare DeleteDocument con un AWS SDK o CLI](#)
  - [Usare DeleteMaintenanceWindow con un AWS SDK o CLI](#)
  - [Usare DeleteOpsItem con un AWS SDK](#)
  - [Utilizzo di DeleteParameter con una CLI](#)
  - [Utilizzo di DeletePatchBaseline con una CLI](#)
  - [Utilizzo di DeregisterManagedInstance con una CLI](#)
  - [Utilizzo di DeregisterPatchBaselineForPatchGroup con una CLI](#)
  - [Utilizzo di DeregisterTargetFromMaintenanceWindow con una CLI](#)
  - [Utilizzo di DeregisterTaskFromMaintenanceWindow con una CLI](#)
  - [Utilizzo di DescribeActivations con una CLI](#)
  - [Utilizzo di DescribeAssociation con una CLI](#)
  - [Utilizzo di DescribeAssociationExecutionTargets con una CLI](#)



- [Utilizzo di DescribeAssociationExecutions con una CLI](#)
- [Utilizzo di DescribeAutomationExecutions con una CLI](#)
- [Utilizzo di DescribeAutomationStepExecutions con una CLI](#)
- [Utilizzo di DescribeAvailablePatches con una CLI](#)
- [Usare DescribeDocument con un AWS SDK o CLI](#)
- [Utilizzo di DescribeDocumentPermission con una CLI](#)
- [Utilizzo di DescribeEffectiveInstanceAssociations con una CLI](#)
- [Utilizzo di DescribeEffectivePatchesForPatchBaseline con una CLI](#)
- [Utilizzo di DescribeInstanceAssociationsStatus con una CLI](#)
- [Utilizzo di DescribeInstanceInformation con una CLI](#)
- [Utilizzo di DescribeInstancePatchStates con una CLI](#)
- [Utilizzo di DescribeInstancePatchStatesForPatchGroup con una CLI](#)
- [Utilizzo di DescribeInstancePatches con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindowExecutionTaskInvocations con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindowExecutionTasks con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindowExecutions con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindowTargets con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindowTasks con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindows con una CLI](#)
- [Usare DescribeOpsItems con un AWS SDK o CLI](#)
- [Usare DescribeParameters con un AWS SDK o CLI](#)
- [Utilizzo di DescribePatchBaselines con una CLI](#)
- [Utilizzo di DescribePatchGroupState con una CLI](#)
- [Utilizzo di DescribePatchGroups con una CLI](#)
- [Utilizzo di GetAutomationExecution con una CLI](#)
- [Utilizzo di GetCommandInvocation con una CLI](#)
- [Utilizzo di GetConnectionStatus con una CLI](#)
- [Utilizzo di GetDefaultPatchBaseline con una CLI](#)
- [Utilizzo di GetDeployablePatchSnapshotForInstance con una CLI](#)
- [Utilizzo di GetDocument con una CLI](#)

- [Utilizzo di GetInventory con una CLI](#)
- [Utilizzo di GetInventorySchema con una CLI](#)
- [Utilizzo di GetMaintenanceWindow con una CLI](#)
- [Utilizzo di GetMaintenanceWindowExecution con una CLI](#)
- [Utilizzo di GetMaintenanceWindowExecutionTask con una CLI](#)
- [Usare GetParameter con un AWS SDK o CLI](#)
- [Utilizzo di GetParameterHistory con una CLI](#)
- [Utilizzo di GetParameters con una CLI](#)
- [Utilizzo di GetPatchBaseline con una CLI](#)
- [Utilizzo di GetPatchBaselineForPatchGroup con una CLI](#)
- [Utilizzo di ListAssociationVersions con una CLI](#)
- [Utilizzo di ListAssociations con una CLI](#)
- [Usare ListCommandInvocations con un AWS SDK o CLI](#)
- [Utilizzo di ListCommands con una CLI](#)
- [Utilizzo di ListComplianceItems con una CLI](#)
- [Utilizzo di ListComplianceSummaries con una CLI](#)
- [Utilizzo di ListDocumentVersions con una CLI](#)
- [Utilizzo di ListDocuments con una CLI](#)
- [Utilizzo di ListInventoryEntries con una CLI](#)
- [Utilizzo di ListResourceComplianceSummaries con una CLI](#)
- [Utilizzo di ListTagsForResource con una CLI](#)
- [Utilizzo di ModifyDocumentPermission con una CLI](#)
- [Utilizzo di PutComplianceItems con una CLI](#)
- [Utilizzo di PutInventory con una CLI](#)
- [Usare PutParameter con un AWS SDK o CLI](#)
- [Utilizzo di RegisterDefaultPatchBaseline con una CLI](#)
- [Utilizzo di RegisterPatchBaselineForPatchGroup con una CLI](#)
- [Utilizzo di RegisterTargetWithMaintenanceWindow con una CLI](#)
- [Utilizzo di RegisterTaskWithMaintenanceWindow con una CLI](#)
- [Utilizzo di RemoveTagsForResource con una CLI](#)

- [Usare SendCommand con un AWS SDK o CLI](#)
- [Utilizzo di StartAutomationExecution con una CLI](#)
- [Utilizzo di StartSession con una CLI](#)
- [Utilizzo di StopAutomationExecution con una CLI](#)
- [Utilizzo di UpdateAssociation con una CLI](#)
- [Utilizzo di UpdateAssociationStatus con una CLI](#)
- [Utilizzo di UpdateDocument con una CLI](#)
- [Utilizzo di UpdateDocumentDefaultVersion con una CLI](#)
- [Usare UpdateMaintenanceWindow con un AWS SDK o CLI](#)
- [Utilizzo di UpdateManagedInstanceRole con una CLI](#)
- [Usare UpdateOpsItem con un AWS SDK o CLI](#)
- [Utilizzo di UpdatePatchBaseline con una CLI](#)

## Salve Systems Manager

L'esempio di codice seguente mostra come iniziare a utilizzare Systems Manager.

Java

SDK per Java 2.x

### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ssm.SsmClient;
import software.amazon.awssdk.services.ssm.model.DocumentFilter;
import software.amazon.awssdk.services.ssm.model.ListDocumentsRequest;
import software.amazon.awssdk.services.ssm.model.ListDocumentsResponse;

public class HelloSSM {

 public static void main(String[] args) {
```

```
final String usage = ""

 Usage:
 <awsAccount>

 Where:
 awsAccount - Your AWS Account number.
""";

if (args.length != 1) {
 System.out.println(usage);
 System.exit(1);
}

String awsAccount = args[0] ;
Region region = Region.US_EAST_1;
SsmClient ssmClient = SsmClient.builder()
 .region(region)
 .build();

listDocuments(ssmClient, awsAccount);
}

/*
This code automatically fetches the next set of results using the `nextToken`
and
stops once the desired maxResults (20 in this case) have been reached.
*/
public static void listDocuments(SsmClient ssmClient, String awsAccount) {
 String nextToken = null;
 int totalDocumentsReturned = 0;
 int maxResults = 20;
 do {
 ListDocumentsRequest request = ListDocumentsRequest.builder()
 .documentFilterList(
 DocumentFilter.builder()
 .key("Owner")
 .value(awsAccount)
 .build()
)
 .maxResults(maxResults)
 .nextToken(nextToken)
 .build();
 }
```

```

 ListDocumentsResponse response = ssmClient.listDocuments(request);
 response.documentIdentifiers().forEach(identifier ->
 System.out.println("Document Name: " + identifier.name()));
 nextToken = response.nextToken();
 totalDocumentsReturned += response.documentIdentifiers().size();
 } while (nextToken != null && totalDocumentsReturned < maxResults);
}
}

```

- Per i dettagli sulle API, consulta la [ListDocuments](#) sezione AWS SDK for Java 2.x API Reference.

## JavaScript

### SDK per JavaScript (v3)

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```

import { paginateListDocuments, SSMClient } from "@aws-sdk/client-ssm";

// Call ListDocuments and display the result.
export const main = async () => {
 const client = new SSMClient();
 const listDocumentsPaginated = [];
 console.log(
 "Hello, AWS Systems Manager! Let's list some of your documents:\n",
);
 try {
 // The paginate function is a wrapper around the base command.
 const paginator = paginateListDocuments({ client }, { MaxResults: 5 });
 for await (const page of paginator) {
 listDocumentsPaginated.push(...page.DocumentIdentifiers);
 }
 } catch (caught) {
 console.error(`There was a problem saying hello: ${caught.message}`);
 throw caught;
 }
}

```

```
}

for (const { Name, DocumentFormat, CreatedDate } of listDocumentsPaginated) {
 console.log(`${Name} - ${DocumentFormat} - ${CreatedDate}`);
}
};

// Call function if run directly.
import { fileURLToPath } from "node:url";
if (process.argv[1] === fileURLToPath(import.meta.url)) {
 main();
}
```

- Per i dettagli sulle API, consulta la [ListDocuments](#) sezione AWS SDK per JavaScript API Reference.

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
import boto3
from botocore.exceptions import ClientError

def hello_systems_manager(ssm_client):
 """
 Use the AWS SDK for Python (Boto3) to create an AWS Systems Manager
 client and list the first 5 documents in your account.
 This example uses the default settings specified in your shared credentials
 and config files.

 :param ssm_client: A Boto3 AWS Systems Manager Client object. This object
 wraps
 the low-level AWS Systems Manager service API.
```

```
"""
print("Hello, AWS Systems Manager! Let's list some of your documents:\n")

paginator = ssm_client.get_paginator("list_documents")
page_iterator = paginator.paginate(PaginationConfig={"MaxItems": 5})
for page in page_iterator:
 for document in page["DocumentIdentifiers"]:
 print(f" {document['Name']}")

if __name__ == "__main__":
 try:
 hello_systems_manager(boto3.client("ssm"))
 except ClientError as err:
 print("Hello systems manager had an error.")
 print(err.response["Error"]["Code"])
 print(err.response["Error"]["Message"])
```

- Per i dettagli sulle API, vedi [ListDocuments](#) in AWS SDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Impara le basi di Systems Manager con un AWS SDK

Gli esempi di codice seguenti mostrano come:

- Creare una finestra di manutenzione.
- Modificare la pianificazione della finestra di manutenzione.
- Crea un documento.
- Inviare un comando a un'istanza EC2 specificata.
- Crea un OpsItem.
- Aggiorna e risolvi il OpsItem.
- Elimina la finestra di manutenzione OpsItem e il documento.

## Java

### SDK per Java 2.x

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
import software.amazon.awssdk.services.ssm.model.DocumentAlreadyExistsException;
import software.amazon.awssdk.services.ssm.model.SsmException;

import java.util.Map;
import java.util.Scanner;
public class SSMScenario {
 public static final String DASHES = new String(new char[80]).replace("\0",
"-");
 private static final String ROLES_STACK = "SsmStack3`1";

 public static void main(String[] args) {
 String usage = ""
 Usage:
 <title> <source> <category> <severity>

 Where:
 title - The title of the parameter (default is Disk Space Alert).
 source - The source of the parameter (default is EC2).
 category - The category of the parameter. Valid values are
'Availability', 'Cost', 'Performance', 'Recovery', 'Security' (default is
Performance).
 severity - The severity of the parameter. Severity should be a
number from 1 to 4 (default is 2).
 """;

 Scanner scanner = new Scanner(System.in);
 SSMActions actions = new SSMActions();
 String documentName;
 String windowName;

 System.out.println("Use AWS CloudFormation to create the EC2 instance
that is required for this scenario.");
```



```

 CloudFormationHelper.deployCloudFormationStack(ROLES_STACK);
 Map<String, String> stackOutputs =
CloudFormationHelper.getStackOutputsAsync(ROLES_STACK).join();
 String instanceId = stackOutputs.get("InstanceId");
 System.out.println("The Instance ID: " + instanceId + " was created.");
 String title = "Disk Space Alert" ;
 String source = "EC2" ;
 String category = "Availability" ;
 String severity = "2" ;

 System.out.println(DASHES);
 System.out.println("""
 Welcome to the AWS Systems Manager SDK Basics scenario.
 This Java program demonstrates how to interact with AWS Systems
Manager using the AWS SDK for Java (v2).
 AWS Systems Manager is the operations hub for your AWS
applications and resources and a secure end-to-end management solution.
 The program's primary functionalities include creating a
maintenance window, creating a document, sending a command to a document,
 listing documents, listing commands, creating an OpsItem,
modifying an OpsItem, and deleting AWS SSM resources.
 Upon completion of the program, all AWS resources are cleaned up.
 Let's get started...

 """);
 waitForInputToContinue(scanner);
 System.out.println(DASHES);

 System.out.println("1. Create an SSM maintenance window.");
 System.out.println("Please enter the maintenance window name (default is
ssm-maintenance-window):");
 String win = scanner.nextLine();
 windowName = win.isEmpty() ? "ssm-maintenance-window" : win;
 String winId = null;
 try {
 winId = actions.createMaintenanceWindow(windowName);
 waitForInputToContinue(scanner);
 System.out.println("The maintenance window ID is: " + winId);
 } catch (DocumentAlreadyExistsException e) {
 System.err.println("The SSM maintenance window already exists.
Retrieving existing window ID...");
 String existingWinId = actions.createMaintenanceWindow(windowName);
 System.out.println("Existing window ID: " + existingWinId);
 } catch (SsmException e) {

```

```
 System.err.println("SSM error: " + e.getMessage());
 return;
 } catch (RuntimeException e) {
 System.err.println("Unexpected error: " + e.getMessage());
 return;
 }
 waitForInputToContinue(scanner);
 System.out.println(DASHES);

 System.out.println("2. Modify the maintenance window by changing the
schedule");
 waitForInputToContinue(scanner);
 try {
 actions.updateSSMMaintenanceWindow(winId, windowName);
 waitForInputToContinue(scanner);
 System.out.println("The SSM maintenance window was successfully
updated");
 } catch (SsmException e) {
 System.err.println("SSM error: " + e.getMessage());
 return;
 } catch (RuntimeException e) {
 System.err.println("Unexpected error: " + e.getMessage());
 return;
 }
 waitForInputToContinue(scanner);
 System.out.println(DASHES);

 System.out.println("3. Create an SSM document that defines the actions
that Systems Manager performs on your managed nodes.");
 System.out.println("Please enter the document name (default is
ssmdocument):");
 String doc = scanner.nextLine();
 documentName = doc.isEmpty() ? "ssmdocument" : doc;
 try {
 actions.createSSMDoc(documentName);
 waitForInputToContinue(scanner);
 System.out.println("The SSM document was successfully created");
 } catch (DocumentAlreadyExistsException e) {
 System.err.println("The SSM document already exists. Moving on");
 } catch (SsmException e) {
 System.err.println("SSM error: " + e.getMessage());
 return;
 } catch (RuntimeException e) {
 System.err.println("Unexpected error: " + e.getMessage());
```

```
 }
 waitForInputToContinue(scanner);
 System.out.println(DASHES);

 System.out.println("4. Now we are going to run a command on an EC2
instance");
 waitForInputToContinue(scanner);
 String commandId="";
 try {
 commandId = actions.sendSSMCommand(documentName, instanceId);
 waitForInputToContinue(scanner);
 System.out.println("The command was successfully sent. Command ID: "
+ commandId);
 } catch (SsmException e) {
 System.err.println("SSM error: " + e.getMessage());
 } catch (InterruptedException e) {
 System.err.println("Thread was interrupted: " + e.getMessage());
 } catch (RuntimeException e) {
 System.err.println("Unexpected error: " + e.getMessage());
 }
 waitForInputToContinue(scanner);
 System.out.println(DASHES);

 System.out.println("5. Lets get the time when the specific command was
sent to the specific managed node");
 waitForInputToContinue(scanner);
 try {
 actions.displayCommands(commandId);
 System.out.println("The command invocations were successfully
displayed.");
 } catch (SsmException e) {
 System.err.println("SSM error: " + e.getMessage());
 return;
 } catch (RuntimeException e) {
 System.err.println("Unexpected error: " + e.getMessage());
 return;
 }
 waitForInputToContinue(scanner);
 System.out.println(DASHES);

 System.out.println(DASHES);
 System.out.println("""
 6. Now we will create an SSM OpsItem.
```

A SSM OpsItem is a feature provided by Amazon's Systems Manager (SSM) service.

It is a type of operational data item that allows you to manage and track various operational issues, events, or tasks within your AWS environment.

You can create OpsItems to track and manage operational issues as they arise.

For example, you could create an OpsItem whenever your application detects a critical error

or an anomaly in your infrastructure.

```
""");
```

```

waitForInputToContinue(scanner);
String opsItemId;
try {
 opsItemId = actions.createSSMOpsItem(title, source, category,
severity);
 System.out.println(opsItemId + " was created");
} catch (SsmException e) {
 System.err.println("SSM error: " + e.getMessage());
 return;
} catch (RuntimeException e) {
 System.err.println("Unexpected error: " + e.getMessage());
 return;
}
waitForInputToContinue(scanner);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("7. Now we will update the SSM OpsItem "+opsItemId);
waitForInputToContinue(scanner);
String description = "An update to "+opsItemId ;
try {
 actions.updateOpsItem(opsItemId, title, description);
} catch (SsmException e) {
 System.err.println("SSM error: " + e.getMessage());
 return;
} catch (RuntimeException e) {
 System.err.println("Unexpected error: " + e.getMessage());
 return;
}

System.out.println(DASHES);
```

```
 System.out.println("8. Now we will get the status of the SSM OpsItem\n"+opsItemId);\n waitForInputToContinue(scanner);\n try {\n actions.describeOpsItems(opsItemId);\n } catch (SsmException e) {\n System.err.println("SSM error: " + e.getMessage());\n return;\n } catch (RuntimeException e) {\n System.err.println("Unexpected error: " + e.getMessage());\n return;\n }\n\n System.out.println(DASHES);\n System.out.println("9. Now we will resolve the SSM OpsItem "+opsItemId);\n waitForInputToContinue(scanner);\n try {\n actions.resolveOpsItem(opsItemId);\n } catch (SsmException e) {\n System.err.println("SSM error: " + e.getMessage());\n return;\n } catch (RuntimeException e) {\n System.err.println("Unexpected error: " + e.getMessage());\n return;\n }\n\n System.out.println(DASHES);\n System.out.println("10. Would you like to delete the AWS Systems Manager\nresources? (y/n)");\n String delAns = scanner.nextLine().trim();\n if (delAns.equalsIgnoreCase("y")) {\n System.out.println("You selected to delete the resources.");\n waitForInputToContinue(scanner);\n try {\n actions.deleteMaintenanceWindow(winId);\n actions.deleteDoc(documentName);\n } catch (SsmException e) {\n System.err.println("SSM error: " + e.getMessage());\n return;\n } catch (RuntimeException e) {\n System.err.println("Unexpected error: " + e.getMessage());\n return;\n }\n } else {
```

```

 System.out.println("The AWS Systems Manager resources will not be
deleted");
 }
 System.out.println(DASHES);
 CloudFormationHelper.destroyCloudFormationStack(ROLES_STACK);
 System.out.println("This concludes the AWS Systems Manager SDK Basics
scenario.");
 System.out.println(DASHES);
}

private static void waitForInputToContinue(Scanner scanner) {
 while (true) {
 System.out.println("");
 System.out.println("Enter 'c' followed by <ENTER> to continue:");
 String input = scanner.nextLine();

 if (input.trim().equalsIgnoreCase("c")) {
 System.out.println("Continuing with the program...");
 System.out.println("");
 break;
 } else {
 // Handle invalid input.
 System.out.println("Invalid input. Please try again.");
 }
 }
}
}
}

```

Una classe wrapper per i metodi SDK di Systems Manager.

```

public class SSMActions {

 private static SsmAsyncClient ssmAsyncClient;

 private static SsmAsyncClient getAsyncClient() {
 if (ssmAsyncClient == null) {
 SdkAsyncHttpClient httpClient = NettyNioAsyncHttpClient.builder()
 .maxConcurrency(100)
 .connectionTimeout(Duration.ofSeconds(60))
 .readTimeout(Duration.ofSeconds(60))
 .writeTimeout(Duration.ofSeconds(60))
 .build();
 }
 }
}

```

```

 ClientOverrideConfiguration overrideConfig =
ClientOverrideConfiguration.builder()
 .apiCallTimeout(Duration.ofMinutes(2))
 .apiCallAttemptTimeout(Duration.ofSeconds(90))
 .retryPolicy(RetryPolicy.builder()
 .numRetries(3)
 .build())
 .build();

 ssmAsyncClient = SsmAsyncClient.builder()
 .region(Region.US_WEST_2)
 .httpClient(httpClient)
 .overrideConfiguration(overrideConfig)
 .build();
 }
 return ssmAsyncClient;
}

/**
 * Deletes an AWS SSM document asynchronously.
 *
 * @param documentName The name of the document to delete.
 * <p>
 * This method initiates an asynchronous request to delete an SSM document.
 * If an exception occurs, it handles the error appropriately.
 */
public void deleteDoc(String documentName) {
 DeleteDocumentRequest documentRequest = DeleteDocumentRequest.builder()
 .name(documentName)
 .build();

 CompletableFuture<Void> future = CompletableFuture.runAsync(() -> {
 getAsyncClient().deleteDocument(documentRequest)
 .thenAccept(response -> {
 System.out.println("The SSM document was successfully
deleted.");
 })
 .exceptionally(ex -> {
 throw new CompletionException(ex);
 }).join();
 }).exceptionally(ex -> {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;

```

```

 if (cause instanceof SsmException) {
 throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
 } else {
 throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
 }
 });

 try {
 future.join();
 } catch (CompletionException ex) {
 throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
ex.getCause() : ex;
 }
}

/**
 * Deletes an AWS SSM Maintenance Window asynchronously.
 *
 * @param winId The ID of the Maintenance Window to delete.
 * <p>
 * This method initiates an asynchronous request to delete an SSM Maintenance
Window.
 * If an exception occurs, it handles the error appropriately.
 */
public void deleteMaintenanceWindow(String winId) {
 DeleteMaintenanceWindowRequest windowRequest =
DeleteMaintenanceWindowRequest.builder()
 .windowId(winId)
 .build();

 CompletableFuture<Void> future = CompletableFuture.runAsync(() -> {
 getAsyncClient().deleteMaintenanceWindow(windowRequest)
 .thenAccept(response -> {
 System.out.println("The maintenance window was
successfully deleted.");
 })
 .exceptionally(ex -> {
 throw new CompletionException(ex);
 }).join();
 }).exceptionally(ex -> {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;

```



```

 if (cause instanceof SsmException) {
 throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
 } else {
 throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
 }
 });

 try {
 future.join();
 } catch (CompletionException ex) {
 throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
ex.getCause() : ex;
 }
}

/**
 * Resolves an AWS SSM OpsItem asynchronously.
 *
 * @param opsID The ID of the OpsItem to resolve.
 * <p>
 * This method initiates an asynchronous request to resolve an SSM OpsItem.
 * If an exception occurs, it handles the error appropriately.
 */
public void resolveOpsItem(String opsID) {
 UpdateOpsItemRequest opsItemRequest = UpdateOpsItemRequest.builder()
 .opsItemId(opsID)
 .status(OpsItemStatus.RESOLVED)
 .build();

 CompletableFuture<Void> future = CompletableFuture.runAsync(() -> {
 getAsyncClient().updateOpsItem(opsItemRequest)
 .thenAccept(response -> {
 System.out.println("OpsItem resolved successfully.");
 })
 .exceptionally(ex -> {
 throw new CompletionException(ex);
 }).join();
 }).exceptionally(ex -> {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
 if (cause instanceof SsmException) {

```

```

 throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
 } else {
 throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
 }
});

 try {
 future.join();
 } catch (CompletionException ex) {
 throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
ex.getCause() : ex;
 }
}

/**
 * Describes AWS SSM OpsItems asynchronously.
 *
 * @param key The key to filter OpsItems by (e.g., OPS_ITEM_ID).
 *
 * This method initiates an asynchronous request to describe SSM OpsItems.
 * If the request is successful, it prints the title and status of each
OpsItem.
 * If an exception occurs, it handles the error appropriately.
 */
public void describeOpsItems(String key) {
 OpsItemFilter filter = OpsItemFilter.builder()
 .key(OpsItemFilterKey.OPS_ITEM_ID)
 .values(key)
 .operator(OpsItemFilterOperator.EQUAL)
 .build();

 DescribeOpsItemsRequest itemsRequest = DescribeOpsItemsRequest.builder()
 .maxResults(10)
 .opsItemFilters(filter)
 .build();

 CompletableFuture<Void> future = CompletableFuture.runAsync(() -> {
 getAsyncClient().describeOpsItems(itemsRequest)
 .thenAccept(itemsResponse -> {
 List<OpsItemSummary> items =
itemsResponse.opsItemSummaries();
 for (OpsItemSummary item : items) {

```

```

 System.out.println("The item title is " +
 item.title() + " and the status is " + item.status().toString());
 }
})
 .exceptionally(ex -> {
 throw new CompletionException(ex);
 }).join();
}).exceptionally(ex -> {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
 if (cause instanceof SsmException) {
 throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
 } else {
 throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
 }
});

 try {
 future.join();
 } catch (CompletionException ex) {
 throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
ex.getCause() : ex;
 }
}

/**
 * Updates the AWS SSM OpsItem asynchronously.
 *
 * @param opsItemId The ID of the OpsItem to update.
 * @param title The new title of the OpsItem.
 * @param description The new description of the OpsItem.
 * <p>
 * This method initiates an asynchronous request to update an SSM OpsItem.
 * If the request is successful, it completes without returning a value.
 * If an exception occurs, it handles the error appropriately.
 */
public void updateOpsItem(String opsItemId, String title, String description)
{
 Map<String, OpsItemDataValue> operationalData = new HashMap<>();
 operationalData.put("key1",
OpsItemDataValue.builder().value("value1").build());

```

```

 operationalData.put("key2",
OpsItemDataValue.builder().value("value2").build());

 CompletableFuture<Void> future =
getOpsItem(opsItemId).thenCompose(opsItem -> {
 UpdateOpsItemRequest request = UpdateOpsItemRequest.builder()
 .opsItemId(opsItemId)
 .title(title)
 .operationalData(operationalData)
 .status(opsItem.statusAsString())
 .description(description)
 .build();

 return getAsyncClient().updateOpsItem(request).thenAccept(response ->
{
 System.out.println(opsItemId + " updated successfully.");
 }).exceptionally(ex -> {
 throw new CompletionException(ex);
 });
 }).exceptionally(ex -> {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
 if (cause instanceof SsmException) {
 throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
 } else {
 throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
 }
 });

 try {
 future.join();
 } catch (CompletionException ex) {
 throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
ex.getCause() : ex;
 }
 }

 private static CompletableFuture<OpsItem> getOpsItem(String opsItemId) {
 GetOpsItemRequest request =
GetOpsItemRequest.builder().opsItemId(opsItemId).build();

```

```

 return
getAsyncClient().getOpsItem(request).thenApply(GetOpsItemResponse::opsItem);
 }

 /**
 * Creates an SSM OpsItem asynchronously.
 *
 * @param title The title of the OpsItem.
 * @param source The source of the OpsItem.
 * @param category The category of the OpsItem.
 * @param severity The severity of the OpsItem.
 * @return The ID of the created OpsItem.
 * <p>
 * This method initiates an asynchronous request to create an SSM OpsItem.
 * If the request is successful, it returns the OpsItem ID.
 * If an exception occurs, it handles the error appropriately.
 */
 public String createSSMOpsItem(String title, String source, String category,
String severity) {
 CreateOpsItemRequest opsItemRequest = CreateOpsItemRequest.builder()
 .description("Created by the SSM Java API")
 .title(title)
 .source(source)
 .category(category)
 .severity(severity)
 .build();

 CompletableFuture<CreateOpsItemResponse> future =
getAsyncClient().createOpsItem(opsItemRequest);

 try {
 CreateOpsItemResponse response = future.join();
 return response.opsItemId();
 } catch (CompletionException e) {
 Throwable cause = e.getCause();
 if (cause instanceof SsmException) {
 throw (SsmException) cause;
 } else {
 throw new RuntimeException(cause);
 }
 }
 }

 /**

```

```

 * Displays the date and time when the specific command was invoked.
 *
 * @param commandId The ID of the command to describe.
 * <p>
 * This method initiates an asynchronous request to list command invocations
 and prints the date and time of each command invocation.
 * If an exception occurs, it handles the error appropriately.
 */
 public void displayCommands(String commandId) {
 ListCommandInvocationsRequest commandInvocationsRequest =
ListCommandInvocationsRequest.builder()
 .commandId(commandId)
 .build();

 CompletableFuture<ListCommandInvocationsResponse> future =
getAsyncClient().listCommandInvocations(commandInvocationsRequest);
 future.thenAccept(response -> {
 List<CommandInvocation> commandList = response.commandInvocations();
 DateTimeFormatter formatter = DateTimeFormatter.ofPattern("yyyy-MM-dd
HH:mm:ss").withZone(ZoneId.systemDefault());
 for (CommandInvocation invocation : commandList) {
 System.out.println("The time of the command invocation is " +
formatter.format(invocation.requestedDateTime()));
 }
 }).exceptionally(ex -> {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
 if (cause instanceof SsmException) {
 throw (SsmException) cause;
 } else {
 throw new RuntimeException(cause);
 }
 }).join();
 }

 /**
 * Sends a SSM command to a managed node asynchronously.
 *
 * @param documentName The name of the document to use.
 * @param instanceId The ID of the instance to send the command to.
 * @return The command ID.
 * <p>
 * This method initiates asynchronous requests to send a SSM command to a
 managed node.

```

```
 * It waits until the document is active, sends the command, and checks the
 command execution status.
 */
 public String sendSSMCommand(String documentName, String instanceId) throws
 InterruptedException, SsmException {
 // Before we use Document to send a command - make sure it is active.
 CompletableFuture<Void> documentActiveFuture =
 CompletableFuture.runAsync(() -> {
 boolean isDocumentActive = false;
 DescribeDocumentRequest request = DescribeDocumentRequest.builder()
 .name(documentName)
 .build();

 while (!isDocumentActive) {
 CompletableFuture<DescribeDocumentResponse> response =
 getAsyncClient().describeDocument(request);
 String documentStatus =
 response.join().document().statusAsString();
 if (documentStatus.equals("Active")) {
 System.out.println("The SSM document is active and ready to
 use.");
 isDocumentActive = true;
 } else {
 System.out.println("The SSM document is not active. Status: "
 + documentStatus);
 try {
 Thread.sleep(5000);
 } catch (InterruptedException e) {
 throw new RuntimeException(e);
 }
 }
 }
 });

 documentActiveFuture.join();

 // Create the SendCommandRequest.
 SendCommandRequest commandRequest = SendCommandRequest.builder()
 .documentName(documentName)
 .instanceIds(instanceId)
 .build();

 // Send the command.
```

```

 CompletableFuture<SendCommandResponse> commandFuture =
getAsyncClient().sendCommand(commandRequest);
 final String[] commandId = {null};

 commandFuture.whenComplete((commandResponse, ex) -> {
 if (commandResponse != null) {
 commandId[0] = commandResponse.command().commandId();
 System.out.println("Command ID: " + commandId[0]);

 // Wait for the command execution to complete.
 GetCommandInvocationRequest invocationRequest =
GetCommandInvocationRequest.builder()
 .commandId(commandId[0])
 .instanceId(instanceId)
 .build();

 try {
 System.out.println("Wait 5 secs");
 TimeUnit.SECONDS.sleep(5);

 // Retrieve the command execution details.
 CompletableFuture<GetCommandInvocationResponse>
invocationFuture = getAsyncClient().getCommandInvocation(invocationRequest);
 invocationFuture.whenComplete((commandInvocationResponse,
invocationEx) -> {
 if (commandInvocationResponse != null) {
 // Check the status of the command execution.
 CommandInvocationStatus status =
commandInvocationResponse.status();
 if (status == CommandInvocationStatus.SUCCESS) {
 System.out.println("Command execution
successful");
 } else {
 System.out.println("Command execution failed.
Status: " + status);
 }
 } else {
 Throwable invocationCause = (invocationEx instanceof
CompletionException) ? invocationEx.getCause() : invocationEx;
 throw new CompletionException(invocationCause);
 }
 }).join();
 } catch (InterruptedException e) {
 throw new RuntimeException(e);

```



```

 }
 } else {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
 if (cause instanceof SsmException) {
 throw (SsmException) cause;
 } else {
 throw new RuntimeException(cause);
 }
 }
}).join();

return commandId[0];
}

/**
 * Creates an AWS SSM document asynchronously.
 *
 * @param docName The name of the document to create.
 * <p>
 * This method initiates an asynchronous request to create an SSM document.
 * If the request is successful, it prints the document status.
 * If an exception occurs, it handles the error appropriately.
 */
public void createSSMDoc(String docName) throws SsmException {
 String jsonData = ""
 {
 "schemaVersion": "2.2",
 "description": "Run a simple shell command",
 "mainSteps": [
 {
 "action": "aws:runShellScript",
 "name": "runEchoCommand",
 "inputs": {
 "runCommand": [
 "echo 'Hello, world!'"
]
 }
 }
]
 }
 """;

 CreateDocumentRequest request = CreateDocumentRequest.builder()

```

```

 .content(jsonData)
 .name(docName)
 .documentType(DocumentType.COMMAND)
 .build();

 CompletableFuture<CreateDocumentResponse> future =
getAsyncClient().createDocument(request);
 future.thenAccept(response -> {
 System.out.println("The status of the SSM document is " +
response.documentDescription().status());
 }).exceptionally(ex -> {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
 if (cause instanceof DocumentAlreadyExistsException) {
 throw new CompletionException(cause);
 } else if (cause instanceof SsmException) {
 throw new CompletionException(cause);
 } else {
 throw new RuntimeException(cause);
 }
 }).join();
}

/**
 * Updates an SSM maintenance window asynchronously.
 *
 * @param id The ID of the maintenance window to update.
 * @param name The new name for the maintenance window.
 * <p>
 * This method initiates an asynchronous request to update an SSM maintenance
window.
 * If the request is successful, it prints a success message.
 * If an exception occurs, it handles the error appropriately.
 */
public void updateSSMMaintenanceWindow(String id, String name) throws
SsmException {
 UpdateMaintenanceWindowRequest updateRequest =
UpdateMaintenanceWindowRequest.builder()
 .windowId(id)
 .allowUnassociatedTargets(true)
 .duration(24)
 .enabled(true)
 .name(name)
 .schedule("cron(0 0 ? * MON *)")

```

```

 .build();

 CompletableFuture<UpdateMaintenanceWindowResponse> future =
getAsyncClient().updateMaintenanceWindow(updateRequest);
 future.whenComplete((response, ex) -> {
 if (response != null) {
 System.out.println("The SSM maintenance window was successfully
updated");
 } else {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
 if (cause instanceof SsmException) {
 throw new CompletionException(cause);
 } else {
 throw new RuntimeException(cause);
 }
 }
 }).join();
 }

/**
 * Creates an SSM maintenance window asynchronously.
 *
 * @param winName The name of the maintenance window.
 * @return The ID of the created or existing maintenance window.
 * <p>
 * This method initiates an asynchronous request to create an SSM maintenance
window.
 * If the request is successful, it prints the maintenance window ID.
 * If an exception occurs, it handles the error appropriately.
 */
 public String createMaintenanceWindow(String winName) throws SsmException,
DocumentAlreadyExistsException {
 CreateMaintenanceWindowRequest request =
CreateMaintenanceWindowRequest.builder()
 .name(winName)
 .description("This is my maintenance window")
 .allowUnassociatedTargets(true)
 .duration(2)
 .cutoff(1)
 .schedule("cron(0 10 ? * MON-FRI *)")
 .build();
 }

```

```

 CompletableFuture<CreateMaintenanceWindowResponse> future =
getAsyncClient().createMaintenanceWindow(request);
 final String[] windowId = {null};
 future.whenComplete((response, ex) -> {
 if (response != null) {
 String maintenanceWindowId = response.windowId();
 System.out.println("The maintenance window id is " +
maintenanceWindowId);
 windowId[0] = maintenanceWindowId;
 } else {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
 if (cause instanceof DocumentAlreadyExistsException) {
 throw new CompletionException(cause);
 } else if (cause instanceof SsmException) {
 throw new CompletionException(cause);
 } else {
 throw new RuntimeException(cause);
 }
 }
 }).join();

 if (windowId[0] == null) {
 MaintenanceWindowFilter filter = MaintenanceWindowFilter.builder()
 .key("name")
 .values(winName)
 .build();

 DescribeMaintenanceWindowsRequest winRequest =
DescribeMaintenanceWindowsRequest.builder()
 .filters(filter)
 .build();

 CompletableFuture<DescribeMaintenanceWindowsResponse> describeFuture
= getAsyncClient().describeMaintenanceWindows(winRequest);
 describeFuture.whenComplete((describeResponse, describeEx) -> {
 if (describeResponse != null) {
 List<MaintenanceWindowIdentity> windows =
describeResponse.windowIdentities();
 if (!windows.isEmpty()) {
 windowId[0] = windows.get(0).windowId();
 System.out.println("Window ID: " + windowId[0]);
 } else {
 System.out.println("Window not found.");
 }
 }
 });
 }
 }
}

```

```
 windowId[0] = "";
 }
 } else {
 Throwable describeCause = (describeEx instanceof
CompletionException) ? describeEx.getCause() : describeEx;
 throw new RuntimeException("Error describing maintenance
windows: " + describeCause.getMessage(), describeCause);
 }
 }).join();
}

return windowId[0];
}
}
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento API di AWS SDK for Java 2.x .
  - [CreateDocument](#)
  - [CreateMaintenanceWindow](#)
  - [CreateOpsItem](#)
  - [DeleteMaintenanceWindow](#)
  - [ListCommandInvocations](#)
  - [SendCommand](#)
  - [UpdateOpsItem](#)

## JavaScript

### SDK per JavaScript (v3)

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
import {
 Scenario,
```

```

 ScenarioAction,
 ScenarioInput,
 ScenarioOutput,
} from "@aws-doc-sdk-examples/lib/scenario/index.js";
import { fileURLToPath } from "node:url";
import {
 CreateDocumentCommand,
 CreateMaintenanceWindowCommand,
 CreateOpsItemCommand,
 DeleteDocumentCommand,
 DeleteMaintenanceWindowCommand,
 DeleteOpsItemCommand,
 DescribeOpsItemsCommand,
 DocumentAlreadyExists,
 OpsItemStatus,
 waitUntilCommandExecuted,
 CancelCommandCommand,
 paginateListCommandInvocations,
 SendCommandCommand,
 UpdateMaintenanceWindowCommand,
 UpdateOpsItemCommand,
 SSMClient,
} from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * @typedef {{
 * ssmClient: import('@aws-sdk/client-ssm').SSMClient,
 * documentName?: string
 * maintenanceWindow?: string
 * winId?: int
 * ec2InstanceId?: string
 * requestedDateTime?: Date
 * opsItemId?: string
 * askToDeleteResources?: boolean
 * }} State
 */

const defaultMaintenanceWindow = "ssm-maintenance-window";
const defaultDocumentName = "ssmdocument";
// The timeout duration is highly dependent on the specific setup and environment
// necessary. This example handles only the most common error cases, and uses a
// much shorter duration than most productions systems would use.
const COMMAND_TIMEOUT_DURATION_SECONDS = 30; // 30 seconds

```

```
const pressEnter = new ScenarioInput("continue", "Press Enter to continue", {
 type: "confirm",
});

const greet = new ScenarioOutput(
 "greet",
 `Welcome to the AWS Systems Manager SDK Getting Started scenario.
 This program demonstrates how to interact with Systems Manager using the AWS
 SDK for JavaScript V3.
 Systems Manager is the operations hub for your AWS applications and resources
 and a secure end-to-end management solution.
 The program's primary functions include creating a maintenance window,
 creating a document, sending a command to a document,
 listing documents, listing commands, creating an OpsItem, modifying an
 OpsItem, and deleting Systems Manager resources.
 Upon completion of the program, all AWS resources are cleaned up.
 Let's get started...`,
 { header: true },
);

const createMaintenanceWindow = new ScenarioOutput(
 "createMaintenanceWindow",
 "Step 1: Create a Systems Manager maintenance window.",
);

const getMaintenanceWindow = new ScenarioInput(
 "maintenanceWindow",
 "Please enter the maintenance window name:",
 { type: "input", default: defaultMaintenanceWindow },
);

export const sdkCreateMaintenanceWindow = new ScenarioAction(
 "sdkCreateMaintenanceWindow",
 async (/** @type {State} */ state) => {
 try {
 const response = await state.ssmClient.send(
 new CreateMaintenanceWindowCommand({
 Name: state.maintenanceWindow,
 Schedule: "cron(0 10 ? * MON-FRI *)", //The schedule of the maintenance
 window in the form of a cron or rate expression.
 Duration: 2, //The duration of the maintenance window in hours.
 })
);
 } catch (error) {
 console.error(error);
 }
 })
);
```

```

 Cutoff: 1, //The number of hours before the end of the maintenance
 window that Amazon Web Services Systems Manager stops scheduling new tasks for
 execution.
 AllowUnassociatedTargets: true, //Allow the maintenance window to run
 on managed nodes, even if you haven't registered those nodes as targets.
 })),
);
 state.winId = response.WindowId;
} catch (caught) {
 console.error(caught.message);
 console.log(
 `An error occurred while creating the maintenance window. Please fix the
 error and try again. Error message: ${caught.message}`,
);
 throw caught;
}
},
);

const modifyMaintenanceWindow = new ScenarioOutput(
 "modifyMaintenanceWindow",
 "Modify the maintenance window by changing the schedule.",
);

const sdkModifyMaintenanceWindow = new ScenarioAction(
 "sdkModifyMaintenanceWindow",
 async (** @type {State} */ state) => {
 try {
 await state.ssmClient.send(
 new UpdateMaintenanceWindowCommand({
 WindowId: state.winId,
 Schedule: "cron(0 0 ? * MON *)",
 }),
);
 } catch (caught) {
 console.error(caught.message);
 console.log(
 `An error occurred while modifying the maintenance window. Please fix the
 error and try again. Error message: ${caught.message}`,
);
 throw caught;
 }
 },
);

```



```
const createSystemsManagerActions = new ScenarioOutput(
 "createSystemsManagerActions",
 "Create a document that defines the actions that Systems Manager performs on
 your EC2 instance.",
);

const getDocumentName = new ScenarioInput(
 "documentName",
 "Please enter the document: ",
 { type: "input", default: defaultDocumentName },
);

const sdkCreateSSMDoc = new ScenarioAction(
 "sdkCreateSSMDoc",
 async (** @type {State} */ state) => {
 const contentData = `{
 "schemaVersion": "2.2",
 "description": "Run a simple shell command",
 "mainSteps": [
 {
 "action": "aws:runShellScript",
 "name": "runEchoCommand",
 "inputs": {
 "runCommand": [
 "echo 'Hello, world!'"
]
 }
 }
]
 }`;

 try {
 await state.ssmClient.send(
 new CreateDocumentCommand({
 Content: contentData,
 Name: state.documentName,
 DocumentType: "Command",
 }),
);
 } catch (caught) {
 console.log(`Exception type: (${typeof caught})`);
 if (caught instanceof DocumentAlreadyExists) {
 console.log("Document already exists. Continuing...\n");
 } else {
```

```

 console.error(caught.message);
 console.log(
 `An error occurred while creating the document. Please fix the error
and try again. Error message: ${caught.message}`,
);
 throw caught;
 }
}
},
);

const ec2HelloWorld = new ScenarioOutput(
 "ec2HelloWorld",
 `Now you have the option of running a command on an EC2 instance that echoes
'Hello, world!'. In order to run this command, you must provide the instance ID
of a Linux EC2 instance. If you do not already have a running Linux EC2 instance
in your account, you can create one using the AWS console. For information
about creating an EC2 instance, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-launch-instance-wizard.html.`,
);

const enterIdOrSkipEC2HelloWorld = new ScenarioInput(
 "enterIdOrSkipEC2HelloWorld",
 "Enter your EC2 InstanceId or press enter to skip this step: ",
 { type: "input", default: "" },
);

const sdkEC2HelloWorld = new ScenarioAction(
 "sdkEC2HelloWorld",
 async (** @type {State} */ state) => {
 try {
 const response = await state.ssmClient.send(
 new SendCommandCommand({
 DocumentName: state.documentName,
 InstanceIds: [state.ec2InstanceId],
 TimeoutSeconds: COMMAND_TIMEOUT_DURATION_SECONDS,
 }),
);
 state.CommandId = response.Command.CommandId;
 } catch (caught) {
 console.error(caught.message);
 console.log(
 `An error occurred while sending the command. Please fix the error and
try again. Error message: ${caught.message}`,
);
 }
 },
);

```

```

);
 throw caught;
 }
},
{
 skipWhen: (/** @type {State} */ state) =>
 state.enterIdOrSkipEC2HelloWorld === "",
},
);

const sdkGetCommandTime = new ScenarioAction(
 "sdkGetCommandTime",
 async (/** @type {State} */ state) => {
 const listInvocationsPaginated = [];
 console.log(
 "Let's get the time when the specific command was sent to the specific
managed node.",
);

 console.log(
 `First, we'll wait for the command to finish executing. This may take up to
${COMMAND_TIMEOUT_DURATION_SECONDS} seconds.`,
);
 const commandExecutedResult = waitUntilCommandExecuted(
 { client: state.ssmClient },
 {
 CommandId: state.CommandId,
 InstanceId: state.ec2InstanceId,
 },
);
 // This is necessary because the TimeoutSeconds of SendCommandCommand is only
 for the delivery, not execution.
 try {
 await new Promise((_, reject) =>
 setTimeout(
 reject,
 COMMAND_TIMEOUT_DURATION_SECONDS * 1000,
 new Error("Command Timed Out"),
),
);
 } catch (caught) {
 if (caught.message === "Command Timed Out") {
 commandExecutedResult.state = "TIMED_OUT";
 } else {

```

```

 throw caught;
 }
}

if (commandExecutedResult.state !== "SUCCESS") {
 console.log(
 `The command with id: ${state.CommandId} did not execute in the allotted
time. Canceling command.`,
);
 state.ssmClient.send(
 new CancelCommandCommand({
 CommandId: state.CommandId,
 }),
);
 state.enterIdOrSkipEC2HelloWorld === "";
 return;
}

for await (const page of paginateListCommandInvocations(
 { client: state.ssmClient },
 { CommandId: state.CommandId },
)) {
 listInvocationsPaginated.push(...page.CommandInvocations);
}
/**
 * @type {import('@aws-sdk/client-ssm').CommandInvocation}
 */
const commandInvocation = listInvocationsPaginated.shift(); // Because the
call was made with CommandId, there's only one result, so shift it off.
state.requestedDateTime = commandInvocation.RequestedDateTime;

console.log(
 `The command invocation happened at: ${state.requestedDateTime}.`,
);
},
{
 skipWhen: (/** @type {State} */ state) =>
 state.enterIdOrSkipEC2HelloWorld === "",
},
);

const createSSMOpsItem = new ScenarioOutput(
 "createSSMOpsItem",

```

```

 `Now we will create a Systems Manager OpsItem. An OpsItem is a feature provided
 by the Systems Manager service. It is a type of operational data item that
 allows you to manage and track various operational issues, events, or tasks
 within your AWS environment.
 You can create OpsItems to track and manage operational issues as they arise.
 For example, you could create an OpsItem whenever your application detects a
 critical error or an anomaly in your infrastructure.`
);

const sdkCreateSSMOpsItem = new ScenarioAction(
 "sdkCreateSSMOpsItem",
 async (/** @type {State} */ state) => {
 try {
 const response = await state.ssmClient.send(
 new CreateOpsItemCommand({
 Description: "Created by the System Manager Javascript API",
 Title: "Disk Space Alert",
 Source: "EC2",
 Category: "Performance",
 Severity: "2",
 })
);
 state.opsItemId = response.OpsItemId;
 } catch (caught) {
 console.error(caught.message);
 console.log(
 `An error occurred while creating the ops item. Please fix the error and
 try again. Error message: ${caught.message}`
);
 throw caught;
 }
 },
);

const updateOpsItem = new ScenarioOutput(
 "updateOpsItem",
 (/** @type {State} */ state) => {
 `Now we will update the OpsItem: ${state.opsItemId}`,
),
);

const sdkUpdateOpsItem = new ScenarioAction(
 "sdkUpdateOpsItem",
 async (/** @type {State} */ state) => {
 try {

```

```
const _response = await state.ssmClient.send(
 new UpdateOpsItemCommand({
 OpsItemId: state.opsItemId,
 Description: `An update to ${state.opsItemId}`,
 }),
);
} catch (caught) {
 console.error(caught.message);
 console.log(
 `An error occurred while updating the ops item. Please fix the error and
 try again. Error message: ${caught.message}`,
);
 throw caught;
}
},
);

const getOpsItemStatus = new ScenarioOutput(
 "getOpsItemStatus",
 (/** @type {State} */ state) =>
 `Now we will get the status of the OpsItem: ${state.opsItemId}`,
);

const sdkOpsItemStatus = new ScenarioAction(
 "sdkGetOpsItemStatus",
 async (/** @type {State} */ state) => {
 try {
 const response = await state.ssmClient.send(
 new DescribeOpsItemsCommand({
 OpsItemId: state.opsItemId,
 }),
);
 state.opsItemStatus = response.OpsItemStatus;
 } catch (caught) {
 console.error(caught.message);
 console.log(
 `An error occurred while describing the ops item. Please fix the error
 and try again. Error message: ${caught.message}`,
);
 throw caught;
 }
 },
);
```

```
const resolveOpsItem = new ScenarioOutput(
 "resolveOpsItem",
 (/** @type {State} */ state) =>
 `Now we will resolve the OpsItem: ${state.opsItemId}`,
);

const sdkResolveOpsItem = new ScenarioAction(
 "sdkResolveOpsItem",
 async (/** @type {State} */ state) => {
 try {
 const _response = await state.ssmClient.send(
 new UpdateOpsItemCommand({
 OpsItemId: state.opsItemId,
 Status: OpsItemStatus.RESOLVED,
 }),
);
 } catch (caught) {
 console.error(caught.message);
 console.log(
 `An error occurred while updating the ops item. Please fix the error and try again. Error message: ${caught.message}`,
);
 throw caught;
 }
 },
);

const askToDeleteResources = new ScenarioInput(
 "askToDeleteResources",
 "Would you like to delete the Systems Manager resources created during this example run?",
 { type: "confirm" },
);

const confirmDeleteChoice = new ScenarioOutput(
 "confirmDeleteChoice",
 (/** @type {State} */ state) => {
 if (state.askToDeleteResources) {
 return "You chose to delete the resources.";
 }
 return "The Systems Manager resources will not be deleted. Please delete them manually to avoid charges.";
 },
);
```

```
export const sdkDeleteResources = new ScenarioAction(
 "sdkDeleteResources",
 async (** @type {State} */ state) => {
 try {
 await state.ssmClient.send(
 new DeleteOpsItemCommand({
 OpsItemId: state.opsItemId,
 }),
);
 console.log(`The ops item: ${state.opsItemId} was successfully deleted.`);
 } catch (caught) {
 console.log(
 `There was a problem deleting the ops item: ${state.opsItemId}. Please delete it manually. Error: ${caught.message}`,
);
 }

 try {
 await state.ssmClient.send(
 new DeleteMaintenanceWindowCommand({
 Name: state.maintenanceWindow,
 WindowId: state.winId,
 }),
);
 console.log(
 `The maintenance window: ${state.maintenanceWindow} was successfully deleted.`,
);
 } catch (caught) {
 console.log(
 `There was a problem deleting the maintenance window: ${state.opsItemId}. Please delete it manually. Error: ${caught.message}`,
);
 }

 try {
 await state.ssmClient.send(
 new DeleteDocumentCommand({
 Name: state.documentName,
 }),
);
 console.log(
 `The document: ${state.documentName} was successfully deleted.`,
);
 }
 },
);
```



```
);
 } catch (caught) {
 console.log(
 `There was a problem deleting the document: ${state.documentName}. Please
delete it manually. Error: ${caught.message}`,
);
 }
},
{ skipWhen: (/** @type {} */ state) => !state.askToDeleteResources },
);

const goodbye = new ScenarioOutput(
 "goodbye",
 "This concludes the Systems Manager Basics scenario for the AWS Javascript SDK
v3. Thank you!",
);

const myScenario = new Scenario(
 "SSM Basics",
 [
 greet,
 pressEnter,
 createMaintenanceWindow,
 getMaintenanceWindow,
 sdkCreateMaintenanceWindow,
 modifyMaintenanceWindow,
 pressEnter,
 sdkModifyMaintenanceWindow,
 createSystemsManagerActions,
 getDocumentName,
 sdkCreateSSMDoc,
 ec2HelloWorld,
 enterIdOrSkipEC2HelloWorld,
 sdkEC2HelloWorld,
 sdkGetCommandTime,
 pressEnter,
 createSSMOpsItem,
 pressEnter,
 sdkCreateSSMOpsItem,
 updateOpsItem,
 pressEnter,
 sdkUpdateOpsItem,
 getOpsItemStatus,
 pressEnter,
```

```
 sdkOpsItemStatus,
 resolveOpsItem,
 pressEnter,
 sdkResolveOpsItem,
 askToDeleteResources,
 confirmDeleteChoice,
 sdkDeleteResources,
 goodbye,
],
 { ssmClient: new SSMClient({}) },
);

/** @type {{ stepHandlerOptions: StepHandlerOptions }} */
export const main = async (stepHandlerOptions) => {
 await myScenario.run(stepHandlerOptions);
};

// Invoke main function if this file was run directly.
if (process.argv[1] === fileURLToPath(import.meta.url)) {
 const { values } = parseArgs({
 options: {
 yes: {
 type: "boolean",
 short: "y",
 },
 },
 });
 main({ confirmAll: values.yes });
}
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella documentazione di riferimento dell'API AWS SDK per JavaScript .
  - [CreateDocument](#)
  - [CreateMaintenanceWindow](#)
  - [CreateOpsItem](#)
  - [DeleteMaintenanceWindow](#)
  - [ListCommandInvocations](#)
  - [SendCommand](#)
  - [UpdateOpsItem](#)

## Python

### SDK per Python (Boto3)

#### Note

C'è dell'altro GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

Esegui uno scenario interattivo al prompt dei comandi.

```
class SystemsManagerScenario:
 """Runs an interactive scenario that shows how to get started using Amazon
 Systems Manager."""

 def __init__(self, document_wrapper, maintenance_window_wrapper,
ops_item_wrapper):
 """
 :param document_wrapper: An object that wraps Systems Manager document
 functions.
 :param maintenance_window_wrapper: An object that wraps Systems Manager
 maintenance window functions.
 :param ops_item_wrapper: An object that wraps Systems Manager OpsItem
 functions.
 """
 self.document_wrapper = document_wrapper
 self.maintenance_window_wrapper = maintenance_window_wrapper
 self.ops_item_wrapper = ops_item_wrapper

 def run(self):
 """Demonstrates how to use the AWS SDK for Python (Boto3) to get started
 with Systems Manager."""
 try:
 print("-" * 88)
 print(
 """
Welcome to the AWS Systems Manager SDK Getting Started scenario.
This program demonstrates how to interact with Systems Manager using the AWS SDK
for Python (Boto3).
Systems Manager is the operations hub for your AWS applications and resources and
a secure end-to-end management
```

solution. The program's primary functions include creating a maintenance window, creating a document, sending a command to a document, listing documents, listing commands, creating an OpsItem, modifying an OpsItem, and deleting Systems Manager resources. Upon completion of the program, all AWS resources are cleaned up.

Let's get started..."

```

)
 q.ask("Please hit Enter")

 print("-" * 88)
 print("Create a Systems Manager maintenance window.")
 maintenance_window_name = q.ask(
 "Please enter the maintenance window name (default is ssm-
maintenance-window):",
)
 if not maintenance_window_name:
 maintenance_window_name = "ssm-maintenance-window"

 self.maintenance_window_wrapper.create(
 name=maintenance_window_name,
 schedule="cron(0 10 ? * MON-FRI *)",
 duration=2,
 cutoff=1,
 allow_unassociated_targets=True,
)

 print("-" * 88)
 print("Modify the maintenance window by changing the schedule")
 q.ask("Please hit Enter")

 self.maintenance_window_wrapper.update(
 name=maintenance_window_name,
 schedule="cron(0 0 ? * MON *)",
 duration=24,
 cutoff=1,
 allow_unassociated_targets=True,
 enabled=True,
)

 print("-" * 88)
 print(
 "Create a document that defines the actions that Systems Manager
performs on your EC2 instance."

```

```

)
 document_name = q.ask(
 "Please enter the document name (default is ssmdocument):"
)

 if not document_name:
 document_name = "ssmdocument"

 self.document_wrapper.create(
 name=document_name,
 content="""
{
 "schemaVersion": "2.2",
 "description": "Run a simple shell command",
 "mainSteps": [
 {
 "action": "aws:runShellScript",
 "name": "runEchoCommand",
 "inputs": {
 "runCommand": [
 "echo 'Hello, world!'"
]
 }
 }
]
}
 """,
)

 self.document_wrapper.wait_until_active()

 print(
 """

```

Now you have the option of running a command on an EC2 instance that echoes 'Hello, world!'.

In order to run this command, you must provide the instance ID of a Linux EC2 instance. If you do

not already have a running Linux EC2 instance in your account, you can create one using the AWS console.

For information about creating an EC2 instance, see

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-launch-instance-wizard.html>.

```

 """,
)

```

```

 if q.ask(
 "Would you like to run a command on an EC2 instance? (y/n)",
 q.is_yesno,
):
 instance_id = q.ask(
 "Please enter the instance ID of the EC2 instance:",
 q.non_empty
)
 command_id = self.document_wrapper.send_command(
 instance_ids=[instance_id]
)

 self.document_wrapper.wait_command_executed(
 command_id=command_id, instance_id=instance_id
)

 print("-" * 88)
 print(
 "Lets get the time when the specific command was sent to the
specific managed node"
)
 q.ask("Please hit Enter")

self.document_wrapper.list_command_invocations(instance_id=instance_id)

 print("-" * 88)
 print("-" * 88)
 print(
 """
Now we will create a Systems Manager OpsItem.
An OpsItem is a feature provided by the Systems Manager service.
It is a type of operational data item that allows you to manage and track various
operational issues,
events, or tasks within your AWS environment.

You can create OpsItems to track and manage operational issues as they arise.
For example, you could create an OpsItem whenever your application detects a
critical error
or an anomaly in your infrastructure.
 """
)
 q.ask("Please hit Enter")

```

```
self.ops_item_wrapper.create(
 title="Disk Space Alert",
 description="Created by the Systems Manager Python (Boto3) API",
 source="EC2",
 category="Performance",
 severity="2",
)

print("-" * 88)
print("-" * 88)
print(f"Now we will update the OpsItem {self.ops_item_wrapper.id}")
q.ask("Please hit Enter")

self.ops_item_wrapper.update(
 title="Disk Space Alert",
 description=f"An update to {self.ops_item_wrapper.id}",
)

print(
 f"Now we will get the status of the OpsItem {self.ops_item_wrapper.id}"
)
q.ask("Please hit Enter")

It may take a second for the ops item to be available
counter = 0
while not self.ops_item_wrapper.describe() and counter < 5:
 counter += 1
 time.sleep(1)

print(f"Now we will resolve the OpsItem {self.ops_item_wrapper.id}")
q.ask("Please hit Enter")

self.ops_item_wrapper.update(status="Resolved")

print("-" * 88)
print("-" * 88)
if q.ask(
 "Would you like to delete the Systems Manager resources? (y/n)",
 q.is_yesno,
):
 print("You selected to delete the resources.")
 self.cleanup()
```

```

 else:
 print("The Systems Manager resources will not be deleted")

 print("-" * 88)
 print("This concludes the Systems Manager SDK Getting Started
scenario.")
 print("-" * 88)

 except Exception:
 self.cleanup()
 raise

 def cleanup(self):
 self.maintenance_window_wrapper.delete()
 self.ops_item_wrapper.delete()
 self.document_wrapper.delete()

if __name__ == "__main__":
 try:
 scenario = SystemsManagerScenario(
 DocumentWrapper.from_client(),
 MaintenanceWindowWrapper.from_client(),
 OpsItemWrapper.from_client(),
)
 scenario.run()
 except Exception:
 logging.exception("Something went wrong with the demo.")

```

Definisci una classe wrapper per le operazioni di documenti e comandi.

```

class DocumentWrapper:
 """Encapsulates AWS Systems Manager Document actions."""

 def __init__(self, ssm_client):
 """
 :param ssm_client: A Boto3 Systems Manager client.
 """
 self.ssm_client = ssm_client
 self.name = None

 @classmethod

```



```
def from_client(cls):
 ssm_client = boto3.client("ssm")
 return cls(ssm_client)

def create(self, content, name):
 """
 Creates a document.

 :param content: The content of the document.
 :param name: The name of the document.
 """
 try:
 self.ssm_client.create_document(
 Name=name, Content=content, DocumentType="Command"
)
 self.name = name
 except self.ssm_client.exceptions.DocumentAlreadyExists:
 print(f"Document {name} already exists.")
 self.name = name
 except ClientError as err:
 logger.error(
 "Couldn't create %s. Here's why: %s: %s",
 name,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise

def delete(self):
 """
 Deletes an AWS Systems Manager document.
 """
 if self.name is None:
 return

 try:
 self.ssm_client.delete_document(Name=self.name)
 print(f"Deleted document {self.name}.")
 self.name = None
 except ClientError as err:
 logger.error(
 "Couldn't delete %s. Here's why: %s: %s",
```

```

 self.name,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise

def send_command(self, instance_ids):
 """
 Sends a command to one or more instances.

 :param instance_ids: The IDs of the instances to send the command to.
 :return: The ID of the command.
 """
 try:
 response = self.ssm_client.send_command(
 InstanceIds=instance_ids, DocumentName=self.name,
TimeoutSeconds=3600
)
 return response["Command"]["CommandId"]
 except ClientError as err:
 logger.error(
 "Couldn't send command to %s. Here's why: %s: %s",
 self.name,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise

def describe(self):
 """
 Describes the document.

 :return: Document status.
 """
 try:
 response = self.ssm_client.describe_document(Name=self.name)
 return response["Document"]["Status"]
 except ClientError as err:
 logger.error(
 "Couldn't get %s. Here's why: %s: %s",
 self.name,
 err.response["Error"]["Code"],

```

```
 err.response["Error"]["Message"],
)
 raise

def wait_until_active(self, max_attempts=20, delay=5):
 """
 Waits until the document is active.

 :param max_attempts: The maximum number of attempts for checking the
status.
 :param delay: The delay in seconds between each check.
 """
 attempt = 0
 status = ""
 while attempt <= max_attempts:
 status = self.describe()
 if status == "Active":
 break
 attempt += 1
 time.sleep(delay)

 if status != "Active":
 logger.error("Document is not active.")
 else:
 logger.info("Document is active.")

def wait_command_executed(self, command_id, instance_id):
 """
 Waits until the command is executed on the instance.

 :param command_id: The ID of the command.
 :param instance_id: The ID of the instance.
 """

 waiter = self.ssm_client.get_waiter("command_executed")
 waiter.wait(CommandId=command_id, InstanceId=instance_id)

def list_command_invocations(self, instance_id):
 """
 Lists the commands for an instance.

 :param instance_id: The ID of the instance.
 :return: The list of commands.
```

```

"""
try:
 paginator = self.ssm_client.get_paginator("list_command_invocations")
 command_invocations = []
 for page in paginator.paginate(InstanceId=instance_id):
 command_invocations.extend(page["CommandInvocations"])
 num_of_commands = len(command_invocations)
 print(
 f"{num_of_commands} command invocation(s) found for instance
{instance_id}."
)

 if num_of_commands > 10:
 print("Displaying the first 10 commands:")
 num_of_commands = 10
 date_format = "%A, %d %B %Y %I:%M%p"
 for command in command_invocations[:num_of_commands]:
 print(
 f" The time of command invocation is
{command['RequestedDateTime'].strftime(date_format)}"
)
except ClientError as err:
 logger.error(
 "Couldn't list commands for %s. Here's why: %s: %s",
 instance_id,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
raise

```

Definisci una classe wrapper per le operazioni sugli OpsItem.

```

class OpsItemWrapper:
 """Encapsulates AWS Systems Manager OpsItem actions."""

 def __init__(self, ssm_client):
 """
 :param ssm_client: A Boto3 Systems Manager client.
 """

```

```

 self.ssm_client = ssm_client
 self.id = None

 @classmethod
 def from_client(cls):
 """
 :return: A OpsItemWrapper instance.
 """
 ssm_client = boto3.client("ssm")
 return cls(ssm_client)

 def create(self, title, source, category, severity, description):
 """
 Create an OpsItem

 :param title: The OpsItem title.
 :param source: The OpsItem source.
 :param category: The OpsItem category.
 :param severity: The OpsItem severity.
 :param description: The OpsItem description.

 """
 try:
 response = self.ssm_client.create_ops_item(
 Title=title,
 Source=source,
 Category=category,
 Severity=severity,
 Description=description,
)
 self.id = response["OpsItemId"]
 except self.ssm_client.exceptions.OpsItemLimitExceededException as err:
 logger.error(
 "Couldn't create ops item because you have exceeded your open\nOpsItem limit. "
 "Here's why: %s: %s",
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise
 except ClientError as err:
 logger.error(
 "Couldn't create ops item %s. Here's why: %s: %s",

```

```

 title,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise

def delete(self):
 """
 Delete the OpsItem.
 """
 if self.id is None:
 return
 try:
 self.ssm_client.delete_ops_item(OpsItemId=self.id)
 print(f"Deleted ops item with id {self.id}")
 self.id = None
 except ClientError as err:
 logger.error(
 "Couldn't delete ops item %s. Here's why: %s: %s",
 self.id,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise

def describe(self):
 """
 Describe an OpsItem.
 """
 try:
 paginator = self.ssm_client.get_paginator("describe_ops_items")
 ops_items = []
 for page in paginator.paginate(
 OpsItemFilters=[
 {"Key": "OpsItemId", "Values": [self.id], "Operator":
"Equal"}
]
):
 ops_items.extend(page["OpsItemSummaries"])

 for item in ops_items:
 print(

```

```

 f"The item title is {item['Title']} and the status is
 {item['Status']}"
)
 return len(ops_items) > 0
except ClientError as err:
 logger.error(
 "Couldn't describe ops item %s. Here's why: %s: %s",
 self.id,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise

def update(self, title=None, description=None, status=None):
 """
 Update an OpsItem.

 :param title: The new OpsItem title.
 :param description: The new OpsItem description.
 :param status: The new OpsItem status.
 :return:
 """
 args = dict(OpsItemId=self.id)
 if title is not None:
 args["Title"] = title
 if description is not None:
 args["Description"] = description
 if status is not None:
 args["Status"] = status
 try:
 self.ssm_client.update_ops_item(**args)
 except ClientError as err:
 logger.error(
 "Couldn't update ops item %s. Here's why: %s: %s",
 self.id,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise

```

Definisci una classe wrapper per le operazioni della finestra di manutenzione.

```
class MaintenanceWindowWrapper:
 """Encapsulates AWS Systems Manager maintenance window actions."""

 def __init__(self, ssm_client):
 """
 :param ssm_client: A Boto3 Systems Manager client.
 """
 self.ssm_client = ssm_client
 self.window_id = None
 self.name = None

 @classmethod
 def from_client(cls):
 ssm_client = boto3.client("ssm")
 return cls(ssm_client)

 def create(self, name, schedule, duration, cutoff,
allow_unassociated_targets):
 """
 Create an AWS Systems Manager maintenance window.

 :param name: The name of the maintenance window.
 :param schedule: The schedule of the maintenance window.
 :param duration: The duration of the maintenance window.
 :param cutoff: The cutoff time of the maintenance window.
 :param allow_unassociated_targets: Allow the maintenance window to run on
managed nodes, even
 if you haven't registered those nodes
as targets.
 """
 try:
 response = self.ssm_client.create_maintenance_window(
 Name=name,
 Schedule=schedule,
 Duration=duration,
 Cutoff=cutoff,
 AllowUnassociatedTargets=allow_unassociated_targets,
)
```



```

 self.window_id = response["WindowId"]
 self.name = name
 logger.info("Created maintenance window %s.", self.window_id)
 except ParamValidationError as error:
 logger.error(
 "Parameter validation error when trying to create maintenance
window %s. Here's why: %s",
 self.window_id,
 error,
)
 raise
 except ClientError as err:
 logger.error(
 "Couldn't create maintenance window %s. Here's why: %s: %s",
 name,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise

def delete(self):
 """
 Delete the associated AWS Systems Manager maintenance window.
 """
 if self.window_id is None:
 return

 try:
 self.ssm_client.delete_maintenance_window(WindowId=self.window_id)
 logger.info("Deleted maintenance window %s.", self.window_id)
 print(f"Deleted maintenance window {self.name}")
 self.window_id = None
 except ClientError as err:
 logger.error(
 "Couldn't delete maintenance window %s. Here's why: %s: %s",
 self.window_id,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise

def update(

```

```

 self, name, enabled, schedule, duration, cutoff,
 allow_unassociated_targets
):
 """
 Update an AWS Systems Manager maintenance window.

 :param name: The name of the maintenance window.
 :param enabled: Whether the maintenance window is enabled to run on
 managed nodes.
 :param schedule: The schedule of the maintenance window.
 :param duration: The duration of the maintenance window.
 :param cutoff: The cutoff time of the maintenance window.
 :param allow_unassociated_targets: Allow the maintenance window to run on
 managed nodes, even
 if you haven't registered those nodes
 as targets.
 """
 try:
 self.ssm_client.update_maintenance_window(
 WindowId=self.window_id,
 Name=name,
 Enabled=enabled,
 Schedule=schedule,
 Duration=duration,
 Cutoff=cutoff,
 AllowUnassociatedTargets=allow_unassociated_targets,
)
 self.name = name
 logger.info("Updated maintenance window %s.", self.window_id)
 except ParamValidationError as error:
 logger.error(
 "Parameter validation error when trying to update maintenance
 window %s. Here's why: %s",
 self.window_id,
 error,
)
 raise
 except ClientError as err:
 logger.error(
 "Couldn't update maintenance window %s. Here's why: %s: %s",
 self.name,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)

```

```
raise
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento API SDK AWS per Python (Boto3).
  - [CreateDocument](#)
  - [CreateMaintenanceWindow](#)
  - [CreateOpsItem](#)
  - [DeleteMaintenanceWindow](#)
  - [ListCommandInvocations](#)
  - [SendCommand](#)
  - [UpdateOpsItem](#)

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [l'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Azioni per Systems Manager utilizzando AWS SDK

I seguenti esempi di codice dimostrano come eseguire singole azioni di Systems Manager con gli AWS SDK. Ogni esempio include un collegamento a GitHub, dove è possibile trovare le istruzioni per l'impostazione e l'esecuzione del codice.

Questi estratti chiamano l'API di Systems Manager e sono estratti di codice di programmi più grandi che devono essere eseguiti nel contesto. È possibile visualizzare le azioni nel contesto in [Scenari per l'utilizzo di Systems Manager AWS SDK](#).

Gli esempi seguenti includono solo le azioni più comunemente utilizzate. Per un elenco completo, consulta la [documentazione di riferimento dell'API AWS Systems Manager](#).

### Esempi

- [Utilizzo di AddTagsToResource con una CLI](#)
- [Utilizzo di CancelCommand con una CLI](#)
- [Utilizzo di CreateActivation con una CLI](#)
- [Utilizzo di CreateAssociation con una CLI](#)

- [Utilizzo di CreateAssociationBatch con una CLI](#)
- [Usare CreateDocument con un AWS SDK o CLI](#)
- [Usare CreateMaintenanceWindow con un AWS SDK o CLI](#)
- [Usare CreateOpsItem con un AWS SDK o CLI](#)
- [Utilizzo di CreatePatchBaseline con una CLI](#)
- [Utilizzo di DeleteActivation con una CLI](#)
- [Utilizzo di DeleteAssociation con una CLI](#)
- [Usare DeleteDocument con un AWS SDK o CLI](#)
- [Usare DeleteMaintenanceWindow con un AWS SDK o CLI](#)
- [Usare DeleteOpsItem con un AWS SDK](#)
- [Utilizzo di DeleteParameter con una CLI](#)
- [Utilizzo di DeletePatchBaseline con una CLI](#)
- [Utilizzo di DeregisterManagedInstance con una CLI](#)
- [Utilizzo di DeregisterPatchBaselineForPatchGroup con una CLI](#)
- [Utilizzo di DeregisterTargetFromMaintenanceWindow con una CLI](#)
- [Utilizzo di DeregisterTaskFromMaintenanceWindow con una CLI](#)
- [Utilizzo di DescribeActivations con una CLI](#)
- [Utilizzo di DescribeAssociation con una CLI](#)
- [Utilizzo di DescribeAssociationExecutionTargets con una CLI](#)
- [Utilizzo di DescribeAssociationExecutions con una CLI](#)
- [Utilizzo di DescribeAutomationExecutions con una CLI](#)
- [Utilizzo di DescribeAutomationStepExecutions con una CLI](#)
- [Utilizzo di DescribeAvailablePatches con una CLI](#)
- [Usare DescribeDocument con un AWS SDK o CLI](#)
- [Utilizzo di DescribeDocumentPermission con una CLI](#)
- [Utilizzo di DescribeEffectiveInstanceAssociations con una CLI](#)
- [Utilizzo di DescribeEffectivePatchesForPatchBaseline con una CLI](#)
- [Utilizzo di DescribeInstanceAssociationsStatus con una CLI](#)
- [Utilizzo di DescribeInstanceInformation con una CLI](#)
- [Utilizzo di DescribeInstancePatchStates con una CLI](#)

- [Utilizzo di DescribeInstancePatchStatesForPatchGroup con una CLI](#)
- [Utilizzo di DescribeInstancePatches con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindowExecutionTaskInvocations con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindowExecutionTasks con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindowExecutions con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindowTargets con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindowTasks con una CLI](#)
- [Utilizzo di DescribeMaintenanceWindows con una CLI](#)
- [Usare DescribeOpsItems con un AWS SDK o CLI](#)
- [Usare DescribeParameters con un AWS SDK o CLI](#)
- [Utilizzo di DescribePatchBaselines con una CLI](#)
- [Utilizzo di DescribePatchGroupState con una CLI](#)
- [Utilizzo di DescribePatchGroups con una CLI](#)
- [Utilizzo di GetAutomationExecution con una CLI](#)
- [Utilizzo di GetCommandInvocation con una CLI](#)
- [Utilizzo di GetConnectionStatus con una CLI](#)
- [Utilizzo di GetDefaultPatchBaseline con una CLI](#)
- [Utilizzo di GetDeployablePatchSnapshotForInstance con una CLI](#)
- [Utilizzo di GetDocument con una CLI](#)
- [Utilizzo di GetInventory con una CLI](#)
- [Utilizzo di GetInventorySchema con una CLI](#)
- [Utilizzo di GetMaintenanceWindow con una CLI](#)
- [Utilizzo di GetMaintenanceWindowExecution con una CLI](#)
- [Utilizzo di GetMaintenanceWindowExecutionTask con una CLI](#)
- [Usare GetParameter con un AWS SDK o CLI](#)
- [Utilizzo di GetParameterHistory con una CLI](#)
- [Utilizzo di GetParameters con una CLI](#)
- [Utilizzo di GetPatchBaseline con una CLI](#)
- [Utilizzo di GetPatchBaselineForPatchGroup con una CLI](#)
- [Utilizzo di ListAssociationVersions con una CLI](#)

- [Utilizzo di ListAssociations con una CLI](#)
- [Usare ListCommandInvocations con un AWS SDK o CLI](#)
- [Utilizzo di ListCommands con una CLI](#)
- [Utilizzo di ListComplianceItems con una CLI](#)
- [Utilizzo di ListComplianceSummaries con una CLI](#)
- [Utilizzo di ListDocumentVersions con una CLI](#)
- [Utilizzo di ListDocuments con una CLI](#)
- [Utilizzo di ListInventoryEntries con una CLI](#)
- [Utilizzo di ListResourceComplianceSummaries con una CLI](#)
- [Utilizzo di ListTagsForResource con una CLI](#)
- [Utilizzo di ModifyDocumentPermission con una CLI](#)
- [Utilizzo di PutComplianceItems con una CLI](#)
- [Utilizzo di PutInventory con una CLI](#)
- [Usare PutParameter con un AWS SDK o CLI](#)
- [Utilizzo di RegisterDefaultPatchBaseline con una CLI](#)
- [Utilizzo di RegisterPatchBaselineForPatchGroup con una CLI](#)
- [Utilizzo di RegisterTargetWithMaintenanceWindow con una CLI](#)
- [Utilizzo di RegisterTaskWithMaintenanceWindow con una CLI](#)
- [Utilizzo di RemoveTagsFromResource con una CLI](#)
- [Usare SendCommand con un AWS SDK o CLI](#)
- [Utilizzo di StartAutomationExecution con una CLI](#)
- [Utilizzo di StartSession con una CLI](#)
- [Utilizzo di StopAutomationExecution con una CLI](#)
- [Utilizzo di UpdateAssociation con una CLI](#)
- [Utilizzo di UpdateAssociationStatus con una CLI](#)
- [Utilizzo di UpdateDocument con una CLI](#)
- [Utilizzo di UpdateDocumentDefaultVersion con una CLI](#)
- [Usare UpdateMaintenanceWindow con un AWS SDK o CLI](#)
- [Utilizzo di UpdateManagedInstanceRole con una CLI](#)
- [Usare UpdateOpsItem con un AWS SDK o CLI](#)

- [Utilizzo di UpdatePatchBaseline con una CLI](#)

## Utilizzo di **AddTagsToResource** con una CLI

I seguenti esempi di codice mostrano come usare **AddTagsToResource**.

### CLI

#### AWS CLI

Esempio 1: per aggiungere tag a una finestra di manutenzione

L'esempio seguente `add-tags-to-resource` aggiunge un tag alla finestra di manutenzione specificata.

```
aws ssm add-tags-to-resource \
 --resource-type "MaintenanceWindow" \
 --resource-id "mw-03eb9db428EXAMPLE" \
 --tags "Key=Stack,Value=Production"
```

Questo comando non produce alcun output.

Esempio 2: come aggiungere tag a un parametro

L'esempio seguente `add-tags-to-resource` aggiunge due tag al parametro specificato.

```
aws ssm add-tags-to-resource \
 --resource-type "Parameter" \
 --resource-id "My-Parameter" \
 --tags '[{"Key":"Region","Value":"East"}, {"Key":"Environment",
 "Value":"Production"}]'
```

Questo comando non produce alcun output.

Esempio 3: come aggiungere tag a un documento SSM

L'esempio seguente `add-tags-to-resource` aggiunge un tag al documento specificato.

```
aws ssm add-tags-to-resource \
 --resource-type "Document" \
 --resource-id "My-Document" \
 --tags "Key=Quarter,Value=Q322"
```

Questo comando non produce alcun output.

Per ulteriori informazioni, consulta [Applicazione di tag alle risorse di Systems Manager](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [AddTagsToResource](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio aggiorna una finestra di manutenzione con nuovi tag. Se il comando va a buon fine, non viene generato output. La sintassi utilizzata da questo esempio richiede la PowerShell versione 3 o successiva.

```
$option1 = @{{Key="Stack";Value=@("Production")}}
Add-SSMResourceTag -ResourceId "mw-03eb9db42890fb82d" -ResourceType
"MaintenanceWindow" -Tag $option1
```

Esempio 2: con PowerShell la versione 2, è necessario utilizzare New-Object per creare ogni tag. Se il comando va a buon fine, non viene generato output.

```
$tag1 = New-Object Amazon.SimpleSystemsManagement.Model.Tag
$tag1.Key = "Stack"
$tag1.Value = "Production"

Add-SSMResourceTag -ResourceId "mw-03eb9db42890fb82d" -ResourceType
"MaintenanceWindow" -Tag $tag1
```

- Per i dettagli sull'API, vedere [AddTagsToResource](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio aggiorna una finestra di manutenzione con nuovi tag. Se il comando va a buon fine, non viene generato output. La sintassi utilizzata da questo esempio richiede la PowerShell versione 3 o successiva.

```
$option1 = @{{Key="Stack";Value=@("Production")}}
Add-SSMResourceTag -ResourceId "mw-03eb9db42890fb82d" -ResourceType
"MaintenanceWindow" -Tag $option1
```



Esempio 2: con PowerShell la versione 2, è necessario utilizzare New-Object per creare ogni tag. Se il comando va a buon fine, non viene generato output.

```
$tag1 = New-Object Amazon.SimpleSystemsManagement.Model.Tag
$tag1.Key = "Stack"
$tag1.Value = "Production"

Add-SSMResourceTag -ResourceId "mw-03eb9db42890fb82d" -ResourceType
 "MaintenanceWindow" -Tag $tag1
```

- Per i dettagli sull'API, vedere [AddTagsToResource](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **CancelCommand** con una CLI

I seguenti esempi di codice mostrano come usare **CancelCommand**.

### CLI

#### AWS CLI

Esempio 1: per annullare un comando per tutte le istanze

L'esempio seguente **cancel-command** tenta di annullare il comando specificato che è già in esecuzione per tutte le istanze.

```
aws ssm cancel-command \
 --command-id "662add3d-5831-4a10-b64a-f2ff3EXAMPLE"
```

Questo comando non produce alcun output.

Esempio 2: come annullare un comando per istanze specifiche

L'esempio seguente **cancel-command** tenta di annullare un comando solo per l'istanza specificata.

```
aws ssm cancel-command \
```

```
--command-id "662add3d-5831-4a10-b64a-f2ff3EXAMPLE"
--instance-ids "i-02573cafcfEXAMPLE"
```

Questo comando non produce alcun output.

Per ulteriori informazioni, consulta [Applicazione di tag a parametri di Systems Manager](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [CancelCommand](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio tenta di annullare un comando. Se l'operazione va a buon fine, non viene generato output.

```
Stop-SSMCommand -CommandId "9ded293e-e792-4440-8e3e-7b8ec5feaa38"
```

- Per i dettagli sull'API, vedere [CancelCommand](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio tenta di annullare un comando. Se l'operazione va a buon fine, non viene generato output.

```
Stop-SSMCommand -CommandId "9ded293e-e792-4440-8e3e-7b8ec5feaa38"
```

- Per i dettagli sull'API, vedere [CancelCommand](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **CreateActivation** con una CLI

I seguenti esempi di codice mostrano come usare `CreateActivation`.

## CLI

### AWS CLI

Per creare un'attivazione di un'istanza gestita

L'esempio seguente `create-activation` crea un'attivazione gestita dell'istanza.

```
aws ssm create-activation \
 --default-instance-name "HybridWebServers" \
 --iam-role "HybridWebServersRole" \
 --registration-limit 5
```

Output:

```
{
 "ActivationId": "5743558d-563b-4457-8682-d16c3EXAMPLE",
 "ActivationCode": "dRmgnYaFv567vEXAMPLE"
}
```

Per ulteriori informazioni, vedere la [Fase 4: Creazione di un' Managed-Instance attivazione per un ambiente ibrido](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [CreateActivation](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio crea un'istanza gestita.

```
New-SSMAutomation -DefaultInstanceName "MyWebServers" -IamRole
 "SSMAutomationRole" -RegistrationLimit 10
```

Output:

ActivationCode	ActivationId
-----	-----
KWChh0xBTiwDcKE9B1KC	08e51e79-1e36-446c-8e63-9458569c1363

- Per i dettagli sull'API, vedere [CreateActivation](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio crea un'istanza gestita.

```
New-SSMActivation -DefaultInstanceName "MyWebServers" -IamRole
"SSMAutomationRole" -RegistrationLimit 10
```

Output:

```
ActivationCode ActivationId

KWChh0xBTiwDcKE9BlKC 08e51e79-1e36-446c-8e63-9458569c1363
```

- Per i dettagli sull'API, vedere [CreateActivation](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **CreateAssociation** con una CLI

I seguenti esempi di codice mostrano come usare `CreateAssociation`.

### CLI

#### AWS CLI

Esempio 1: per associare un documento utilizzando gli ID di istanza

Questo esempio associa un documento di configurazione a un'istanza, utilizzando gli ID delle istanze.

```
aws ssm create-association \
 --instance-id "i-0cb2b964d3e14fd9f" \
 --name "AWS-UpdateSSMAgent"
```

Output:

```
{
 "AssociationDescription": {
```

```

 "Status": {
 "Date": 1487875500.33,
 "Message": "Associated with AWS-UpdateSSMAgent",
 "Name": "Associated"
 },
 "Name": "AWS-UpdateSSMAgent",
 "InstanceId": "i-0cb2b964d3e14fd9f",
 "Overview": {
 "Status": "Pending",
 "DetailedStatus": "Creating"
 },
 "AssociationId": "b7c3266e-a544-44db-877e-b20d3a108189",
 "DocumentVersion": "$DEFAULT",
 "LastUpdateAssociationDate": 1487875500.33,
 "Date": 1487875500.33,
 "Targets": [
 {
 "Values": [
 "i-0cb2b964d3e14fd9f"
],
 "Key": "InstanceIds"
 }
]
 }
}

```

Per ulteriori informazioni, consulta [CreateAssociation](#) la sezione AWS Systems Manager API Reference.

Esempio 2: come associare un documento utilizzando destinazioni

Questo esempio associa un documento di configurazione a un'istanza, utilizzando destinazioni.

```

aws ssm create-association \
 --name "AWS-UpdateSSMAgent" \
 --targets "Key=instanceids,Values=i-0cb2b964d3e14fd9f"

```

Output:

```

{
 "AssociationDescription": {

```

```

 "Status": {
 "Date": 1487875500.33,
 "Message": "Associated with AWS-UpdateSSMAgent",
 "Name": "Associated"
 },
 "Name": "AWS-UpdateSSMAgent",
 "InstanceId": "i-0cb2b964d3e14fd9f",
 "Overview": {
 "Status": "Pending",
 "DetailedStatus": "Creating"
 },
 "AssociationId": "b7c3266e-a544-44db-877e-b20d3a108189",
 "DocumentVersion": "$DEFAULT",
 "LastUpdateAssociationDate": 1487875500.33,
 "Date": 1487875500.33,
 "Targets": [
 {
 "Values": [
 "i-0cb2b964d3e14fd9f"
],
 "Key": "InstanceIds"
 }
]
 }
}

```

Per ulteriori informazioni, vedere [CreateAssociation](#) nella Guida di riferimento alle API di AWS Systems Manager.

Esempio 3: come creare un'associazione che viene eseguita una sola volta

Questo esempio crea una nuova associazione che viene eseguita solo una volta nella data e ora specificate. Le associazioni create con una data passata o presente (nel momento in cui viene elaborata la data è passata) vengono eseguite immediatamente.

```

aws ssm create-association \
 --name "AWS-UpdateSSMAgent" \
 --targets "Key=instanceids,Values=i-0cb2b964d3e14fd9f" \
 --schedule-expression "at(2020-05-14T15:55:00)" \
 --apply-only-at-cron-interval

```

Output:

```
{
 "AssociationDescription": {
 "Status": {
 "Date": 1487875500.33,
 "Message": "Associated with AWS-UpdateSSMAgent",
 "Name": "Associated"
 },
 "Name": "AWS-UpdateSSMAgent",
 "InstanceId": "i-0cb2b964d3e14fd9f",
 "Overview": {
 "Status": "Pending",
 "DetailedStatus": "Creating"
 },
 "AssociationId": "b7c3266e-a544-44db-877e-b20d3a108189",
 "DocumentVersion": "$DEFAULT",
 "LastUpdateAssociationDate": 1487875500.33,
 "Date": 1487875500.33,
 "Targets": [
 {
 "Values": [
 "i-0cb2b964d3e14fd9f"
],
 "Key": "InstanceIds"
 }
]
 }
}
```

Per ulteriori informazioni, vedere [CreateAssociation](#) la sezione Riferimento o [riferimento alle API di AWS Systems Manager: espressioni Cron and rate per Systems Manager](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [CreateAssociation](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio associa un documento di configurazione a un'istanza, utilizzando gli ID delle istanze.

```
New-SSMAssociation -InstanceId "i-0cb2b964d3e14fd9f" -Name "AWS-UpdateSSMAgent"
```

**Output:**

```

Name : AWS-UpdateSSMAgent
InstanceId : i-0000293ffd8c57862
Date : 2/23/2017 6:55:22 PM
Status.Name : Associated
Status.Date : 2/20/2015 8:31:11 AM
Status.Message : Associated with AWS-UpdateSSMAgent
Status.AdditionalInfo :

```

Esempio 2: questo esempio associa un documento di configurazione a un'istanza, utilizzando destinazioni.

```

$target = @{{Key="instanceids";Values=@("i-0cb2b964d3e14fd9f")}}
New-SSMAssociation -Name "AWS-UpdateSSMAgent" -Target $target

```

**Output:**

```

Name : AWS-UpdateSSMAgent
InstanceId :
Date : 3/1/2017 6:22:21 PM
Status.Name :
Status.Date :
Status.Message :
Status.AdditionalInfo :

```

Esempio 3: questo esempio associa un documento di configurazione a un'istanza, utilizzando destinazioni e parametri.

```

$target = @{{Key="instanceids";Values=@("i-0cb2b964d3e14fd9f")}}
$params = @{
 "action"="configure"
 "mode"="ec2"
 "optionalConfigurationSource"="ssm"
 "optionalConfigurationLocation"=""
 "optionalRestart"="yes"
}
New-SSMAssociation -Name "Configure-CloudWatch" -AssociationName
"CWConfiguration" -Target $target -Parameter $params

```

**Output:**



```

Name : Configure-CloudWatch
InstanceId :
Date : 5/17/2018 3:17:44 PM
Status.Name :
Status.Date :
Status.Message :
Status.AdditionalInfo :

```

Esempio 4: questo esempio crea un'associazione con tutte le istanze della regione, con **AWS-GatherSoftwareInventory**. Fornisce inoltre file personalizzati e posizioni di registro nei parametri da raccogliere

```

$params =
 [Collections.Generic.Dictionary[String,Collections.Generic.List[String]]]:new()
$params["windowsRegistry"] = '[{"Path":"HKEY_LOCAL_MACHINE\SOFTWARE\Amazon
\MachineImage","Recursive":false,"ValueNames":["AMIName"]}]'
$params["files"] = '[{"Path":"C:\Program Files","Pattern":
["*.exe"],"Recursive":true}, {"Path":"C:\ProgramData","Pattern":
["*.log"],"Recursive":true}]'
New-SSMAssociation -AssociationName new-in-mum -Name AWS-GatherSoftwareInventory
-Target @{Key="instanceids";Values="*"} -Parameter $params -region ap-south-1 -
ScheduleExpression "rate(720 minutes)"

```

Output:

```

Name : AWS-GatherSoftwareInventory
InstanceId :
Date : 6/9/2019 8:57:56 AM
Status.Name :
Status.Date :
Status.Message :
Status.AdditionalInfo :

```

- Per i dettagli sull'API, vedere [CreateAssociation](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio associa un documento di configurazione a un'istanza, utilizzando gli ID delle istanze.

```
New-SSMAssociation -InstanceId "i-0cb2b964d3e14fd9f" -Name "AWS-UpdateSSMAgent"
```

#### Output:

```
Name : AWS-UpdateSSMAgent
InstanceId : i-0000293ffd8c57862
Date : 2/23/2017 6:55:22 PM
Status.Name : Associated
Status.Date : 2/20/2015 8:31:11 AM
Status.Message : Associated with AWS-UpdateSSMAgent
Status.AdditionalInfo :
```

Esempio 2: questo esempio associa un documento di configurazione a un'istanza, utilizzando destinazioni.

```
$target = @{"Key"="instanceids";Values=@"i-0cb2b964d3e14fd9f"}
New-SSMAssociation -Name "AWS-UpdateSSMAgent" -Target $target
```

#### Output:

```
Name : AWS-UpdateSSMAgent
InstanceId :
Date : 3/1/2017 6:22:21 PM
Status.Name :
Status.Date :
Status.Message :
Status.AdditionalInfo :
```

Esempio 3: questo esempio associa un documento di configurazione a un'istanza, utilizzando destinazioni e parametri.

```
$target = @{"Key"="instanceids";Values=@"i-0cb2b964d3e14fd9f"}
$params = @{
 "action"="configure"
 "mode"="ec2"
 "optionalConfigurationSource"="ssm"
 "optionalConfigurationLocation"=""
 "optionalRestart"="yes"
}
```

```
New-SSMAssociation -Name "Configure-CloudWatch" -AssociationName
"CWConfiguration" -Target $target -Parameter $params
```

### Output:

```
Name : Configure-CloudWatch
InstanceId :
Date : 5/17/2018 3:17:44 PM
Status.Name :
Status.Date :
Status.Message :
Status.AdditionalInfo :
```

Esempio 4: questo esempio crea un'associazione con tutte le istanze della regione, con **AWS-GatherSoftwareInventory**. Fornisce inoltre file personalizzati e posizioni di registro nei parametri da raccogliere

```
$params =
[Collections.Generic.Dictionary[String,Collections.Generic.List[String]]::new()
$params["windowsRegistry"] = '[{"Path":"HKEY_LOCAL_MACHINE\SOFTWARE\Amazon
\MachineImage","Recursive":false,"ValueNames":["AMIName"]}]'
$params["files"] = '[{"Path":"C:\Program Files","Pattern":
["*.exe"],"Recursive":true}, {"Path":"C:\ProgramData","Pattern":
["*.log"],"Recursive":true}]'
New-SSMAssociation -AssociationName new-in-mum -Name AWS-GatherSoftwareInventory
-Target @{Key="instanceids";Values="*"} -Parameter $params -region ap-south-1 -
ScheduleExpression "rate(720 minutes)"
```

### Output:

```
Name : AWS-GatherSoftwareInventory
InstanceId :
Date : 6/9/2019 8:57:56 AM
Status.Name :
Status.Date :
Status.Message :
Status.AdditionalInfo :
```

- Per i dettagli sull'API, vedere [CreateAssociation](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **CreateAssociationBatch** con una CLI

I seguenti esempi di codice mostrano come usare `CreateAssociationBatch`.

### CLI

#### AWS CLI

Per creare più associazioni

Questo esempio associa un documento di configurazione a più istanze. L'output restituisce un elenco di operazioni riuscite e non riuscite, se applicabile.

Comando:

```
aws ssm create-association-batch --entries "Name=AWS-UpdateSSMAgent,InstanceId=i-1234567890abcdef0" "Name=AWS-UpdateSSMAgent,InstanceId=i-9876543210abcdef0"
```

Output:

```
{
 "Successful": [
 {
 "Name": "AWS-UpdateSSMAgent",
 "InstanceId": "i-1234567890abcdef0",
 "AssociationVersion": "1",
 "Date": 1550504725.007,
 "LastUpdateAssociationDate": 1550504725.007,
 "Status": {
 "Date": 1550504725.007,
 "Name": "Associated",
 "Message": "Associated with AWS-UpdateSSMAgent"
 },
 "Overview": {
 "Status": "Pending",
 "DetailedStatus": "Creating"
 },
 },
],
}
```

```

 "DocumentVersion": "$DEFAULT",
 "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
 "i-1234567890abcdef0"
]
 }
]
 },
 {
 "Name": "AWS-UpdateSSMAgent",
 "InstanceId": "i-9876543210abcdef0",
 "AssociationVersion": "1",
 "Date": 1550504725.057,
 "LastUpdateAssociationDate": 1550504725.057,
 "Status": {
 "Date": 1550504725.057,
 "Name": "Associated",
 "Message": "Associated with AWS-UpdateSSMAgent"
 },
 "Overview": {
 "Status": "Pending",
 "DetailedStatus": "Creating"
 },
 "DocumentVersion": "$DEFAULT",
 "AssociationId": "9c9f7f20-5154-4fed-a83e-0123456789ab",
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
 "i-9876543210abcdef0"
]
 }
]
 }
],
"Failed": []
}

```

- Per i dettagli sull'API, vedi [CreateAssociationBatch](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio associa un documento di configurazione a più istanze. L'output restituisce un elenco di operazioni riuscite e non riuscite, se applicabile.

```
$option1 = @{InstanceId="i-0cb2b964d3e14fd9f";Name=@"AWS-UpdateSSMAgent"}
$option2 = @{InstanceId="i-0000293ffd8c57862";Name=@"AWS-UpdateSSMAgent"}
New-SSMAssociationFromBatch -Entry $option1,$option2
```

Output:

```
Failed Successful

{} {Amazon.SimpleSystemsManagement.Model.FailedCreateAssociation,
Amazon.SimpleSystemsManagement.Model.FailedCreateAsso...
```

Esempio 2: questo esempio mostrerà tutti i dettagli di un'operazione riuscita.

```
$option1 = @{InstanceId="i-0cb2b964d3e14fd9f";Name=@"AWS-UpdateSSMAgent"}
$option2 = @{InstanceId="i-0000293ffd8c57862";Name=@"AWS-UpdateSSMAgent"}
(New-SSMAssociationFromBatch -Entry $option1,$option2).Successful
```

- Per i dettagli sull'API, vedere [CreateAssociationBatch](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio associa un documento di configurazione a più istanze. L'output restituisce un elenco di operazioni riuscite e non riuscite, se applicabile.

```
$option1 = @{InstanceId="i-0cb2b964d3e14fd9f";Name=@"AWS-UpdateSSMAgent"}
$option2 = @{InstanceId="i-0000293ffd8c57862";Name=@"AWS-UpdateSSMAgent"}
New-SSMAssociationFromBatch -Entry $option1,$option2
```

Output:

```
Failed Successful

{} {Amazon.SimpleSystemsManagement.Model.FailedCreateAssociation,
Amazon.SimpleSystemsManagement.Model.FailedCreateAsso...
```

Esempio 2: questo esempio mostrerà tutti i dettagli di un'operazione riuscita.

```
$option1 = @{"InstanceId"="i-0cb2b964d3e14fd9f";Name=@"AWS-UpdateSSMAgent"}
$option2 = @{"InstanceId"="i-0000293ffd8c57862";Name=@"AWS-UpdateSSMAgent"}
(New-SSMAssociationFromBatch -Entry $option1,$option2).Successful
```

- Per i dettagli sull'API, vedere [CreateAssociationBatch](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Usare **CreateDocument** con un AWS SDK o CLI

I seguenti esempi di codice mostrano come usare `CreateDocument`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- [Informazioni di base](#)

### CLI

#### AWS CLI

Come creare un documento

L'esempio seguente `create-document` crea un documento di Systems Manager.

```
aws ssm create-document \
 --content file://exampleDocument.yml \
 --name "Example" \
 --document-type "Automation" \
 --document-format YAML
```

Output:

```
{
```

```

 "DocumentDescription": {
 "Hash":
"fc2410281f40779e694a8b95975d0f9f316da8a153daa94e3d9921102EXAMPLE",
 "HashType": "Sha256",
 "Name": "Example",
 "Owner": "29884EXAMPLE",
 "CreateDate": 1583256349.452,
 "Status": "Creating",
 "DocumentVersion": "1",
 "Description": "Document Example",
 "Parameters": [
 {
 "Name": "AutomationAssumeRole",
 "Type": "String",
 "Description": "(Required) The ARN of the role that allows
Automation to perform the actions on your behalf. If no role is specified,
Systems Manager Automation uses your IAM permissions to execute this document.",
 "DefaultValue": ""
 },
 {
 "Name": "InstanceId",
 "Type": "String",
 "Description": "(Required) The ID of the Amazon EC2 instance.",
 "DefaultValue": ""
 }
],
 "PlatformTypes": [
 "Windows",
 "Linux"
],
 "DocumentType": "Automation",
 "SchemaVersion": "0.3",
 "LatestVersion": "1",
 "DefaultVersion": "1",
 "DocumentFormat": "YAML",
 "Tags": []
 }
 }
}

```

Per ulteriori informazioni, consulta [Creazione di documenti di Systems Manager](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [CreateDocument](#) in AWS CLI Command Reference.



## Java

### SDK per Java 2.x

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
/**
 * Creates an AWS SSM document asynchronously.
 *
 * @param docName The name of the document to create.
 * <p>
 * This method initiates an asynchronous request to create an SSM document.
 * If the request is successful, it prints the document status.
 * If an exception occurs, it handles the error appropriately.
 */
public void createSSMDoc(String docName) throws SsmException {
 String jsonData = ""
 {
 "schemaVersion": "2.2",
 "description": "Run a simple shell command",
 "mainSteps": [
 {
 "action": "aws:runShellScript",
 "name": "runEchoCommand",
 "inputs": {
 "runCommand": [
 "echo 'Hello, world!'"
]
 }
 }
]
 }
 """;

 CreateDocumentRequest request = CreateDocumentRequest.builder()
 .content(jsonData)
 .name(docName)
 .documentType(DocumentType.COMMAND)
```

```

 .build();

 CompletableFuture<CreateDocumentResponse> future =
getAsyncClient().createDocument(request);
 future.thenAccept(response -> {
 System.out.println("The status of the SSM document is " +
response.documentDescription().status());
 }).exceptionally(ex -> {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
 if (cause instanceof DocumentAlreadyExistsException) {
 throw new CompletionException(cause);
 } else if (cause instanceof SsmException) {
 throw new CompletionException(cause);
 } else {
 throw new RuntimeException(cause);
 }
 }).join();
 }
}

```

- Per i dettagli sulle API, consulta la [CreateDocument](#) sezione AWS SDK for Java 2.x API Reference.

## JavaScript

### SDK per JavaScript (v3)

#### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```

import { CreateDocumentCommand, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Create an SSM document.
 * @param {{ content: string, name: string, documentType?: DocumentType }}
 */

```

```
export const main = async ({ content, name, documentType }) => {
 const client = new SSMClient({});
 try {
 const { documentDescription } = await client.send(
 new CreateDocumentCommand({
 Content: content, // The content for the new SSM document. The content
 must not exceed 64KB.
 Name: name,
 DocumentType: documentType, // Document format type can be JSON, YAML, or
 TEXT. The default format is JSON.
 }),
);
 console.log("Document created successfully.");
 return { DocumentDescription: documentDescription };
 } catch (caught) {
 if (caught instanceof Error && caught.name === "DocumentAlreadyExists") {
 console.warn(`${caught.message}. Did you provide a new document name?`);
 } else {
 throw caught;
 }
 }
};
```

- Per i dettagli sulle API, consulta la [CreateDocument](#) sezione AWS SDK per JavaScript API Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio crea un documento nell'account. Il documento deve essere in formato JSON. Per ulteriori informazioni sulla scrittura di un documento di configurazione, consulta il Documento di configurazione nella Documentazione di riferimento API SSM.

```
New-SSMDocument -Content (Get-Content -Raw "c:\temp\RunShellScript.json") -Name
"RunShellScript" -DocumentType "Command"
```

Output:

```
CreatedDate : 3/1/2017 1:21:33 AM
DefaultVersion : 1
```

```

Description : Run an updated script
DocumentType : Command
DocumentVersion : 1
Hash :
 1d5ce820e999ff051eb4841ed887593daf77120fd76cae0d18a53cc42e4e22c1
HashType : Sha256
LatestVersion : 1
Name : RunShellScript
Owner : 809632081692
Parameters : {commands}
PlatformTypes : {Linux}
SchemaVersion : 2.0
Sha1 :
Status : Creating

```

- Per i dettagli sull'API, vedere [CreateDocument](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio crea un documento nell'account. Il documento deve essere in formato JSON. Per ulteriori informazioni sulla scrittura di un documento di configurazione, consulta il Documento di configurazione nella Documentazione di riferimento API SSM.

```

New-SSMDocument -Content (Get-Content -Raw "c:\temp\RunShellScript.json") -Name
"RunShellScript" -DocumentType "Command"

```

## Output:

```

CreatedDate : 3/1/2017 1:21:33 AM
DefaultVersion : 1
Description : Run an updated script
DocumentType : Command
DocumentVersion : 1
Hash :
 1d5ce820e999ff051eb4841ed887593daf77120fd76cae0d18a53cc42e4e22c1
HashType : Sha256
LatestVersion : 1
Name : RunShellScript
Owner : 809632081692
Parameters : {commands}
PlatformTypes : {Linux}
SchemaVersion : 2.0

```

```
Sha1 :
Status : Creating
```

- Per i dettagli sull'API, vedere [CreateDocument](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
class DocumentWrapper:
 """Encapsulates AWS Systems Manager Document actions."""

 def __init__(self, ssm_client):
 """
 :param ssm_client: A Boto3 Systems Manager client.
 """
 self.ssm_client = ssm_client
 self.name = None

 @classmethod
 def from_client(cls):
 ssm_client = boto3.client("ssm")
 return cls(ssm_client)

 def create(self, content, name):
 """
 Creates a document.

 :param content: The content of the document.
 :param name: The name of the document.
 """
 try:
 self.ssm_client.create_document(

```

```

 Name=name, Content=content, DocumentType="Command"
)
 self.name = name
except self.ssm_client.exceptions.DocumentAlreadyExists:
 print(f"Document {name} already exists.")
 self.name = name
except ClientError as err:
 logger.error(
 "Couldn't create %s. Here's why: %s: %s",
 name,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise

```

- Per i dettagli sulle API, vedi [CreateDocument](#) in AWS SDK for Python (Boto3) API Reference.

## SAP ABAP

### SDK per SAP ABAP

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```

TRY.
 lo_ssm->createdocument(
 iv_name = iv_name
 iv_content = iv_content
 iv_documenttype = 'Command').
 MESSAGE 'Document created.' TYPE 'I'.
CATCH /aws1/cx_ssmdocalreadyexists.
 MESSAGE 'Document already exists.' TYPE 'I'.
CATCH /aws1/cx_ssminvaliddoccontent.
 MESSAGE 'Invalid document content.' TYPE 'I'.
ENDTRY.

```

- Per i dettagli sulle API, consulta [CreateDocument](#) la sezione AWS SDK for SAP ABAP API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Usare **CreateMaintenanceWindow** con un AWS SDK o CLI

I seguenti esempi di codice mostrano come usare `CreateMaintenanceWindow`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- [Informazioni di base](#)

### CLI

#### AWS CLI

Esempio 1: come creare una finestra di manutenzione

L'esempio seguente `create-maintenance-window` crea una nuova finestra di manutenzione che ogni cinque minuti per un massimo di due ore (se necessario), impedisce l'avvio di nuove attività entro un'ora dalla fine dell'esecuzione della finestra di manutenzione, consente destinazioni non associate (istanze che non sono state registrate nella finestra di manutenzione) e indica, tramite l'uso di tag personalizzati, che il suo creatore intende utilizzarla in un tutorial.

```
aws ssm create-maintenance-window \
 --name "My-Tutorial-Maintenance-Window" \
 --schedule "rate(5 minutes)" \
 --duration 2 --cutoff 1 \
 --allow-unassociated-targets \
 --tags "Key=Purpose,Value=Tutorial"
```

Output:

```
{
 "WindowId": "mw-0c50858d01EXAMPLE"
}
```

Esempio 2: come creare una finestra di manutenzione che viene eseguita solo una volta

L'esempio seguente `create-maintenance-window` crea una nuova finestra di manutenzione che viene eseguita una sola volta nella data e all'ora specificate.

```
aws ssm create-maintenance-window \
 --name My-One-Time-Maintenance-Window \
 --schedule "at(2020-05-14T15:55:00)" \
 --duration 5 \
 --cutoff 2 \
 --allow-unassociated-targets \
 --tags "Key=Environment,Value=Production"
```

Output:

```
{
 "WindowId": "mw-01234567890abcdef"
}
```

Per ulteriori informazioni, consulta [Finestre di manutenzione](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [CreateMaintenanceWindow](#) in AWS CLI Command Reference.

## Java

### SDK per Java 2.x

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
/**
 * Creates an SSM maintenance window asynchronously.
```



```

*
* @param winName The name of the maintenance window.
* @return The ID of the created or existing maintenance window.
* <p>
* This method initiates an asynchronous request to create an SSM maintenance
window.
* If the request is successful, it prints the maintenance window ID.
* If an exception occurs, it handles the error appropriately.
*/
public String createMaintenanceWindow(String winName) throws SsmException,
DocumentAlreadyExistsException {
 CreateMaintenanceWindowRequest request =
CreateMaintenanceWindowRequest.builder()
 .name(winName)
 .description("This is my maintenance window")
 .allowUnassociatedTargets(true)
 .duration(2)
 .cutoff(1)
 .schedule("cron(0 10 ? * MON-FRI *)")
 .build();

 CompletableFuture<CreateMaintenanceWindowResponse> future =
getAsyncClient().createMaintenanceWindow(request);
 final String[] windowId = {null};
 future.whenComplete((response, ex) -> {
 if (response != null) {
 String maintenanceWindowId = response.windowId();
 System.out.println("The maintenance window id is " +
maintenanceWindowId);
 windowId[0] = maintenanceWindowId;
 } else {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
 if (cause instanceof DocumentAlreadyExistsException) {
 throw new CompletionException(cause);
 } else if (cause instanceof SsmException) {
 throw new CompletionException(cause);
 } else {
 throw new RuntimeException(cause);
 }
 }
 }).join();

 if (windowId[0] == null) {

```

```

 MaintenanceWindowFilter filter = MaintenanceWindowFilter.builder()
 .key("name")
 .values(winName)
 .build();

 DescribeMaintenanceWindowsRequest winRequest =
 DescribeMaintenanceWindowsRequest.builder()
 .filters(filter)
 .build();

 CompletableFuture<DescribeMaintenanceWindowsResponse> describeFuture
 = getAsyncClient().describeMaintenanceWindows(winRequest);
 describeFuture.whenComplete((describeResponse, describeEx) -> {
 if (describeResponse != null) {
 List<MaintenanceWindowIdentity> windows =
 describeResponse.windowIdentities();
 if (!windows.isEmpty()) {
 windowId[0] = windows.get(0).windowId();
 System.out.println("Window ID: " + windowId[0]);
 } else {
 System.out.println("Window not found.");
 windowId[0] = "";
 }
 } else {
 Throwable describeCause = (describeEx instanceof
 CompletionException) ? describeEx.getCause() : describeEx;
 throw new RuntimeException("Error describing maintenance
 windows: " + describeCause.getMessage(), describeCause);
 }
 }).join();
 }

 return windowId[0];
}

```

- Per i dettagli sulle API, consulta la [CreateMaintenanceWindow](#) sezione AWS SDK for Java 2.x API Reference.

## JavaScript

### SDK per JavaScript (v3)

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
import { CreateMaintenanceWindowCommand, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Create an SSM maintenance window.
 * @param {{ name: string, allowUnassociatedTargets: boolean, duration: number,
 * cutoff: number, schedule: string, description?: string }}
 */
export const main = async ({
 name,
 allowUnassociatedTargets, // Allow the maintenance window to run on managed
 nodes, even if you haven't registered those nodes as targets.
 duration, // The duration of the maintenance window in hours.
 cutoff, // The number of hours before the end of the maintenance window that
 Amazon Web Services Systems Manager stops scheduling new tasks for execution.
 schedule, // The schedule of the maintenance window in the form of a cron or
 rate expression.
 description = undefined,
}) => {
 const client = new SSMClient({});

 try {
 const { windowId } = await client.send(
 new CreateMaintenanceWindowCommand({
 Name: name,
 Description: description,
 AllowUnassociatedTargets: allowUnassociatedTargets, // Allow the
 maintenance window to run on managed nodes, even if you haven't registered those
 nodes as targets.
 Duration: duration, // The duration of the maintenance window in hours.
```

```
 Cutoff: cutoff, // The number of hours before the end of the maintenance
window that Amazon Web Services Systems Manager stops scheduling new tasks for
execution.
 Schedule: schedule, // The schedule of the maintenance window in the form
of a cron or rate expression.
 }},
);
console.log(`Maintenance window created with Id: ${windowId}`);
return { WindowId: windowId };
} catch (caught) {
 if (caught instanceof Error && caught.name === "MissingParameter") {
 console.warn(`${caught.message}. Did you provide these values?`);
 } else {
 throw caught;
 }
}
};
```

- Per i dettagli sulle API, consulta la [CreateMaintenanceWindow](#) sezione AWS SDK per JavaScript API Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio crea una nuova finestra di manutenzione con il nome specificato che viene eseguita alle 16:00 di ogni martedì per 4 ore, con un limite di 1 ora e che consente obiettivi non associati.

```
New-SSMMaintenanceWindow -Name "MyMaintenanceWindow" -Duration 4 -Cutoff 1 -
AllowUnassociatedTarget $true -Schedule "cron(0 16 ? * TUE *)"
```

Output:

```
mw-03eb53e1ea7383998
```

- Per i dettagli sull'API, vedere [CreateMaintenanceWindow](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio crea una nuova finestra di manutenzione con il nome specificato che viene eseguita alle 16:00 di ogni martedì per 4 ore, con un limite di 1 ora e che consente obiettivi non associati.

```
New-SSMMaintenanceWindow -Name "MyMaintenanceWindow" -Duration 4 -Cutoff 1 -
AllowUnassociatedTarget $true -Schedule "cron(0 16 ? * TUE *)"
```

Output:

```
mw-03eb53e1ea7383998
```

- Per i dettagli sull'API, vedere [CreateMaintenanceWindow](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
class MaintenanceWindowWrapper:
 """Encapsulates AWS Systems Manager maintenance window actions."""

 def __init__(self, ssm_client):
 """
 :param ssm_client: A Boto3 Systems Manager client.
 """
 self.ssm_client = ssm_client
 self.window_id = None
 self.name = None

 @classmethod
 def from_client(cls):
 ssm_client = boto3.client("ssm")
```

```

 return cls(ssm_client)

 def create(self, name, schedule, duration, cutoff,
allow_unassociated_targets):
 """
 Create an AWS Systems Manager maintenance window.

 :param name: The name of the maintenance window.
 :param schedule: The schedule of the maintenance window.
 :param duration: The duration of the maintenance window.
 :param cutoff: The cutoff time of the maintenance window.
 :param allow_unassociated_targets: Allow the maintenance window to run on
managed nodes, even
 if you haven't registered those nodes
as targets.
 """
 try:
 response = self.ssm_client.create_maintenance_window(
 Name=name,
 Schedule=schedule,
 Duration=duration,
 Cutoff=cutoff,
 AllowUnassociatedTargets=allow_unassociated_targets,
)
 self.window_id = response["WindowId"]
 self.name = name
 logger.info("Created maintenance window %s.", self.window_id)
 except ParamValidationError as error:
 logger.error(
 "Parameter validation error when trying to create maintenance
window %s. Here's why: %s",
 self.window_id,
 error,
)
 raise
 except ClientError as err:
 logger.error(
 "Couldn't create maintenance window %s. Here's why: %s: %s",
 name,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise

```

- Per i dettagli sulle API, vedi [CreateMaintenanceWindow](#) in AWS SDK for Python (Boto3) API Reference.

## SAP ABAP

### SDK per SAP ABAP

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
TRY.
 oo_result = lo_ssm->createmaintenancewindow(
 iv_name = iv_name
 iv_schedule = iv_schedule
 iv_duration = iv_duration
 iv_cutoff = iv_cutoff
 iv_allowunassociatedtargets = iv_allow_unassociated_targets).
 MESSAGE 'Maintenance window created.' TYPE 'I'.
CATCH /aws1/cx_ssmresrclimitexcdex.
 MESSAGE 'Resource limit exceeded.' TYPE 'I'.
ENDTRY.
```

- Per i dettagli sulle API, consulta [CreateMaintenanceWindow](#) la sezione AWS SDK for SAP ABAP API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Usare **CreateOpsItem** con un AWS SDK o CLI

I seguenti esempi di codice mostrano come usare `CreateOpsItem`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- [Informazioni di base](#)

## CLI

### AWS CLI

Per creare un OpsItems

L'create-ops-item esempio seguente utilizza il aws/resources tasto/ OperationalData per creare un file OpsItem con una risorsa correlata ad Amazon DynamoDB.

```
aws ssm create-ops-item \
 --title "EC2 instance disk full" \
 --description "Log clean up may have failed which caused the disk to be full" \
 \
 --priority 2 \
 --source ec2 \
 --operational-data '{"aws/resources":{"Value":[{"arn
": "arn:aws:dynamodb:us-west-2:12345678:table/OpsItems
"}]}', "Type":"SearchableString"}' \
 --notifications Arn="arn:aws:sns:us-west-2:12345678:TestUser"
```

Output:

```
{
 "OpsItemId": "oi-1a2b3c4d5e6f"
}
```

Per ulteriori informazioni, consulta [Creating OpsItems](#) nella AWS Systems Manager User Guide.

- Per i dettagli sull'API, vedere [CreateOpsItem](#) in AWS CLI Command Reference.



## Java

### SDK per Java 2.x

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
/**
 * Creates an SSM OpsItem asynchronously.
 *
 * @param title The title of the OpsItem.
 * @param source The source of the OpsItem.
 * @param category The category of the OpsItem.
 * @param severity The severity of the OpsItem.
 * @return The ID of the created OpsItem.
 * <p>
 * This method initiates an asynchronous request to create an SSM OpsItem.
 * If the request is successful, it returns the OpsItem ID.
 * If an exception occurs, it handles the error appropriately.
 */
public String createSSMOpsItem(String title, String source, String category,
String severity) {
 CreateOpsItemRequest opsItemRequest = CreateOpsItemRequest.builder()
 .description("Created by the SSM Java API")
 .title(title)
 .source(source)
 .category(category)
 .severity(severity)
 .build();

 CompletableFuture<CreateOpsItemResponse> future =
getAsyncClient().createOpsItem(opsItemRequest);

 try {
 CreateOpsItemResponse response = future.join();
 return response.opsItemId();
 } catch (CompletionException e) {
 Throwable cause = e.getCause();
 if (cause instanceof SsmException) {
```

```

 throw (SsmException) cause;
 } else {
 throw new RuntimeException(cause);
 }
}
}

```

- Per i dettagli sulle API, consulta la [CreateOpsItem](#) sezione AWS SDK for Java 2.x API Reference.

## JavaScript

### SDK per JavaScript (v3)

#### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```

import { CreateOpsItemCommand, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Create an SSM OpsItem.
 * @param {{ title: string, source: string, category?: string, severity?:
 * string }}
 */
export const main = async ({
 title,
 source,
 category = undefined,
 severity = undefined,
}) => {
 const client = new SSMClient({});
 try {
 const { opsItemArn, opsItemId } = await client.send(
 new CreateOpsItemCommand({
 Title: title,

```

```

 Source: source, // The origin of the OpsItem, such as Amazon EC2 or
 Systems Manager.
 Category: category,
 Severity: severity,
)),
);
 console.log(`Ops item created with id: ${opsItemId}`);
 return { OpsItemArn: opsItemArn, OpsItemId: opsItemId };
} catch (caught) {
 if (caught instanceof Error && caught.name === "MissingParameter") {
 console.warn(`${caught.message}. Did you provide these values?`);
 } else {
 throw caught;
 }
}
};

```

- Per i dettagli sulle API, consulta la [CreateOpsItem](#) sezione AWS SDK per JavaScript API Reference.

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```

class OpsItemWrapper:
 """Encapsulates AWS Systems Manager OpsItem actions."""

 def __init__(self, ssm_client):
 """
 :param ssm_client: A Boto3 Systems Manager client.
 """
 self.ssm_client = ssm_client
 self.id = None

```

```

@classmethod
def from_client(cls):
 """
 :return: A OpsItemWrapper instance.
 """
 ssm_client = boto3.client("ssm")
 return cls(ssm_client)

def create(self, title, source, category, severity, description):
 """
 Create an OpsItem

 :param title: The OpsItem title.
 :param source: The OpsItem source.
 :param category: The OpsItem category.
 :param severity: The OpsItem severity.
 :param description: The OpsItem description.

 """
 try:
 response = self.ssm_client.create_ops_item(
 Title=title,
 Source=source,
 Category=category,
 Severity=severity,
 Description=description,
)
 self.id = response["OpsItemId"]
 except self.ssm_client.exceptions.OpsItemLimitExceededException as err:
 logger.error(
 "Couldn't create ops item because you have exceeded your open\nOpsItem limit. "
 "Here's why: %s: %s",
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise
 except ClientError as err:
 logger.error(
 "Couldn't create ops item %s. Here's why: %s: %s",
 title,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)

```

```
)
raise
```

- Per i dettagli sulle API, vedi [CreateOpsItem](#) in AWS SDK for Python (Boto3) API Reference.

## SAP ABAP

### SDK per SAP ABAP

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
TRY.
 oo_result = lo_ssm->createopsitem(
 iv_title = iv_title
 iv_source = iv_source
 iv_category = iv_category
 iv_severity = iv_severity
 iv_description = iv_description).
 MESSAGE 'OpsItem created.' TYPE 'I'.
CATCH /aws1/cx_ssmopsitemlimitexcdex.
 MESSAGE 'You have exceeded your open OpsItem limit.' TYPE 'I'.
CATCH /aws1/cx_ssmopsitemalrdyexex.
 MESSAGE 'OpsItem already exists.' TYPE 'I'.
ENDTRY.
```

- Per i dettagli sulle API, consulta [CreateOpsItem](#) la sezione AWS SDK for SAP ABAP API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **CreatePatchBaseline** con una CLI

I seguenti esempi di codice mostrano come usare `CreatePatchBaseline`.

### CLI

#### AWS CLI

Esempio 1: per creare una baseline delle patch con approvazione automatica

L'esempio seguente `create-patch-baseline` crea una baseline delle patch per Windows Server che approva le patch per un ambiente di produzione sette giorni dopo che sono state rilasciate da Microsoft.

```
aws ssm create-patch-baseline \
 --name "Windows-Production-Baseline-AutoApproval" \
 --operating-system "WINDOWS" \
 --approval-
rules "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=MSRC_SEVERITY,Values=[Critical,I
{Key=CLASSIFICATION,Values=[SecurityUpdates,Updates,UpdateRollups,CriticalUpdates]}}],App
\
 --description "Baseline containing all updates approved for Windows Server
production systems"
```

Output:

```
{
 "BaselineId": "pb-045f10b4f3EXAMPLE"
}
```

Esempio 2: come creare una baseline delle patch con una data limite di approvazione

L'esempio seguente `create-patch-baseline` crea una baseline delle patch per Windows Server che approva tutte le patch per un ambiente di produzione rilasciate entro il 7 luglio 2020.

```
aws ssm create-patch-baseline \
 --name "Windows-Production-Baseline-AutoApproval" \
 --operating-system "WINDOWS" \
 --approval-
rules "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=MSRC_SEVERITY,Values=[Critical,I
```

```
{Key=CLASSIFICATION,Values=[SecurityUpdates,Updates,UpdateRollups,CriticalUpdates]]}],App
\
--description "Baseline containing all updates approved for Windows Server
production systems"
```

Output:

```
{
 "BaselineId": "pb-045f10b4f3EXAMPLE"
}
```

Esempio 3: come creare una baseline delle patch con regole di approvazione archiviate in un file JSON

L'esempio seguente `create-patch-baseline` crea una baseline delle patch per Amazon Linux 2017.09 che approva le patch per un ambiente di produzione sette giorni dopo il loro rilascio, specifica le regole di approvazione per la baseline della patch e specifica un repository personalizzato per le patch.

```
aws ssm create-patch-baseline \
--cli-input-json file://my-amazon-linux-approval-rules-and-repo.json
```

Contenuto di `my-amazon-linux-approval-rules-and-repo.json`:

```
{
 "Name": "Amazon-Linux-2017.09-Production-Baseline",
 "Description": "My approval rules patch baseline for Amazon Linux 2017.09 instances",
 "OperatingSystem": "AMAZON_LINUX",
 "Tags": [
 {
 "Key": "Environment",
 "Value": "Production"
 }
],
 "ApprovalRules": {
 "PatchRules": [
 {
 "ApproveAfterDays": 7,
 "EnableNonSecurity": true,
 "PatchFilterGroup": {
```

```

 "PatchFilters": [
 {
 "Key": "SEVERITY",
 "Values": [
 "Important",
 "Critical"
]
 },
 {
 "Key": "CLASSIFICATION",
 "Values": [
 "Security",
 "Bugfix"
]
 },
 {
 "Key": "PRODUCT",
 "Values": [
 "AmazonLinux2017.09"
]
 }
]
 },
 "Sources": [
 {
 "Name": "My-AL2017.09",
 "Products": [
 "AmazonLinux2017.09"
],
 "Configuration": "[amzn-main] \nname=amzn-main-Base
\nmirrorlist=http://repo.$awsregion.$awsdomain/$releasever/main/
mirror.list //nmirrorlist_expire=300//nmetadata_expire=300 \npriority=10
\nfailovermethod=priority \nfastestmirror_enabled=0 \ngpgcheck=1
\npgpkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-amazon-ga \nenabled=1 \nretries=3
\ntimeout=5\nreport_instanceid=yes"
 }
]
}

```

Esempio 4: come creare una baseline delle patch che specifichi le patch approvate e rifiutate



L'esempio seguente `create-patch-baseline` specifica esplicitamente le patch da approvare e rifiutare come eccezione alle regole di approvazione predefinite.

```
aws ssm create-patch-baseline \
 --name "Amazon-Linux-2017.09-Alpha-Baseline" \
 --description "My custom approve/reject patch baseline for Amazon Linux
2017.09 instances" \
 --operating-system "AMAZON_LINUX" \
 --approved-patches "CVE-2018-1234567,example-pkg-EE-2018*.amzn1.noarch" \
 --approved-patches-compliance-level "HIGH" \
 --approved-patches-enable-non-security \
 --tags "Key=Environment,Value=Alpha"
```

Per ulteriori informazioni, consulta [Creare una baseline delle patch personalizzata](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [CreatePatchBaseline](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio crea una baseline delle patch che approva le patch, sette giorni dopo che sono state rilasciate da Microsoft, per istanze gestite che eseguono Windows Server 2019 in un ambiente di produzione.

```
$rule = New-Object Amazon.SimpleSystemsManagement.Model.PatchRule
$rule.ApproveAfterDays = 7

$ruleFilters = New-Object Amazon.SimpleSystemsManagement.Model.PatchFilterGroup

$patchFilter = New-Object Amazon.SimpleSystemsManagement.Model.PatchFilter
$patchFilter.Key="PRODUCT"
$patchFilter.Values="WindowsServer2019"

$severityFilter = New-Object Amazon.SimpleSystemsManagement.Model.PatchFilter
$severityFilter.Key="MSRC_SEVERITY"
$severityFilter.Values.Add("Critical")
$severityFilter.Values.Add("Important")
$severityFilter.Values.Add("Moderate")
```

```

$classificationFilter = New-Object
 Amazon.SimpleSystemsManagement.Model.PatchFilter
$classificationFilter.Key = "CLASSIFICATION"
$classificationFilter.Values.Add("SecurityUpdates")
$classificationFilter.Values.Add("Updates")
$classificationFilter.Values.Add("UpdateRollups")
$classificationFilter.Values.Add("CriticalUpdates")

$ruleFilters.PatchFilters.Add($severityFilter)
$ruleFilters.PatchFilters.Add($classificationFilter)
$ruleFilters.PatchFilters.Add($patchFilter)
$rule.PatchFilterGroup = $ruleFilters

New-SSMPatchBaseline -Name "Production-Baseline-Windows2019" -Description
 "Baseline containing all updates approved for production systems" -
ApprovalRules_PatchRule $rule

```

Output:

```
pb-0z4z6221c4296b23z
```

- Per i dettagli sull'API, vedere [CreatePatchBaseline](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio crea una baseline delle patch che approva le patch, sette giorni dopo che sono state rilasciate da Microsoft, per istanze gestite che eseguono Windows Server 2019 in un ambiente di produzione.

```

$rule = New-Object Amazon.SimpleSystemsManagement.Model.PatchRule
$rule.ApproveAfterDays = 7

$ruleFilters = New-Object Amazon.SimpleSystemsManagement.Model.PatchFilterGroup

$patchFilter = New-Object Amazon.SimpleSystemsManagement.Model.PatchFilter
$patchFilter.Key="PRODUCT"
$patchFilter.Values="WindowsServer2019"

$severityFilter = New-Object Amazon.SimpleSystemsManagement.Model.PatchFilter
$severityFilter.Key="MSRC_SEVERITY"
$severityFilter.Values.Add("Critical")
$severityFilter.Values.Add("Important")

```

```
$severityFilter.Values.Add("Moderate")

$classificationFilter = New-Object
 Amazon.SimpleSystemsManagement.Model.PatchFilter
$classificationFilter.Key = "CLASSIFICATION"
$classificationFilter.Values.Add("SecurityUpdates")
$classificationFilter.Values.Add("Updates")
$classificationFilter.Values.Add("UpdateRollups")
$classificationFilter.Values.Add("CriticalUpdates")

$ruleFilters.PatchFilters.Add($severityFilter)
$ruleFilters.PatchFilters.Add($classificationFilter)
$ruleFilters.PatchFilters.Add($patchFilter)
$rule.PatchFilterGroup = $ruleFilters

New-SSMPatchBaseline -Name "Production-Baseline-Windows2019" -Description
 "Baseline containing all updates approved for production systems" -
ApprovalRules_PatchRule $rule
```

Output:

```
pb-0z4z6221c4296b23z
```

- Per i dettagli sull'API, vedere [CreatePatchBaseline](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DeleteActivation** con una CLI

I seguenti esempi di codice mostrano come usare `DeleteActivation`.

### CLI

#### AWS CLI

Per eliminare un'attivazione di un'istanza gestita

L'esempio seguente `delete-activation` elimina l'attivazione di un'istanza gestita.

```
aws ssm delete-activation \
 --activation-id "aa673477-d926-42c1-8757-1358cEXAMPLE"
```

Questo comando non produce alcun output.

Per ulteriori informazioni, vedere [Configurazione di AWS Systems Manager per ambienti ibridi](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [DeleteActivation](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elimina un'attivazione. Se il comando va a buon fine, non viene generato output.

```
Remove-SSMActivation -ActivationId "08e51e79-1e36-446c-8e63-9458569c1363"
```

- Per i dettagli sull'API, vedere [DeleteActivation](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio elimina un'attivazione. Se il comando va a buon fine, non viene generato output.

```
Remove-SSMActivation -ActivationId "08e51e79-1e36-446c-8e63-9458569c1363"
```

- Per i dettagli sull'API, vedere [DeleteActivation](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DeleteAssociation** con una CLI

I seguenti esempi di codice mostrano come usare `DeleteAssociation`.

## CLI

### AWS CLI

Esempio 1: per eliminare un'associazione utilizzando l'ID dell'associazione

L'esempio seguente `delete-association` elimina l'associazione per l'ID di associazione specificato. Se il comando va a buon fine, non viene generato output.

```
aws ssm delete-association \
 --association-id "8dfe3659-4309-493a-8755-0123456789ab"
```

Questo comando non produce alcun output.

Per ulteriori informazioni, consulta [Modifica e creazione di una nuova versione di un'associazione](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 2: come eliminare un'associazione

L'esempio seguente `delete-association` elimina l'associazione tra un'istanza e un documento. Se il comando va a buon fine, non viene generato output.

```
aws ssm delete-association \
 --instance-id "i-1234567890abcdef0" \
 --name "AWS-UpdateSSMAgent"
```

Questo comando non produce alcun output.

Per ulteriori informazioni, consulta [Utilizzo delle associazioni in Systems Manager](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [DeleteAssociation](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elimina l'associazione tra un'istanza e un documento. Se il comando va a buon fine, non viene generato output.

```
Remove-SSMAssociation -InstanceId "i-0cb2b964d3e14fd9f" -Name "AWS-
UpdateSSMAgent"
```

- Per i dettagli sull'API, vedere [DeleteAssociation](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio elimina l'associazione tra un'istanza e un documento. Se il comando va a buon fine, non viene generato output.

```
Remove-SSMAssociation -InstanceId "i-0cb2b964d3e14fd9f" -Name "AWS-UpdateSSMAgent"
```

- Per i dettagli sull'API, vedere [DeleteAssociation](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Usare **DeleteDocument** con un AWS SDK o CLI

I seguenti esempi di codice mostrano come usare `DeleteDocument`.

### CLI

#### AWS CLI

Per eliminare un documento

L'esempio seguente `delete-document` elimina un documento Systems Manager.

```
aws ssm delete-document \
 --name "Example"
```

Questo comando non produce alcun output.

Per ulteriori informazioni, consulta [Creazione di documenti di Systems Manager](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [DeleteDocument](#) in AWS CLI Command Reference.

## Java

### SDK per Java 2.x

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
/**
 * Deletes an AWS SSM document asynchronously.
 *
 * @param documentName The name of the document to delete.
 * <p>
 * This method initiates an asynchronous request to delete an SSM document.
 * If an exception occurs, it handles the error appropriately.
 */
public void deleteDoc(String documentName) {
 DeleteDocumentRequest documentRequest = DeleteDocumentRequest.builder()
 .name(documentName)
 .build();

 CompletableFuture<Void> future = CompletableFuture.runAsync(() -> {
 getAsyncClient().deleteDocument(documentRequest)
 .thenAccept(response -> {
 System.out.println("The SSM document was successfully
deleted.");
 })
 .exceptionally(ex -> {
 throw new CompletionException(ex);
 }).join();
 }).exceptionally(ex -> {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
 if (cause instanceof SsmException) {
 throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
 } else {
 throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
 }
 })
}
```

```

 });

 try {
 future.join();
 } catch (CompletionException ex) {
 throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
ex.getCause() : ex;
 }
}

```

- Per i dettagli sulle API, consulta la [DeleteDocument](#) sezione AWS SDK for Java 2.x API Reference.

## JavaScript

### SDK per JavaScript (v3)

#### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```

import { DeleteDocumentCommand, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Delete an SSM document.
 * @param {{ documentName: string }}
 */
export const main = async ({ documentName }) => {
 const client = new SSMClient({});
 try {
 await client.send(new DeleteDocumentCommand({ Name: documentName }));
 console.log(`Document '${documentName}' deleted.`);
 return { Deleted: true };
 } catch (caught) {
 if (caught instanceof Error && caught.name === "MissingParameter") {
 console.warn(`${caught.message}. Did you provide this value?`);
 } else {

```



```
 throw caught;
 }
}
};
```

- Per i dettagli sulle API, consulta la [DeleteDocument](#) sezione AWS SDK per JavaScript API Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elimina un documento. Se il comando va a buon fine, non viene generato output.

```
Remove-SSMDocument -Name "RunShellScript"
```

- Per i dettagli sull'API, vedere [DeleteDocument](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio elimina un documento. Se il comando va a buon fine, non viene generato output.

```
Remove-SSMDocument -Name "RunShellScript"
```

- Per i dettagli sull'API, vedere [DeleteDocument](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
class DocumentWrapper:
 """Encapsulates AWS Systems Manager Document actions."""

 def __init__(self, ssm_client):
 """
 :param ssm_client: A Boto3 Systems Manager client.
 """
 self.ssm_client = ssm_client
 self.name = None

 @classmethod
 def from_client(cls):
 ssm_client = boto3.client("ssm")
 return cls(ssm_client)

 def delete(self):
 """
 Deletes an AWS Systems Manager document.
 """
 if self.name is None:
 return

 try:
 self.ssm_client.delete_document(Name=self.name)
 print(f"Deleted document {self.name}.")
 self.name = None
 except ClientError as err:
 logger.error(
 "Couldn't delete %s. Here's why: %s: %s",
 self.name,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise
```

- Per i dettagli sulle API, vedi [DeleteDocument](#) in AWS SDK for Python (Boto3) API Reference.

## SAP ABAP

### SDK per SAP ABAP

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
TRY.
 lo_ssm->deletedocument(iv_name = iv_name).
 MESSAGE 'Document deleted.' TYPE 'I'.
CATCH /aws1/cx_ssminvaliddocument.
 MESSAGE 'Invalid document.' TYPE 'I'.
CATCH /aws1/cx_ssmassocdinstances.
 MESSAGE 'Document has associated instances.' TYPE 'I'.
ENDTRY.
```

- Per i dettagli sulle API, consulta [DeleteDocument](#) la sezione AWS SDK for SAP ABAP API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

### Usare **DeleteMaintenanceWindow** con un AWS SDK o CLI

I seguenti esempi di codice mostrano come usareDeleteMaintenanceWindow.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- [Informazioni di base](#)

## CLI

### AWS CLI

Come eliminare una finestra di manutenzione

Questo esempio `delete-maintenance-window` rimuove la finestra di manutenzione specificata.

```
aws ssm delete-maintenance-window \
 --window-id "mw-1a2b3c4d5e6f7g8h9"
```

Output:

```
{
 "WindowId": "mw-1a2b3c4d5e6f7g8h9"
}
```

Per ulteriori informazioni, vedere [Delete a Maintenance Window \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [DeleteMaintenanceWindow](#) in AWS CLI Command Reference.

## Java

### SDK per Java 2.x

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
/**
 * Deletes an AWS SSM Maintenance Window asynchronously.
 *
 * @param winId The ID of the Maintenance Window to delete.
 * <p>
```

```

 * This method initiates an asynchronous request to delete an SSM Maintenance
 Window.
 * If an exception occurs, it handles the error appropriately.
 */
 public void deleteMaintenanceWindow(String winId) {
 DeleteMaintenanceWindowRequest windowRequest =
 DeleteMaintenanceWindowRequest.builder()
 .windowId(winId)
 .build();

 CompletableFuture<Void> future = CompletableFuture.runAsync(() -> {
 getAsyncClient().deleteMaintenanceWindow(windowRequest)
 .thenAccept(response -> {
 System.out.println("The maintenance window was
successfully deleted.");
 })
 .exceptionally(ex -> {
 throw new CompletionException(ex);
 }).join();
 }).exceptionally(ex -> {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
 if (cause instanceof SsmException) {
 throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
 } else {
 throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
 }
 });

 try {
 future.join();
 } catch (CompletionException ex) {
 throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
ex.getCause() : ex;
 }
 }
}

```

- Per i dettagli sulle API, consulta la [DeleteMaintenanceWindow](#) sezione AWS SDK for Java 2.x API Reference.

## JavaScript

### SDK per JavaScript (v3)

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
import { DeleteMaintenanceWindowCommand, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Delete an SSM maintenance window.
 * @param {{ windowId: string }}
 */
export const main = async ({ windowId }) => {
 const client = new SSMClient({});
 try {
 await client.send(
 new DeleteMaintenanceWindowCommand({ WindowId: windowId }),
);
 console.log(`Maintenance window '${windowId}' deleted.`);
 return { Deleted: true };
 } catch (caught) {
 if (caught instanceof Error && caught.name === "MissingParameter") {
 console.warn(`${caught.message}. Did you provide this value?`);
 } else {
 throw caught;
 }
 }
};
```

- Per i dettagli sulle API, consulta la [DeleteMaintenanceWindow](#) sezione AWS SDK per JavaScript API Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio rimuove una finestra di manutenzione.

```
Remove-SSMMaintenanceWindow -WindowId "mw-06d59c1a07c022145"
```

Output:

```
mw-06d59c1a07c022145
```

- Per i dettagli sull'API, vedere [DeleteMaintenanceWindow](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio rimuove una finestra di manutenzione.

```
Remove-SSMMaintenanceWindow -WindowId "mw-06d59c1a07c022145"
```

Output:

```
mw-06d59c1a07c022145
```

- Per i dettagli sull'API, vedere [DeleteMaintenanceWindow](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
class MaintenanceWindowWrapper:
```

```
"""Encapsulates AWS Systems Manager maintenance window actions."""

def __init__(self, ssm_client):
 """
 :param ssm_client: A Boto3 Systems Manager client.
 """
 self.ssm_client = ssm_client
 self.window_id = None
 self.name = None

 @classmethod
 def from_client(cls):
 ssm_client = boto3.client("ssm")
 return cls(ssm_client)

def delete(self):
 """
 Delete the associated AWS Systems Manager maintenance window.
 """
 if self.window_id is None:
 return

 try:
 self.ssm_client.delete_maintenance_window(WindowId=self.window_id)
 logger.info("Deleted maintenance window %s.", self.window_id)
 print(f"Deleted maintenance window {self.name}")
 self.window_id = None
 except ClientError as err:
 logger.error(
 "Couldn't delete maintenance window %s. Here's why: %s: %s",
 self.window_id,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise
```

- Per i dettagli sulle API, vedi [DeleteMaintenanceWindow](#) in AWS SDK for Python (Boto3) API Reference.



## SAP ABAP

### SDK per SAP ABAP

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
TRY.
 lo_ssm->deletemaintenancewindow(iv_windowid = iv_window_id).
 MESSAGE 'Maintenance window deleted.' TYPE 'I'.
CATCH /aws1/cx_ssmininternalservererr.
 MESSAGE 'Internal server error occurred.' TYPE 'I'.
ENDTRY.
```

- Per i dettagli sulle API, consulta [DeleteMaintenanceWindow](#) la sezione AWS SDK for SAP ABAP API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

### Usare **DeleteOpsItem** con un AWS SDK

I seguenti esempi di codice mostrano come usare `DeleteOpsItem`.

#### Python

##### SDK per Python (Boto3)

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
class OpsItemWrapper:
```

```
"""Encapsulates AWS Systems Manager OpsItem actions."""

def __init__(self, ssm_client):
 """
 :param ssm_client: A Boto3 Systems Manager client.
 """
 self.ssm_client = ssm_client
 self.id = None

 @classmethod
 def from_client(cls):
 """
 :return: A OpsItemWrapper instance.
 """
 ssm_client = boto3.client("ssm")
 return cls(ssm_client)

 def delete(self):
 """
 Delete the OpsItem.
 """
 if self.id is None:
 return
 try:
 self.ssm_client.delete_ops_item(OpsItemId=self.id)
 print(f"Deleted ops item with id {self.id}")
 self.id = None
 except ClientError as err:
 logger.error(
 "Couldn't delete ops item %s. Here's why: %s: %s",
 self.id,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise
```

- Per i dettagli sulle API, vedi [DeleteOpsItem](#) in AWS SDK for Python (Boto3) API Reference.

## SAP ABAP

### SDK per SAP ABAP

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
TRY.
 lo_ssm->deleteopsitem(iv_opsitemid = iv_ops_item_id).
 MESSAGE 'OpsItem deleted.' TYPE 'I'.
CATCH /aws1/cx_ssmopsiteminvparamex.
 MESSAGE 'Invalid OpsItem parameter.' TYPE 'I'.
ENDTRY.
```

- Per i dettagli sulle API, consulta [DeleteOpsItem](#) la sezione AWS SDK for SAP ABAP API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

### Utilizzo di **DeleteParameter** con una CLI

I seguenti esempi di codice mostrano come usare `DeleteParameter`.

#### CLI

##### AWS CLI

Per eliminare un parametro

L'esempio seguente `delete-parameter` elimina il singolo parametro specificato.

```
aws ssm delete-parameter \
 --name "MyParameter"
```

Questo comando non produce alcun output.

Per ulteriori informazioni, consulta [Utilizzo dell'Archivio parametri](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [DeleteParameter](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elimina un parametro. Se il comando va a buon fine, non viene generato output.

```
Remove-SSMParameter -Name "helloWorld"
```

- Per i dettagli sull'API, vedere [DeleteParameter](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio elimina un parametro. Se il comando va a buon fine, non viene generato output.

```
Remove-SSMParameter -Name "helloWorld"
```

- Per i dettagli sull'API, vedere [DeleteParameter](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DeletePatchBaseline** con una CLI

I seguenti esempi di codice mostrano come usare `DeletePatchBaseline`.

### CLI

#### AWS CLI

Per eliminare una baseline delle patch

L'esempio seguente `delete-patch-baseline` elimina la baseline delle patch specificata.

```
aws ssm delete-patch-baseline \
 --baseline-id "pb-045f10b4f382baeda"
```

Output:

```
{
 "BaselineId": "pb-045f10b4f382baeda"
}
```

Per ulteriori informazioni, consulta [Aggiornare o eliminare una baseline delle patch \(console\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [DeletePatchBaseline](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elimina una baseline delle patch.

```
Remove-SSMPatchBaseline -BaselineId "pb-045f10b4f382baeda"
```

Output:

```
pb-045f10b4f382baeda
```

- Per i dettagli sull'API, vedere [DeletePatchBaseline](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio elimina una baseline delle patch.

```
Remove-SSMPatchBaseline -BaselineId "pb-045f10b4f382baeda"
```

Output:

```
pb-045f10b4f382baeda
```

- Per i dettagli sull'API, vedere [DeletePatchBaseline](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DeregisterManagedInstance** con una CLI

I seguenti esempi di codice mostrano come usare `DeregisterManagedInstance`.

### CLI

#### AWS CLI

Per annullare la registrazione di un'istanza gestita

L'esempio seguente `deregister-managed-instance` annulla la registrazione dell'istanza gestita specificata.

```
aws ssm deregister-managed-instance \
 --instance-id 'mi-08ab247cdfEXAMPLE'
```

Questo comando non produce alcun output.

Per ulteriori informazioni, consulta [Annullare la registrazione di nodi gestiti in ambienti ibridi e multi-cloud](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [DeregisterManagedInstance](#) in AWS CLI Command Reference.

### PowerShell

#### Strumenti per PowerShell V4

Esempio 1: questo esempio annulla la registrazione di un'istanza gestita. Se il comando va a buon fine, non viene generato output.

```
Unregister-SSMManagedInstance -InstanceId "mi-08ab247cdf1046573"
```

- Per i dettagli sull'API, vedere [DeregisterManagedInstance](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio annulla la registrazione di un'istanza gestita. Se il comando va a buon fine, non viene generato output.

```
Unregister-SSMManagedInstance -InstanceId "mi-08ab247cdf1046573"
```

- Per i dettagli sull'API, vedere [DeregisterManagedInstance](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DeregisterPatchBaselineForPatchGroup** con una CLI

I seguenti esempi di codice mostrano come usare `DeregisterPatchBaselineForPatchGroup`.

### CLI

#### AWS CLI

Annullamento della registrazione di un gruppo di patch da una baseline delle patch

L'esempio seguente `deregister-patch-baseline-for-patch-group` annulla la registrazione del gruppo di patch specificato dalle baseline della patch specificata.

```
aws ssm deregister-patch-baseline-for-patch-group \
 --patch-group "Production" \
 --baseline-id "pb-0ca44a362fEXAMPLE"
```

Output:

```
{
 "PatchGroup": "Production",
 "BaselineId": "pb-0ca44a362fEXAMPLE"
}
```

Per ulteriori informazioni, consulta [Aggiungere un gruppo di patch a una baseline delle patch](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [DeregisterPatchBaselineForPatchGroup](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio annulla la registrazione di un gruppo di patch da una baseline delle patch.

```
Unregister-SSMPatchBaselineForPatchGroup -BaselineId "pb-045f10b4f382baeda" -PatchGroup "Production"
```

Output:

BaselineId	PatchGroup
-----	-----
pb-045f10b4f382baeda	Production

- Per i dettagli sull'API, vedere [DeregisterPatchBaselineForPatchGroup](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio annulla la registrazione di un gruppo di patch da una baseline delle patch.

```
Unregister-SSMPatchBaselineForPatchGroup -BaselineId "pb-045f10b4f382baeda" -PatchGroup "Production"
```

Output:

BaselineId	PatchGroup
-----	-----
pb-045f10b4f382baeda	Production

- Per i dettagli sull'API, vedere [DeregisterPatchBaselineForPatchGroup](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).



Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DeregisterTargetFromMaintenanceWindow** con una CLI

I seguenti esempi di codice mostrano come usare `DeregisterTargetFromMaintenanceWindow`.

### CLI

#### AWS CLI

Per rimuovere una destinazione da una finestra di manutenzione

L'esempio seguente `deregister-target-from-maintenance-window` rimuove la destinazione specificata dalla finestra di manutenzione specificata.

```
aws ssm deregister-target-from-maintenance-window \
 --window-id "mw-ab12cd34ef56gh78" \
 --window-target-id "1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
```

Output:

```
{
 "WindowId": "mw-ab12cd34ef56gh78",
 "WindowTargetId": "1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

Per ulteriori informazioni, vedere [Update a Maintenance Window \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [DeregisterTargetFromMaintenanceWindow](#) in AWS CLI Command Reference.

### PowerShell

#### Strumenti per PowerShell V4

Esempio 1: questo esempio rimuove una destinazione da una finestra di manutenzione.

```
Unregister-SSMTargetFromMaintenanceWindow -WindowTargetId
"6ab5c208-9fc4-4697-84b7-b02a6cc25f7d" -WindowId "mw-06cf17cbefcb4bf4f"
```

Output:

WindowId	WindowTargetId
-----	-----
mw-06cf17cbefcb4bf4f	6ab5c208-9fc4-4697-84b7-b02a6cc25f7d

- Per i dettagli sull'API, vedere [DeregisterTargetFromMaintenanceWindow](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: questo esempio rimuove una destinazione da una finestra di manutenzione.

```
Unregister-SSMTargetFromMaintenanceWindow -WindowTargetId
"6ab5c208-9fc4-4697-84b7-b02a6cc25f7d" -WindowId "mw-06cf17cbefcb4bf4f"
```

Output:

WindowId	WindowTargetId
-----	-----
mw-06cf17cbefcb4bf4f	6ab5c208-9fc4-4697-84b7-b02a6cc25f7d

- Per i dettagli sull'API, vedere [DeregisterTargetFromMaintenanceWindow](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DeregisterTaskFromMaintenanceWindow** con una CLI

I seguenti esempi di codice mostrano come usare `DeregisterTaskFromMaintenanceWindow`.

CLI

AWS CLI

Per rimuovere un'attività da una finestra di manutenzione

L'esempio seguente `deregister-task-from-maintenance-window` rimuove l'attività specificata dalla finestra di manutenzione specificata.

```
aws ssm deregister-task-from-maintenance-window \
 --window-id "mw-ab12cd34ef56gh78" \
 --window-task-id "1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d5e6c"
```

Output:

```
{
 "WindowTaskId": "1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d5e6c",
 "WindowId": "mw-ab12cd34ef56gh78"
}
```

Per ulteriori informazioni, vedere [Systems Manager Maintenance Windows Tutorials \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sulle API, vedere [DeregisterTaskFromMaintenanceWindow](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio rimuove un'attività da una finestra di manutenzione.

```
Unregister-SSMTaskFromMaintenanceWindow -WindowTaskId "f34a2c47-ddfd-4c85-a88d-72366b69af1b" -WindowId "mw-03a342e62c96d31b0"
```

Output:

WindowId	WindowTaskId
-----	-----
mw-03a342e62c96d31b0	f34a2c47-ddfd-4c85-a88d-72366b69af1b

- Per i dettagli sull'API, vedere [DeregisterTaskFromMaintenanceWindow](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio rimuove un'attività da una finestra di manutenzione.

```
Unregister-SSMTaskFromMaintenanceWindow -WindowTaskId "f34a2c47-ddfd-4c85-a88d-72366b69af1b" -WindowId "mw-03a342e62c96d31b0"
```

Output:

WindowId	WindowTaskId
-----	-----
mw-03a342e62c96d31b0	f34a2c47-ddfd-4c85-a88d-72366b69af1b

- Per i dettagli sull'API, vedere [DeregisterTaskFromMaintenanceWindow](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeActivations** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeActivations`.

### CLI

#### AWS CLI

Per descrivere le attivazioni

L'`describe-activation`sempio seguente elenca i dettagli sulle attivazioni nel tuo AWS account.

```
aws ssm describe-activations
```

Output:

```
{
 "ActivationList": [
 {
 "ActivationId": "5743558d-563b-4457-8682-d16c3EXAMPLE",
 "Description": "Example1",
 "IamRole": "HybridWebServersRole,
```

```

 "RegistrationLimit": 5,
 "RegistrationsCount": 5,
 "ExpirationDate": 1584316800.0,
 "Expired": false,
 "CreateDate": 1581954699.792
 },
 {
 "ActivationId": "3ee0322b-f62d-40eb-b672-13ebfEXAMPLE",
 "Description": "Example2",
 "IamRole": "HybridDatabaseServersRole",
 "RegistrationLimit": 5,
 "RegistrationsCount": 5,
 "ExpirationDate": 1580515200.0,
 "Expired": true,
 "CreateDate": 1578064132.002
 },
]
}

```

Per ulteriori informazioni, vedere la [Fase 4: Creazione di un' Managed-Instance attivazione per un ambiente ibrido](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [DescribeActivations](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio fornisce dettagli sulle attivazioni sull'account.

```
Get-SSMActivation
```

Output:

```

ActivationId : 08e51e79-1e36-446c-8e63-9458569c1363
CreateDate : 3/1/2017 12:01:51 AM
DefaultInstanceName : MyWebServers
Description :
ExpirationDate : 3/2/2017 12:01:51 AM
Expired : False
IamRole : AutomationRole
RegistrationLimit : 10

```

```
RegistrationsCount : 0
```

- Per i dettagli sull'API, vedere [DescribeActivations](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio fornisce dettagli sulle attivazioni sull'account.

```
Get-SSMActivation
```

### Output:

```
ActivationId : 08e51e79-1e36-446c-8e63-9458569c1363
CreatedDate : 3/1/2017 12:01:51 AM
DefaultInstanceName : MyWebServers
Description :
ExpirationDate : 3/2/2017 12:01:51 AM
Expired : False
IamRole : AutomationRole
RegistrationLimit : 10
RegistrationsCount : 0
```

- Per i dettagli sull'API, vedere [DescribeActivations](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeAssociation** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeAssociation`.

### CLI

#### AWS CLI

Esempio 1: per ottenere i dettagli di un'associazione

L'esempio seguente `describe-association` descrive l'associazione per l'ID di associazione specificato.

```
aws ssm describe-association \
 --association-id "8dfe3659-4309-493a-8755-0123456789ab"
```

Output:

```
{
 "AssociationDescription": {
 "Name": "AWS-GatherSoftwareInventory",
 "AssociationVersion": "1",
 "Date": 1534864780.995,
 "LastUpdateAssociationDate": 1543235759.81,
 "Overview": {
 "Status": "Success",
 "AssociationStatusAggregatedCount": {
 "Success": 2
 }
 },
 "DocumentVersion": "$DEFAULT",
 "Parameters": {
 "applications": [
 "Enabled"
],
 "awsComponents": [
 "Enabled"
],
 "customInventory": [
 "Enabled"
],
 "files": [
 ""
],
 "instanceDetailedInformation": [
 "Enabled"
],
 "networkConfig": [
 "Enabled"
],
 "services": [
 "Enabled"
],
 "windowsRegistry": [
 ""
],
 },
 },
}
```

```

 "windowsRoles": [
 "Enabled"
],
 "windowsUpdates": [
 "Enabled"
]
 },
 "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
 "*"
]
 }
],
 "ScheduleExpression": "rate(24 hours)",
 "LastExecutionDate": 1550501886.0,
 "LastSuccessfulExecutionDate": 1550501886.0,
 "AssociationName": "Inventory-Association"
}
}

```

Per ulteriori informazioni, consulta [Modifica e creazione di una nuova versione di un'associazione](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 2: come ottenere i dettagli di un'associazione per un'istanza e un documento specifici

L'esempio seguente `describe-association` descrive l'associazione tra un'istanza e un documento.

```

aws ssm describe-association \
 --instance-id "i-1234567890abcdef0" \
 --name "AWS-UpdateSSMAgent"

```

Output:

```

{
 "AssociationDescription": {
 "Status": {
 "Date": 1487876122.564,
 "Message": "Associated with AWS-UpdateSSMAgent",

```



```

 "Name": "Associated"
 },
 "Name": "AWS-UpdateSSMAgent",
 "InstanceId": "i-1234567890abcdef0",
 "Overview": {
 "Status": "Pending",
 "DetailedStatus": "Associated",
 "AssociationStatusAggregatedCount": {
 "Pending": 1
 }
 },
 "AssociationId": "d8617c07-2079-4c18-9847-1234567890ab",
 "DocumentVersion": "$DEFAULT",
 "LastUpdateAssociationDate": 1487876122.564,
 "Date": 1487876122.564,
 "Targets": [
 {
 "Values": [
 "i-1234567890abcdef0"
],
 "Key": "InstanceIds"
 }
]
 }
]
}

```

Per ulteriori informazioni, consulta [Modifica e creazione di una nuova versione di un'associazione](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [DescribeAssociation](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio descrive l'associazione tra un'istanza e un documento.

```
Get-SSMAssociation -InstanceId "i-0000293ffd8c57862" -Name "AWS-UpdateSSMAgent"
```

Output:

```
Name : AWS-UpdateSSMAgent
```

```

InstanceId : i-0000293ffd8c57862
Date : 2/23/2017 6:55:22 PM
Status.Name : Pending
Status.Date : 2/20/2015 8:31:11 AM
Status.Message : temp_status_change
Status.AdditionalInfo : Additional-Config-Needed

```

- Per i dettagli sull'API, vedere [DescribeAssociation](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio descrive l'associazione tra un'istanza e un documento.

```
Get-SSMAssociation -InstanceId "i-0000293ffd8c57862" -Name "AWS-UpdateSSMAgent"
```

Output:

```

Name : AWS-UpdateSSMAgent
InstanceId : i-0000293ffd8c57862
Date : 2/23/2017 6:55:22 PM
Status.Name : Pending
Status.Date : 2/20/2015 8:31:11 AM
Status.Message : temp_status_change
Status.AdditionalInfo : Additional-Config-Needed

```

- Per i dettagli sull'API, vedere [DescribeAssociation](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeAssociationExecutionTargets** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeAssociationExecutionTargets`.

### CLI

#### AWS CLI

Per ottenere dettagli sull'esecuzione di un'associazione

L'esempio seguente `describe-association-execution-targets` descrive l'esecuzione dell'associazione specificata.

```
aws ssm describe-association-execution-targets \
 --association-id "8dfe3659-4309-493a-8755-0123456789ab" \
 --execution-id "7abb6378-a4a5-4f10-8312-0123456789ab"
```

Output:

```
{
 "AssociationExecutionTargets": [
 {
 "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
 "AssociationVersion": "1",
 "ExecutionId": "7abb6378-a4a5-4f10-8312-0123456789ab",
 "ResourceId": "i-1234567890abcdef0",
 "ResourceType": "ManagedInstance",
 "Status": "Success",
 "DetailedStatus": "Success",
 "LastExecutionDate": 1550505538.497,
 "OutputSource": {
 "OutputSourceId": "97fff367-fc5a-4299-aed8-0123456789ab",
 "OutputSourceType": "RunCommand"
 }
 }
]
}
```

Per ulteriori informazioni, consulta [Visualizzazione della cronologia delle associazioni](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [DescribeAssociationExecutionTargets](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio visualizza l'ID della risorsa e il relativo stato di esecuzione che fanno parte degli obiettivi di esecuzione dell'associazione

```
Get-SSMAssociationExecutionTarget -AssociationId 123a45a0-
c678-9012-3456-78901234db5e -ExecutionId 123a45a0-c678-9012-3456-78901234db5e |
Select-Object ResourceId, Status
```

Output:

ResourceId	Status
-----	-----
i-0b1b2a3456f7a890b	Success
i-01c12a45d6fc7a89f	Success
i-0a1caf234f56d7dc8	Success
i-012a3fd45af6dbcf	Failed
i-0ddc1df23c4a5fb67	Success

Esempio 2: questo comando controlla la particolare esecuzione di una particolare automazione a partire da ieri, alla quale è associato un documento di comando. Controlla ulteriormente se l'esecuzione dell'associazione è fallita e, in tal caso, mostrerà i dettagli dell'invocazione del comando per l'esecuzione insieme all'ID dell'istanza

```
$AssociationExecution= Get-SSMAssociationExecutionTarget -
AssociationId 1c234567-890f-1aca-a234-5a678d901cb0 -ExecutionId
12345ca12-3456-2345-2b45-23456789012 |
Where-Object {$_.LastExecutionDate -gt (Get-Date -Hour 00 -Minute
00).AddDays(-1)}

foreach ($execution in $AssociationExecution) {
 if($execution.Status -ne 'Success'){
 Write-Output "There was an issue executing the association
 $($execution.AssociationId) on $($execution.ResourceId)"
 Get-SSMCommandInvocation -CommandId
 $execution.OutputSource.OutputSourceId -Detail:$true | Select-Object -
ExpandProperty CommandPlugins
 }
}
```

Output:

```
There was an issue executing the association 1c234567-890f-1aca-a234-5a678d901cb0
on i-0a1caf234f56d7dc8
```

```

Name : aws:runPowerShellScript
Output :
 -----ERROR-----
 failed to run commands: exit status 1
OutputS3BucketName :
OutputS3KeyPrefix :
OutputS3Region : eu-west-1
ResponseCode : 1
ResponseFinishDateTime : 5/29/2019 11:04:49 AM
ResponseStartDateTime : 5/29/2019 11:04:49 AM
StandardErrorUrl :
StandardOutputUrl :
Status : Failed
StatusDetails : Failed

```

- Per i dettagli sull'API, vedere [DescribeAssociationExecutionTargets](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio visualizza l'ID della risorsa e il relativo stato di esecuzione che fanno parte degli obiettivi di esecuzione dell'associazione

```

Get-SSMAssociationExecutionTarget -AssociationId 123a45a0-
c678-9012-3456-78901234db5e -ExecutionId 123a45a0-c678-9012-3456-78901234db5e |
Select-Object ResourceId, Status

```

Output:

```

ResourceId Status

i-0b1b2a3456f7a890b Success
i-01c12a45d6fc7a89f Success
i-0a1caf234f56d7dc8 Success
i-012a3fd45af6dbcfe Failed
i-0ddc1df23c4a5fb67 Success

```

Esempio 2: questo comando controlla la particolare esecuzione di una particolare automazione a partire da ieri, alla quale è associato un documento di comando. Controlla ulteriormente se l'esecuzione dell'associazione è fallita e, in tal caso, mostrerà i dettagli dell'invocazione del comando per l'esecuzione insieme all'ID dell'istanza

```
$AssociationExecution= Get-SSMAssociationExecutionTarget -
AssociationId 1c234567-890f-1aca-a234-5a678d901cb0 -ExecutionId
12345ca12-3456-2345-2b45-23456789012 |
 Where-Object {$_.LastExecutionDate -gt (Get-Date -Hour 00 -Minute
00).AddDays(-1)}

foreach ($execution in $AssociationExecution) {
 if($execution.Status -ne 'Success'){
 Write-Output "There was an issue executing the association
 $($execution.AssociationId) on $($execution.ResourceId)"
 Get-SSMCommandInvocation -CommandId
 $execution.OutputSource.OutputSourceId -Detail:$true | Select-Object -
ExpandProperty CommandPlugins
 }
}
```

### Output:

```
There was an issue executing the association 1c234567-890f-1aca-a234-5a678d901cb0
on i-0a1caf234f56d7dc8
```

```
Name : aws:runPowerShellScript
Output :
 -----ERROR-----
 failed to run commands: exit status 1
OutputS3BucketName :
OutputS3KeyPrefix :
OutputS3Region : eu-west-1
ResponseCode : 1
ResponseFinishDateTime : 5/29/2019 11:04:49 AM
ResponseStartDateTime : 5/29/2019 11:04:49 AM
StandardErrorUrl :
StandardOutputUrl :
Status : Failed
StatusDetails : Failed
```

- Per i dettagli sull'API, vedere [DescribeAssociationExecutionTargets](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeAssociationExecutions** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeAssociationExecutions`.

### CLI

#### AWS CLI

Esempio 1: per ottenere i dettagli di tutte le esecuzioni di un'associazione

L'esempio seguente `describe-association-executions` descrive tutte le esecuzioni dell'associazione specificata.

```
aws ssm describe-association-executions \
 --association-id "8dfe3659-4309-493a-8755-0123456789ab"
```

Output:

```
{
 "AssociationExecutions": [
 {
 "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
 "AssociationVersion": "1",
 "ExecutionId": "474925ef-1249-45a2-b93d-0123456789ab",
 "Status": "Success",
 "DetailedStatus": "Success",
 "CreatedTime": 1550505827.119,
 "ResourceCountByStatus": "{Success=1}"
 },
 {
 "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
 "AssociationVersion": "1",
 "ExecutionId": "7abb6378-a4a5-4f10-8312-0123456789ab",
 "Status": "Success",
 "DetailedStatus": "Success",
 "CreatedTime": 1550505536.843,
 "ResourceCountByStatus": "{Success=1}"
 },
],
}
```

```
 ...
]
}
```

Per ulteriori informazioni, consulta [Visualizzazione della cronologia delle associazioni](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 2: come ottenere i dettagli di tutte le esecuzioni di un'associazione dopo una data e un'ora specifiche

L'esempio seguente `describe-association-executions` descrive tutte le esecuzioni di un'associazione dopo la data e l'ora specificate.

```
aws ssm describe-association-executions \
 --association-id "8dfe3659-4309-493a-8755-0123456789ab" \
 --filters "Key=CreatedTime,Value=2019-02-18T16:00:00Z,Type=GREATER_THAN"
```

Output:

```
{
 "AssociationExecutions": [
 {
 "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
 "AssociationVersion": "1",
 "ExecutionId": "474925ef-1249-45a2-b93d-0123456789ab",
 "Status": "Success",
 "DetailedStatus": "Success",
 "CreatedTime": 1550505827.119,
 "ResourceCountByStatus": "{Success=1}"
 },
 {
 "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
 "AssociationVersion": "1",
 "ExecutionId": "7abb6378-a4a5-4f10-8312-0123456789ab",
 "Status": "Success",
 "DetailedStatus": "Success",
 "CreatedTime": 1550505536.843,
 "ResourceCountByStatus": "{Success=1}"
 },
 ...
]
}
```



Per ulteriori informazioni, consulta [Visualizzazione della cronologia delle associazioni](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [DescribeAssociationExecutions](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio restituisce le esecuzioni per l'ID di associazione fornito

```
Get-SSMAssociationExecution -AssociationId 123a45a0-c678-9012-3456-78901234db5e
```

Output:

```
AssociationId : 123a45a0-c678-9012-3456-78901234db5e
AssociationVersion : 2
CreatedTime : 3/2/2019 8:53:29 AM
DetailedStatus :
ExecutionId : 123a45a0-c678-9012-3456-78901234db5e
LastExecutionDate : 1/1/0001 12:00:00 AM
ResourceCountByStatus : {Success=4}
Status : Success
```

- Per i dettagli sull'API, vedere [DescribeAssociationExecutions](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio restituisce le esecuzioni per l'ID di associazione fornito

```
Get-SSMAssociationExecution -AssociationId 123a45a0-c678-9012-3456-78901234db5e
```

Output:

```
AssociationId : 123a45a0-c678-9012-3456-78901234db5e
AssociationVersion : 2
CreatedTime : 3/2/2019 8:53:29 AM
DetailedStatus :
ExecutionId : 123a45a0-c678-9012-3456-78901234db5e
LastExecutionDate : 1/1/0001 12:00:00 AM
```

```
ResourceCountByStatus : {Success=4}
Status : Success
```

- Per i dettagli sull'API, vedere [DescribeAssociationExecutions](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeAutomationExecutions** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeAutomationExecutions`.

### CLI

#### AWS CLI

Per descrivere un'esecuzione di automazione

L'esempio seguente `describe-automation-executions` mostra i dettagli sull'esecuzione di un'automazione.

```
aws ssm describe-automation-executions \
 --filters Key=ExecutionId,Values=73c8eef8-f4ee-4a05-820c-e354fEXAMPLE
```

Output:

```
{
 "AutomationExecutionMetadataList": [
 {
 "AutomationExecutionId": "73c8eef8-f4ee-4a05-820c-e354fEXAMPLE",
 "DocumentName": "AWS-StartEC2Instance",
 "DocumentVersion": "1",
 "AutomationExecutionStatus": "Success",
 "ExecutionStartTime": 1583737233.748,
 "ExecutionEndTime": 1583737234.719,
 "ExecutedBy": "arn:aws:sts::29884EXAMPLE:assumed-role/mw_service_role/OrchestrationService",
 "LogFile": "",
 "Outputs": {},
 }
]
}
```

```

 "Mode": "Auto",
 "Targets": [],
 "ResolvedTargets": {
 "ParameterValues": [],
 "Truncated": false
 },
 "AutomationType": "Local"
 }
]
}

```

Per ulteriori informazioni, consulta [Esecuzione di un flusso di lavoro di automazione Simple \(Semplice\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [DescribeAutomationExecutions](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio descrive tutte le esecuzioni di automazione attive e terminate associate all'account.

```
Get-SSMAutomationExecutionList
```

Output:

```

AutomationExecutionId : 4105a4fc-f944-11e6-9d32-8fb2db27a909
AutomationExecutionStatus : Failed
DocumentName : AWS-UpdateLinuxAmi
DocumentVersion : 1
ExecutedBy : admin
ExecutionEndTime : 2/22/2017 9:17:08 PM
ExecutionStartTime : 2/22/2017 9:17:02 PM
LogFile :
Outputs : {[createImage.ImageId,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}

```

Esempio 2: questo esempio visualizza executionID, document, start/end timestamp di esecuzione per le esecuzioni con un valore diverso da «Success» AutomationExecutionStatus

```
Get-SSMAutomationExecutionList | Where-Object AutomationExecutionStatus
 -ne "Success" | Select-Object AutomationExecutionId, DocumentName,
 AutomationExecutionStatus, ExecutionStartTime, ExecutionEndTime | Format-Table -
 AutoSize
```

Output:

AutomationExecutionId	DocumentName	AutomationExecutionStatus	ExecutionStartTime	ExecutionEndTime
e1d2bad3-4567-8901-ae23-456c7c8901be	AWS-UpdateWindowsAmi	Cancelled	4/16/2019 5:37:04 AM	4/16/2019 5:47:29 AM
61234567-a7f8-90e1-2b34-567b8bf9012c	Fixed-UpdateAmi	Cancelled	4/16/2019 5:33:04 AM	4/16/2019 5:40:15 AM
91234d56-7e89-0ac1-2aee-34ea5d6a7c89	AWS-UpdateWindowsAmi	Failed	4/16/2019 5:22:46 AM	4/16/2019 5:27:29 AM

- Per i dettagli sull'API, vedere [DescribeAutomationExecutions](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio descrive tutte le esecuzioni di automazione attive e terminate associate all'account.

```
Get-SSMAutomationExecutionList
```

Output:

```
AutomationExecutionId : 4105a4fc-f944-11e6-9d32-8fb2db27a909
AutomationExecutionStatus : Failed
DocumentName : AWS-UpdateLinuxAmi
DocumentVersion : 1
ExecutedBy : admin
ExecutionEndTime : 2/22/2017 9:17:08 PM
ExecutionStartTime : 2/22/2017 9:17:02 PM
LogFile :
Outputs : {[createImage.ImageId,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
```

Esempio 2: questo esempio visualizza executionID, document, start/end timestamp di esecuzione per le esecuzioni con un valore diverso da «Success» AutomationExecutionStatus

```
Get-SSMAutomationExecutionList | Where-Object AutomationExecutionStatus
-ne "Success" | Select-Object AutomationExecutionId, DocumentName,
AutomationExecutionStatus, ExecutionStartTime, ExecutionEndTime | Format-Table -
AutoSize
```

Output:

AutomationExecutionId	DocumentName	AutomationExecutionStatus	ExecutionStartTime	ExecutionEndTime
e1d2bad3-4567-8901-ae23-456c7c8901be	AWS-UpdateWindowsAmi	Cancelled	4/16/2019 5:37:04 AM	4/16/2019 5:47:29 AM
61234567-a7f8-90e1-2b34-567b8bf9012c	Fixed-UpdateAmi	Cancelled	4/16/2019 5:33:04 AM	4/16/2019 5:40:15 AM
91234d56-7e89-0ac1-2aee-34ea5d6a7c89	AWS-UpdateWindowsAmi	Failed	4/16/2019 5:22:46 AM	4/16/2019 5:27:29 AM

- Per i dettagli sull'API, vedere [DescribeAutomationExecutions](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeAutomationStepExecutions** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeAutomationStepExecutions`.

### CLI

#### AWS CLI

Esempio 1: per descrivere tutti i passaggi per l'esecuzione di un'automazione

L'esempio seguente `describe-automation-step-executions` mostra i dettagli sui passaggi di un'esecuzione di automazione.

```
aws ssm describe-automation-step-executions \
 --automation-execution-id 73c8eef8-f4ee-4a05-820c-e354fEXAMPLE
```

Output:

```
{
 "StepExecutions": [
 {
 "StepName": "startInstances",
 "Action": "aws:changeInstanceState",
 "ExecutionStartTime": 1583737234.134,
 "ExecutionEndTime": 1583737234.672,
 "StepStatus": "Success",
 "Inputs": {
 "DesiredState": "\"running\"",
 "InstanceIds": "[\"i-0cb99161f6EXAMPLE\"]"
 },
 "Outputs": {
 "InstanceStates": [
 "running"
]
 },
 "StepExecutionId": "95e70479-cf20-4d80-8018-7e4e2EXAMPLE",
 "OverriddenParameters": {}
 }
]
}
```

Esempio 2: come descrivere un passaggio specifico per l'esecuzione di un'automazione

L'esempio seguente `describe-automation-step-executions` mostra i dettagli su un passaggio specifico di un'esecuzione di automazione.

```
aws ssm describe-automation-step-executions \
 --automation-execution-id 73c8eef8-f4ee-4a05-820c-e354fEXAMPLE \
 --filters Key=StepExecutionId,Values=95e70479-cf20-4d80-8018-7e4e2EXAMPLE
```

Per ulteriori informazioni, consulta [Procedura dettagliata per l'esecuzione di un flusso di lavoro di automazione \(riga di comando\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [DescribeAutomationStepExecutions](#) in AWS CLI Command Reference.

PowerShell

Strumenti per PowerShell V4

Esempio 1: questo esempio visualizza le informazioni relative a tutte le esecuzioni della fase attive e terminate in un flusso di lavoro di automazione.

```
Get-SSMAutomationStepExecution -AutomationExecutionId e1d2bad3-4567-8901-ae23-456c7c8901be | Select-Object StepName, Action, StepStatus
```

Output:

StepName	Action	StepStatus
-----	-----	-----
LaunchInstance	aws:runInstances	Success
OSCompatibilityCheck	aws:runCommand	Success
RunPreUpdateScript	aws:runCommand	Success
UpdateEC2Config	aws:runCommand	Cancelled
UpdateSSMAgent	aws:runCommand	Pending
UpdateAWSPVDriver	aws:runCommand	Pending
UpdateAWSEnaNetworkDriver	aws:runCommand	Pending
UpdateAWSNVMe	aws:runCommand	Pending
InstallWindowsUpdates	aws:runCommand	Pending
RunPostUpdateScript	aws:runCommand	Pending
RunSysprepGeneralize	aws:runCommand	Pending
StopInstance	aws:changeInstanceState	Pending
CreateImage	aws:createImage	Pending
TerminateInstance	aws:changeInstanceState	Pending

- Per i dettagli sull'API, vedere [DescribeAutomationStepExecutions](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: questo esempio visualizza le informazioni relative a tutte le esecuzioni della fase attive e terminate in un flusso di lavoro di automazione.

```
Get-SSMAutomationStepExecution -AutomationExecutionId e1d2bad3-4567-8901-ae23-456c7c8901be | Select-Object StepName, Action, StepStatus
```

Output:

StepName	Action	StepStatus
-----	-----	-----
LaunchInstance	aws:runInstances	Success
OSCompatibilityCheck	aws:runCommand	Success
RunPreUpdateScript	aws:runCommand	Success
UpdateEC2Config	aws:runCommand	Cancelled
UpdateSSMAgent	aws:runCommand	Pending
UpdateAWSPVDriver	aws:runCommand	Pending
UpdateAWSEnaNetworkDriver	aws:runCommand	Pending
UpdateAWSNVMe	aws:runCommand	Pending
InstallWindowsUpdates	aws:runCommand	Pending
RunPostUpdateScript	aws:runCommand	Pending
RunSysprepGeneralize	aws:runCommand	Pending
StopInstance	aws:changeInstanceState	Pending
CreateImage	aws:createImage	Pending
TerminateInstance	aws:changeInstanceState	Pending

- Per i dettagli sull'API, vedere [DescribeAutomationStepExecutions](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeAvailablePatches** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeAvailablePatches`.

### CLI

#### AWS CLI

Per ottenere le patch disponibili

L'esempio seguente `describe-available-patches` recupera i dettagli su tutte le patch disponibili per Windows Server 2019 che hanno una gravità MSRC pari a Critical.

```
aws ssm describe-available-patches \
 --
 filters "Key=PRODUCT,Values=WindowsServer2019" "Key=MSRC_SEVERITY,Values=Critical"
```



## Output:

```
{
 "Patches": [
 {
 "Id": "fe6bd8c2-3752-4c8b-ab3e-1a7ed08767ba",
 "ReleaseDate": 1544047205.0,
 "Title": "2018-11 Update for Windows Server 2019 for x64-based Systems (KB4470788)",
 "Description": "Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.",
 "ContentUrl": "https://support.microsoft.com/en-us/kb/4470788",
 "Vendor": "Microsoft",
 "ProductFamily": "Windows",
 "Product": "WindowsServer2019",
 "Classification": "SecurityUpdates",
 "MsrcSeverity": "Critical",
 "KbNumber": "KB4470788",
 "MsrcNumber": "",
 "Language": "All"
 },
 {
 "Id": "c96115e1-5587-4115-b851-22baa46a3f11",
 "ReleaseDate": 1549994410.0,
 "Title": "2019-02 Security Update for Adobe Flash Player for Windows Server 2019 for x64-based Systems (KB4487038)",
 "Description": "A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.",
 "ContentUrl": "https://support.microsoft.com/en-us/kb/4487038",
 "Vendor": "Microsoft",
 "ProductFamily": "Windows",
 "Product": "WindowsServer2019",
 "Classification": "SecurityUpdates",
 "MsrcSeverity": "Critical",
 "KbNumber": "KB4487038",
 "MsrcNumber": "",
 "Language": "All"
 },
 ...
]
}
```

```
]
}
```

Come ottenere i dettagli di una patch specifica

L'esempio seguente `describe-available-patches` recupera i dettagli per la patch specificata.

```
aws ssm describe-available-patches \
 --filters "Key=PATCH_ID,Values=KB4480979"
```

Output:

```
{
 "Patches": [
 {
 "Id": "680861e3-fb75-432e-818e-d72e5f2be719",
 "ReleaseDate": 1546970408.0,
 "Title": "2019-01 Security Update for Adobe Flash Player for Windows Server 2016 for x64-based Systems (KB4480979)",
 "Description": "A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article. After you install this update, you may have to restart your system.",
 "ContentUrl": "https://support.microsoft.com/en-us/kb/4480979",
 "Vendor": "Microsoft",
 "ProductFamily": "Windows",
 "Product": "WindowsServer2016",
 "Classification": "SecurityUpdates",
 "MsrcSeverity": "Critical",
 "KbNumber": "KB4480979",
 "MsrcNumber": "",
 "Language": "All"
 }
]
}
```

Per ulteriori informazioni, consulta [Come funzionano le operazioni di Patch Manager](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [DescribeAvailablePatches](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio fa ottenere tutte le patch per Windows Server 2012 che presentano una gravità MSRC pari a Critica. La sintassi utilizzata da questo esempio richiede la PowerShell versione 3 o successiva.

```
$filter1 = @{{Key="PRODUCT";Values=@("WindowsServer2012")}}
$filter2 = @{{Key="MSRC_SEVERITY";Values=@("Critical")}}

Get-SSMAvailablePatch -Filter $filter1,$filter2
```

#### Output:

```
Classification : SecurityUpdates
ContentUrl : https://support.microsoft.com/en-us/kb/2727528
Description : A security issue has been identified that could allow an
 unauthenticated remote attacker to compromise your system and gain control
 over it. You can help protect your system by installing this
 update from Microsoft. After you install this update, you may have to
 restart your system.
Id : 1eb507be-2040-4eeb-803d-abc55700b715
KbNumber : KB2727528
Language : All
MsrcNumber : MS12-072
MsrcSeverity : Critical
Product : WindowsServer2012
ProductFamily : Windows
ReleaseDate : 11/13/2012 6:00:00 PM
Title : Security Update for Windows Server 2012 (KB2727528)
Vendor : Microsoft
...
```

Esempio 2: con PowerShell la versione 2, è necessario utilizzare New-Object per creare ciascun filtro.

```
$filter1 = New-Object
 Amazon.SimpleSystemsManagement.Model.PatchOrchestratorFilter
$filter1.Key = "PRODUCT"
$filter1.Values = "WindowsServer2012"
```

```
$filter2 = New-Object
Amazon.SimpleSystemsManagement.Model.PatchOrchestratorFilter
$filter2.Key = "MSRC_SEVERITY"
$filter2.Values = "Critical"

Get-SSMAvailablePatch -Filter $filter1,$filter2
```

Esempio 3: questo esempio recupera tutti gli aggiornamenti rilasciati negli ultimi 20 giorni e applicabili ai prodotti corrispondenti WindowsServer al 2019

```
Get-SSMAvailablePatch | Where-Object ReleaseDate -ge (Get-Date).AddDays(-20)
| Where-Object Product -eq "WindowsServer2019" | Select-Object ReleaseDate,
Product, Title
```

Output:

ReleaseDate	Product	Title
4/9/2019 5:00:12 PM	WindowsServer2019	2019-04 Security Update for Adobe Flash Player for Windows Server 2019 for x64-based Systems (KB4493478)
4/9/2019 5:00:06 PM	WindowsServer2019	2019-04 Cumulative Update for Windows Server 2019 for x64-based Systems (KB4493509)
4/2/2019 5:00:06 PM	WindowsServer2019	2019-03 Servicing Stack Update for Windows Server 2019 for x64-based Systems (KB4493510)

- Per i dettagli sull'API, vedere [DescribeAvailablePatches](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio fa ottenere tutte le patch per Windows Server 2012 che presentano una gravità MSRC pari a Critica. La sintassi utilizzata da questo esempio richiede la PowerShell versione 3 o successiva.

```
$filter1 = @{Key="PRODUCT";Values=@("WindowsServer2012") }
$filter2 = @{Key="MSRC_SEVERITY";Values=@("Critical") }

Get-SSMAvailablePatch -Filter $filter1,$filter2
```

Output:

```
Classification : SecurityUpdates
```

```

ContentUrl : https://support.microsoft.com/en-us/kb/2727528
Description : A security issue has been identified that could allow an
 unauthenticated remote attacker to compromise your system and gain control
 over it. You can help protect your system by installing this
 update from Microsoft. After you install this update, you may have to
 restart your system.
Id : 1eb507be-2040-4eeb-803d-abc55700b715
KbNumber : KB2727528
Language : All
MsrcNumber : MS12-072
MsrcSeverity : Critical
Product : WindowsServer2012
ProductFamily : Windows
ReleaseDate : 11/13/2012 6:00:00 PM
Title : Security Update for Windows Server 2012 (KB2727528)
Vendor : Microsoft
...

```

Esempio 2: con PowerShell la versione 2, è necessario utilizzare New-Object per creare ciascun filtro.

```

$filter1 = New-Object
 Amazon.SimpleSystemsManagement.Model.PatchOrchestratorFilter
$filter1.Key = "PRODUCT"
$filter1.Values = "WindowsServer2012"
$filter2 = New-Object
 Amazon.SimpleSystemsManagement.Model.PatchOrchestratorFilter
$filter2.Key = "MSRC_SEVERITY"
$filter2.Values = "Critical"

Get-SSMAvailablePatch -Filter $filter1,$filter2

```

Esempio 3: questo esempio recupera tutti gli aggiornamenti rilasciati negli ultimi 20 giorni e applicabili ai prodotti corrispondenti WindowsServer al 2019

```

Get-SSMAvailablePatch | Where-Object ReleaseDate -ge (Get-Date).AddDays(-20)
| Where-Object Product -eq "WindowsServer2019" | Select-Object ReleaseDate,
 Product, Title

```

Output:

ReleaseDate	Product	Title
-------------	---------	-------

```

4/9/2019 5:00:12 PM WindowsServer2019 2019-04 Security Update for Adobe Flash
Player for Windows Server 2019 for x64-based Systems (KB4493478)
4/9/2019 5:00:06 PM WindowsServer2019 2019-04 Cumulative Update for Windows
Server 2019 for x64-based Systems (KB4493509)
4/2/2019 5:00:06 PM WindowsServer2019 2019-03 Servicing Stack Update for Windows
Server 2019 for x64-based Systems (KB4493510)

```

- Per i dettagli sull'API, vedere [DescribeAvailablePatches](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Usare **DescribeDocument** con un AWS SDK o CLI

I seguenti esempi di codice mostrano come usare `DescribeDocument`.

### CLI

#### AWS CLI

Per visualizzare i dettagli di un documento

L'`describe-document` seguente visualizza i dettagli su un documento di Systems Manager presente nell'AWS account.

```
aws ssm describe-document \
 --name "Example"
```

Output:

```
{
 "Document": {
 "Hash":
 "fc2410281f40779e694a8b95975d0f9f316da8a153daa94e3d9921102EXAMPLE",
 "HashType": "Sha256",
 "Name": "Example",
 "Owner": "29884EXAMPLE",
 "CreateDate": 1583257938.266,
 "Status": "Active",
 }
}
```

```
"DocumentVersion": "1",
"Description": "Document Example",
"Parameters": [
 {
 "Name": "AutomationAssumeRole",
 "Type": "String",
 "Description": "(Required) The ARN of the role that allows
Automation to perform the actions on your behalf. If no role is specified,
Systems Manager Automation uses your IAM permissions to execute this document.",
 "DefaultValue": ""
 },
 {
 "Name": "InstanceId",
 "Type": "String",
 "Description": "(Required) The ID of the Amazon EC2 instance.",
 "DefaultValue": ""
 }
],
"PlatformTypes": [
 "Windows",
 "Linux"
],
"DocumentType": "Automation",
"SchemaVersion": "0.3",
"LatestVersion": "1",
"DefaultVersion": "1",
"DocumentFormat": "YAML",
"Tags": []
}
```

Per ulteriori informazioni, consulta [Creazione di documenti di Systems Manager](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [DescribeDocument](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio restituisce informazioni su un documento.

```
Get-SSMDocumentDescription -Name "RunShellScript"
```

**Output:**

```
CreateDate : 2/24/2017 5:25:13 AM
DefaultVersion : 1
Description : Run an updated script
DocumentType : Command
DocumentVersion : 1
Hash :
 f775e5df4904c6fa46686c4722fae9de1950dace25cd9608ff8d622046b68d9b
HashType : Sha256
LatestVersion : 1
Name : RunShellScript
Owner : 123456789012
Parameters : {commands}
PlatformTypes : {Linux}
SchemaVersion : 2.0
Sha1 :
Status : Active
```

- Per i dettagli sull'API, vedere [DescribeDocument](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

**Strumenti per V5 PowerShell**

Esempio 1: questo esempio restituisce informazioni su un documento.

```
Get-SSMDocumentDescription -Name "RunShellScript"
```

**Output:**

```
CreateDate : 2/24/2017 5:25:13 AM
DefaultVersion : 1
Description : Run an updated script
DocumentType : Command
DocumentVersion : 1
Hash :
 f775e5df4904c6fa46686c4722fae9de1950dace25cd9608ff8d622046b68d9b
HashType : Sha256
LatestVersion : 1
Name : RunShellScript
Owner : 123456789012
Parameters : {commands}
PlatformTypes : {Linux}
```



```
SchemaVersion : 2.0
Sha1 :
Status : Active
```

- Per i dettagli sull'API, vedere [DescribeDocument](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

## SAP ABAP

### SDK per SAP ABAP

#### Note

C'è altro su GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
TRY.
 DATA(lo_result) = lo_ssm->describedocument(iv_name = iv_name).
 DATA(lo_document) = lo_result->get_document().
 IF lo_document IS BOUND.
 rv_status = lo_document->get_status().
 MESSAGE |Document status: { rv_status }| TYPE 'I'.
 ENDIF.
 CATCH /aws1/cx_ssminvaliddocument.
 MESSAGE 'Invalid document.' TYPE 'I'.
 ENDTRY.
```

- Per i dettagli sulle API, consulta [DescribeDocument](#) la sezione AWS SDK for SAP ABAP API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeDocumentPermission** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeDocumentPermission`.

## CLI

### AWS CLI

Per descrivere le autorizzazioni dei documenti

L'esempio seguente `describe-document-permission` visualizza i dettagli delle autorizzazioni relative a un documento Systems Manager condiviso pubblicamente.

```
aws ssm describe-document-permission \
 --name "Example" \
 --permission-type "Share"
```

Output:

```
{
 "AccountIds": [
 "all"
],
 "AccountSharingInfoList": [
 {
 "AccountId": "all",
 "SharedDocumentVersion": "$DEFAULT"
 }
]
}
```

Per ulteriori informazioni, consulta [Condividere un documento Systems Manager](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [DescribeDocumentPermission](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca tutte le versioni di un documento.

```
Get-SSMDocumentVersionList -Name "RunShellScript"
```

Output:

CreatedDate	DocumentVersion	IsDefaultVersion	Name
-----	-----	-----	----
2/24/2017 5:25:13 AM	1	True	RunShellScript

- Per i dettagli sull'API, vedere [DescribeDocumentPermission](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca tutte le versioni di un documento.

```
Get-SSMDocumentVersionList -Name "RunShellScript"
```

Output:

CreatedDate	DocumentVersion	IsDefaultVersion	Name
-----	-----	-----	----
2/24/2017 5:25:13 AM	1	True	RunShellScript

- Per i dettagli sull'API, vedere [DescribeDocumentPermission](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeEffectiveInstanceAssociations** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeEffectiveInstanceAssociations`.

### CLI

#### AWS CLI

Per ottenere dettagli sulle associazioni efficaci per un'istanza

L'esempio seguente `describe-effective-instance-associations` recupera i dettagli sulle associazioni efficaci per un'istanza.

Comando:

```
aws ssm describe-effective-instance-associations --instance-id "i-1234567890abcdef0"
```

Output:

```
{
 "Associations": [
 {
 "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
 "InstanceId": "i-1234567890abcdef0",
 "Content": "{\n \"schemaVersion\": \"1.2\",\n \"description\":\n \"Update the Amazon SSM Agent to the latest version or specified version.\",\n \"parameters\": {\n \"version\": {\n \"default\": \"\",\n \"description\": \"(Optional) A specific version of the Amazon SSM Agent\n to install. If not specified, the agent will be updated to the latest version.\",\n \"type\": \"String\"\n },\n \"allowDowngrade\": {\n \"default\": \"false\",\n \"description\": \"(Optional) Allow the Amazon SSM Agent service to be downgraded to an earlier\n version. If set to false, the service can be upgraded to newer versions only\n (default). If set to true, specify the earlier version.\",\n \"type\": \"String\",\n \"allowedValues\": [\n \"true\",\n \"false\"\n]\n },\n \"runtimeConfig\": {\n \"aws:updateSsmAgent\": {\n \"properties\": [\n {\n \"agentName\": \"amazon-ssm-agent\",\n \"source\": \"https://s3.{Region}.amazonaws.com/amazon-ssm-{Region}/ssm-agent-manifest.json\",\n \"allowDowngrade\": \"${ allowDowngrade }\",\n \"targetVersion\": \"${ version }\"\n }\n]\n }\n }\n }\n}"
 "AssociationVersion": "1"
 }
]
}
```

- Per i dettagli sull'API, vedi [DescribeEffectiveInstanceAssociations](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio descrive le associazioni efficaci per un'istanza.

```
Get-SSMEffectiveInstanceAssociationList -InstanceId "i-0000293ffd8c57862" -
MaxResult 5
```

Output:

AssociationId	Content
-----	-----
d8617c07-2079-4c18-9847-1655fc2698b0	{...

Esempio 2: questo esempio visualizza il contenuto delle associazioni efficaci per un'istanza.

```
(Get-SSMEffectiveInstanceAssociationList -InstanceId "i-0000293ffd8c57862" -
MaxResult 5).Content
```

Output:

```
{
 "schemaVersion": "1.2",
 "description": "Update the Amazon SSM Agent to the latest version or
specified version.",
 "parameters": {
 "version": {
 "default": "",
 "description": "(Optional) A specific version of the Amazon SSM Agent
to install. If not specified, the agen
t will be updated to the latest version.",
 "type": "String"
 },
 "allowDowngrade": {
 "default": "false",
 "description": "(Optional) Allow the Amazon SSM Agent service to be
downgraded to an earlier version. If set
to false, the service can be upgraded to newer versions only (default). If set
to true, specify the earlier version.",
 "type": "String",
 "allowedValues": [
 "true",
 "false"
]
 }
 }
},
```

```

 "runtimeConfig": {
 "aws:updateSsmAgent": {
 "properties": [
 {
 "agentName": "amazon-ssm-agent",
 "source": "https://s3.{Region}.amazonaws.com/amazon-ssm-{Region}/ssm-agent-manifest.json",
 "allowDowngrade": "{{ allowDowngrade }}",
 "targetVersion": "{{ version }}"
 }
]
 }
 }
 }
}

```

- Per i dettagli sull'API, vedere [DescribeEffectiveInstanceAssociations](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio descrive le associazioni efficaci per un'istanza.

```
Get-SSMEffectiveInstanceAssociationList -InstanceId "i-0000293ffd8c57862" -
MaxResult 5
```

Output:

AssociationId	Content
-----	-----
d8617c07-2079-4c18-9847-1655fc2698b0	{...

Esempio 2: questo esempio visualizza il contenuto delle associazioni efficaci per un'istanza.

```
(Get-SSMEffectiveInstanceAssociationList -InstanceId "i-0000293ffd8c57862" -
MaxResult 5).Content
```

Output:

```

{
 "schemaVersion": "1.2",
 "description": "Update the Amazon SSM Agent to the latest version or
specified version.",

```

```

 "parameters": {
 "version": {
 "default": "",
 "description": "(Optional) A specific version of the Amazon SSM Agent
to install. If not specified, the agen
t will be updated to the latest version.",
 "type": "String"
 },
 "allowDowngrade": {
 "default": "false",
 "description": "(Optional) Allow the Amazon SSM Agent service to be
downgraded to an earlier version. If set
to false, the service can be upgraded to newer versions only (default). If set
to true, specify the earlier version.",
 "type": "String",
 "allowedValues": [
 "true",
 "false"
]
 }
 },
 "runtimeConfig": {
 "aws:updateSsmAgent": {
 "properties": [
 {
 "agentName": "amazon-ssm-agent",
 "source": "https://s3.{Region}.amazonaws.com/amazon-ssm-{Region}/
ssm-agent-manifest.json",
 "allowDowngrade": "{{ allowDowngrade }}",
 "targetVersion": "{{ version }}"
 }
]
 }
 }
 }
}

```

- Per i dettagli sull'API, vedere [DescribeEffectiveInstanceAssociations](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di `DescribeEffectivePatchesForPatchBaseline` con una CLI

I seguenti esempi di codice mostrano come usare `DescribeEffectivePatchesForPatchBaseline`.

### CLI

#### AWS CLI

Esempio 1: ottenimento di tutte le patch definite da una baseline delle patch

L' `describe-effective-patches-for-patch-baseline` seguente restituisce le patch definite da una baseline di patch personalizzata nell'account corrente. AWS Si noti che per una baseline personalizzata, è richiesto solo l'ID per `--baseline-id`.

```
aws ssm describe-effective-patches-for-patch-baseline \
 --baseline-id "pb-08b654cf9b9681f04"
```

Output:

```
{
 "EffectivePatches": [
 {
 "Patch": {
 "Id": "fe6bd8c2-3752-4c8b-ab3e-1a7ed08767ba",
 "ReleaseDate": 1544047205.0,
 "Title": "2018-11 Update for Windows Server 2019 for x64-based Systems (KB4470788)",
 "Description": "Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.",
 "ContentUrl": "https://support.microsoft.com/en-us/kb/4470788",
 "Vendor": "Microsoft",
 "ProductFamily": "Windows",
 "Product": "WindowsServer2019",
 "Classification": "SecurityUpdates",
 "MsrcSeverity": "Critical",
 "KbNumber": "KB4470788",
 "MsrcNumber": "",
 "Language": "All"
 },
 "PatchStatus": {
```



```

 "DeploymentStatus": "APPROVED",
 "ComplianceLevel": "CRITICAL",
 "ApprovalDate": 1544047205.0
 },
 {
 "Patch": {
 "Id": "915a6b1a-f556-4d83-8f50-b2e75a9a7e58",
 "ReleaseDate": 1549994400.0,
 "Title": "2019-02 Cumulative Update for .NET Framework 3.5 and
4.7.2 for Windows Server 2019 for x64 (KB4483452)",
 "Description": "A security issue has been identified in a
Microsoft software product that could affect your system. You can help protect
your system by installing this update from Microsoft. For a complete listing
of the issues that are included in this update, see the associated Microsoft
Knowledge Base article. After you install this update, you may have to restart
your system.",
 "ContentUrl": "https://support.microsoft.com/en-us/kb/4483452",
 "Vendor": "Microsoft",
 "ProductFamily": "Windows",
 "Product": "WindowsServer2019",
 "Classification": "SecurityUpdates",
 "MsrcSeverity": "Important",
 "KbNumber": "KB4483452",
 "MsrcNumber": "",
 "Language": "All"
 },
 "PatchStatus": {
 "DeploymentStatus": "APPROVED",
 "ComplianceLevel": "CRITICAL",
 "ApprovalDate": 1549994400.0
 }
 },
 ...
],
"NextToken": "--token string truncated--"
}

```

Esempio 2: per ottenere tutte le patch definite da una AWS baseline di patch gestita

L'azione `describe-effective-patches-for-patch-baseline` seguente restituisce le patch definite da una baseline di patch AWS gestita. Si noti che per una baseline AWS gestita, è necessario l'ARN di base completo per `--baseline-id`

```
aws ssm describe-effective-patches-for-patch-baseline \
 --baseline-id "arn:aws:ssm:us-east-2:733109147000:patchbaseline/
pb-020d361a05defe4ed"
```

Vedi l'esempio 1 per un output di esempio.

Per ulteriori informazioni, consulta [Come vengono selezionate le patch di sicurezza](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, consulta la sezione Command [DescribeEffectivePatchesForPatchBaseline](#) Reference AWS CLI .

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca tutte le baseline delle patch, con un elenco di risultati massimo di 1.

```
Get-SSMEffectivePatchesForPatchBaseline -BaselineId "pb-0a2f1059b670ebd31" -
MaxResult 1
```

Output:

Patch	PatchStatus
-----	-----
Amazon.SimpleSystemsManagement.Model.Patch	
Amazon.SimpleSystemsManagement.Model.PatchStatus	

Esempio 2: questo esempio visualizza lo stato delle patch per tutte le baseline delle patch, con un elenco di risultati massimo di 1.

```
(Get-SSMEffectivePatchesForPatchBaseline -BaselineId "pb-0a2f1059b670ebd31" -
MaxResult 1).PatchStatus
```

Output:

ApprovalDate	DeploymentStatus
-----	-----

```
12/21/2010 6:00:00 PM APPROVED
```

- Per i dettagli sull'API, vedere [DescribeEffectivePatchesForPatchBaseline](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca tutte le baseline delle patch, con un elenco di risultati massimo di 1.

```
Get-SSMEffectivePatchesForPatchBaseline -BaselineId "pb-0a2f1059b670ebd31" -
MaxResult 1
```

Output:

Patch	PatchStatus
-----	-----
Amazon.SimpleSystemsManagement.Model.Patch	
Amazon.SimpleSystemsManagement.Model.PatchStatus	

Esempio 2: questo esempio visualizza lo stato delle patch per tutte baseline delle patch, con un elenco di risultati massimo di 1.

```
(Get-SSMEffectivePatchesForPatchBaseline -BaselineId "pb-0a2f1059b670ebd31" -
MaxResult 1).PatchStatus
```

Output:

ApprovalDate	DeploymentStatus
-----	-----
12/21/2010 6:00:00 PM	APPROVED

- Per i dettagli sull'API, vedere [DescribeEffectivePatchesForPatchBaseline](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeInstanceAssociationsStatus** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeInstanceAssociationsStatus`.

### CLI

#### AWS CLI

Per descrivere lo stato delle associazioni delle istanze

Questo esempio mostra i dettagli delle associazioni per un'istanza.

Comando:

```
aws ssm describe-instance-associations-status --instance-id "i-1234567890abcdef0"
```

Output:

```
{
 "InstanceAssociationStatusInfos": [
 {
 "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
 "Name": "AWS-GatherSoftwareInventory",
 "DocumentVersion": "1",
 "AssociationVersion": "1",
 "InstanceId": "i-1234567890abcdef0",
 "ExecutionDate": 1550501886.0,
 "Status": "Success",
 "ExecutionSummary": "1 out of 1 plugin processed, 1 success, 0 failed,
0 timedout, 0 skipped. ",
 "AssociationName": "Inventory-Association"
 },
 {
 "AssociationId": "5c5a31f6-6dae-46f9-944c-0123456789ab",
 "Name": "AWS-UpdateSSMAgent",
 "DocumentVersion": "1",
 "AssociationVersion": "1",
 "InstanceId": "i-1234567890abcdef0",
 "ExecutionDate": 1550505828.548,
 "Status": "Success",
 "DetailedStatus": "Success",
 "AssociationName": "UpdateSSMAgent"
 }
]
}
```

```
]
}
```

- Per i dettagli sull'API, vedi [DescribeInstanceAssociationsStatus](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio mostra i dettagli delle associazioni per un'istanza.

```
Get-SSMInstanceAssociationsStatus -InstanceId "i-0000293ffd8c57862"
```

Output:

```
AssociationId : d8617c07-2079-4c18-9847-1655fc2698b0
DetailedStatus : Pending
DocumentVersion : 1
ErrorCode :
ExecutionDate : 2/20/2015 8:31:11 AM
ExecutionSummary : temp_status_change
InstanceId : i-0000293ffd8c57862
Name : AWS-UpdateSSMAgent
OutputUrl :
Status : Pending
```

Esempio 2: questo esempio controlla lo stato di associazione delle istanze per l'ID di istanza specificato e inoltre visualizza lo stato di esecuzione di tali associazioni

```
Get-SSMInstanceAssociationsStatus -InstanceId i-012e3cb4df567e8aa | ForEach-Object {Get-SSMAssociationExecution -AssociationId .AssociationId}
```

Output:

```
AssociationId : 512a34a5-c678-1234-1234-12345678db9e
AssociationVersion : 2
CreatedTime : 3/2/2019 8:53:29 AM
DetailedStatus :
ExecutionId : 512a34a5-c678-1234-1234-12345678db9e
LastExecutionDate : 1/1/0001 12:00:00 AM
```

```
ResourceCountByStatus : {Success=9}
Status : Success
```

- Per i dettagli sull'API, vedere [DescribeInstanceAssociationsStatus](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio mostra i dettagli delle associazioni per un'istanza.

```
Get-SSMInstanceAssociationsStatus -InstanceId "i-0000293ffd8c57862"
```

### Output:

```
AssociationId : d8617c07-2079-4c18-9847-1655fc2698b0
DetailedStatus : Pending
DocumentVersion : 1
ErrorCode :
ExecutionDate : 2/20/2015 8:31:11 AM
ExecutionSummary : temp_status_change
InstanceId : i-0000293ffd8c57862
Name : AWS-UpdateSSMAgent
OutputUrl :
Status : Pending
```

Esempio 2: questo esempio controlla lo stato di associazione delle istanze per l'ID di istanza specificato e inoltre visualizza lo stato di esecuzione di tali associazioni

```
Get-SSMInstanceAssociationsStatus -InstanceId i-012e3cb4df567e8aa | ForEach-Object {Get-SSMAssociationExecution -AssociationId .AssociationId}
```

### Output:

```
AssociationId : 512a34a5-c678-1234-1234-12345678db9e
AssociationVersion : 2
CreatedTime : 3/2/2019 8:53:29 AM
DetailedStatus :
ExecutionId : 512a34a5-c678-1234-1234-12345678db9e
LastExecutionDate : 1/1/0001 12:00:00 AM
ResourceCountByStatus : {Success=9}
Status : Success
```

- Per i dettagli sull'API, vedere [DescribeInstanceAssociationsStatus](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeInstanceInformation** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeInstanceInformation`.

### CLI

#### AWS CLI

Esempio 1: per descrivere le informazioni sulle istanze gestite

L'esempio seguente `describe-instance-information` recupera i dettagli di ciascuna delle istanze gestite.

```
aws ssm describe-instance-information
```

Esempio 2: come descrivere le informazioni su una specifica istanza gestita

L'esempio seguente `describe-instance-information` mostra i dettagli dell'istanza gestita `i-028ea792daEXAMPLE`.

```
aws ssm describe-instance-information \
 --filters "Key=InstanceIds,Values=i-028ea792daEXAMPLE"
```

Esempio 3: come descrivere le informazioni sulle istanze gestite con una chiave tag specifica

L'esempio seguente `describe-instance-information` mostra i dettagli delle istanze gestite con la chiave tag `DEV`.

```
aws ssm describe-instance-information \
 --filters "Key=tag-key,Values=DEV"
```

Output:

```
{
```

```
"InstanceInformationList": [
 {
 "InstanceId": "i-028ea792daEXAMPLE",
 "PingStatus": "Online",
 "LastPingDateTime": 1582221233.421,
 "AgentVersion": "2.3.842.0",
 "IsLatestVersion": true,
 "PlatformType": "Linux",
 "PlatformName": "SLES",
 "PlatformVersion": "15.1",
 "ResourceType": "EC2Instance",
 "IPAddress": "192.0.2.0",
 "ComputerName": "ip-198.51.100.0.us-east-2.compute.internal",
 "AssociationStatus": "Success",
 "LastAssociationExecutionDate": 1582220806.0,
 "LastSuccessfulAssociationExecutionDate": 1582220806.0,
 "AssociationOverview": {
 "DetailedStatus": "Success",
 "InstanceAssociationStatusAggregatedCount": {
 "Success": 2
 }
 }
 }
]
```

Per ulteriori informazioni, consulta [Istanze gestite](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [DescribeInstanceInformation](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio mostra i dettagli di ciascuna istanza.

```
Get-SSMInstanceInformation
```

Output:

```
ActivationId :
```



```

AgentVersion : 2.0.672.0
AssociationOverview :
 Amazon.SimpleSystemsManagement.Model.InstanceAggregatedAssociationOverview
AssociationStatus : Success
ComputerName : ip-172-31-44-222.us-
west-2.compute.internal
IamRole :
InstanceId : i-0cb2b964d3e14fd9f
IPAddress : 172.31.44.222
IsLatestVersion : True
LastAssociationExecutionDate : 2/24/2017 3:18:09 AM
LastPingDateTime : 2/24/2017 3:35:03 AM
LastSuccessfulAssociationExecutionDate : 2/24/2017 3:18:09 AM
Name :
PingStatus : ConnectionLost
PlatformName : Amazon Linux AMI
PlatformType : Linux
PlatformVersion : 2016.09
RegistrationDate : 1/1/0001 12:00:00 AM
ResourceType : EC2Instance

```

Esempio 2: questo esempio mostra come utilizzare il parametro `-Filter` per filtrare i risultati solo in base alle istanze di AWS Systems Manager nella regione **us-east-1** con un **of. AgentVersion 2.2.800.0** Puoi trovare un elenco di valori di chiave `-Filter` validi nell'argomento di riferimento dell' InstanceInformation API ([https://docs.aws.amazon.com/systems-manager/latest/APIReference/API\\_InstanceInformation.html#systemsmanager-Type-InstanceInformation-ActivationId](https://docs.aws.amazon.com/systems-manager/latest/APIReference/API_InstanceInformation.html#systemsmanager-Type-InstanceInformation-ActivationId)).

```

$Filters = @{
 Key="AgentVersion"
 Values="2.2.800.0"
}
Get-SSMInstanceInformation -Region us-east-1 -Filter $Filters

```

Output:

```

ActivationId :
AgentVersion : 2.2.800.0
AssociationOverview :
 Amazon.SimpleSystemsManagement.Model.InstanceAggregatedAssociationOverview
AssociationStatus : Success
ComputerName : EXAMPLE-EXAMPLE.WORKGROUP

```

```

IamRole :
InstanceId : i-EXAMPLEb0792d98ce
IPAddress : 10.0.0.01
IsLatestVersion : False
LastAssociationExecutionDate : 8/16/2018 12:02:50 AM
LastPingDateTime : 8/16/2018 7:40:27 PM
LastSuccessfulAssociationExecutionDate : 8/16/2018 12:02:50 AM
Name :
PingStatus : Online
PlatformName : Microsoft Windows Server 2016 Datacenter
PlatformType : Windows
PlatformVersion : 10.0.14393
RegistrationDate : 1/1/0001 12:00:00 AM
ResourceType : EC2Instance

ActivationId :
AgentVersion : 2.2.800.0
AssociationOverview :
 Amazon.SimpleSystemsManagement.Model.InstanceAggregatedAssociationOverview
AssociationStatus : Success
ComputerName : EXAMPLE-EXAMPLE.WORKGROUP
IamRole :
InstanceId : i-EXAMPLEac7501d023
IPAddress : 10.0.0.02
IsLatestVersion : False
LastAssociationExecutionDate : 8/16/2018 12:00:20 AM
LastPingDateTime : 8/16/2018 7:40:35 PM
LastSuccessfulAssociationExecutionDate : 8/16/2018 12:00:20 AM
Name :
PingStatus : Online
PlatformName : Microsoft Windows Server 2016 Datacenter
PlatformType : Windows
PlatformVersion : 10.0.14393
RegistrationDate : 1/1/0001 12:00:00 AM
ResourceType : EC2Instance

```

Esempio 3: questo esempio mostra come utilizzare il `InstanceInformationFilterList` parametro - per filtrare i risultati solo in base alle istanze **PlatformTypes** di AWS Systems Manager nella regione **us-east-1** con **Windows** o **Linux**. Puoi trovare un elenco di valori `InstanceInformationFilterList` chiave validi nell'argomento di riferimento dell' `InstanceInformationFilter` API ([https://docs.aws.amazon.com/systems-manager/latest/APIReference/API\\_InstanceInformationFilter.html](https://docs.aws.amazon.com/systems-manager/latest/APIReference/API_InstanceInformationFilter.html)).

```
$Filters = @{
 Key="PlatformTypes"
 ValueSet=("Windows","Linux")
}
Get-SSMInstanceInformation -Region us-east-1 -InstanceInformationFilterList
$Filters
```

## Output:

```
ActivationId :
AgentVersion : 2.2.800.0
AssociationOverview :
 Amazon.SimpleSystemsManagement.Model.InstanceAggregatedAssociationOverview
AssociationStatus : Success
ComputerName : EXAMPLE-EXAMPLE.WORKGROUP
IamRole :
InstanceId : i-EXAMPLEb0792d98ce
IPAddress : 10.0.0.27
IsLatestVersion : False
LastAssociationExecutionDate : 8/16/2018 12:02:50 AM
LastPingDateTime : 8/16/2018 7:40:27 PM
LastSuccessfulAssociationExecutionDate : 8/16/2018 12:02:50 AM
Name :
PingStatus : Online
PlatformName : Ubuntu Server 18.04 LTS
PlatformType : Linux
PlatformVersion : 18.04
RegistrationDate : 1/1/0001 12:00:00 AM
ResourceType : EC2Instance

ActivationId :
AgentVersion : 2.2.800.0
AssociationOverview :
 Amazon.SimpleSystemsManagement.Model.InstanceAggregatedAssociationOverview
AssociationStatus : Success
ComputerName : EXAMPLE-EXAMPLE.WORKGROUP
IamRole :
InstanceId : i-EXAMPLEac7501d023
IPAddress : 10.0.0.100
IsLatestVersion : False
LastAssociationExecutionDate : 8/16/2018 12:00:20 AM
LastPingDateTime : 8/16/2018 7:40:35 PM
LastSuccessfulAssociationExecutionDate : 8/16/2018 12:00:20 AM
```

```

Name :
PingStatus : Online
PlatformName : Microsoft Windows Server 2016 Datacenter
PlatformType : Windows
PlatformVersion : 10.0.14393
RegistrationDate : 1/1/0001 12:00:00 AM
ResourceType : EC2Instance

```

Esempio 4: questo esempio elenca le istanze e le esportazioni InstanceId gestite da ssm LastPingDateTime e PlatformName in un file csv. PingStatus

```

Get-SSMInstanceInformation | Select-Object InstanceId, PingStatus,
 LastPingDateTime, PlatformName | Export-Csv Instance-details.csv -
NoTypeInformation

```

- Per i dettagli sull'API, vedere [DescribeInstanceInformation](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio mostra i dettagli di ciascuna istanza.

```
Get-SSMInstanceInformation
```

Output:

```

ActivationId :
AgentVersion : 2.0.672.0
AssociationOverview :
 Amazon.SimpleSystemsManagement.Model.InstanceAggregatedAssociationOverview
AssociationStatus : Success
ComputerName : ip-172-31-44-222.us-
west-2.compute.internal
IamRole :
InstanceId : i-0cb2b964d3e14fd9f
IPAddress : 172.31.44.222
IsLatestVersion : True
LastAssociationExecutionDate : 2/24/2017 3:18:09 AM
LastPingDateTime : 2/24/2017 3:35:03 AM
LastSuccessfulAssociationExecutionDate : 2/24/2017 3:18:09 AM
Name :
PingStatus : ConnectionLost

```

```

PlatformName : Amazon Linux AMI
PlatformType : Linux
PlatformVersion : 2016.09
RegistrationDate : 1/1/0001 12:00:00 AM
ResourceType : EC2Instance

```

Esempio 2: questo esempio mostra come utilizzare il parametro `-Filter` per filtrare i risultati solo in base alle istanze di AWS Systems Manager nella regione **us-east-1** con un of. **AgentVersion 2.2.800.0** Puoi trovare un elenco di valori di chiave `-Filter` validi nell'argomento di riferimento dell' InstanceInformation API ([https://docs.aws.amazon.com/systems-manager/latest/APIReference/API\\_InstanceInformation.html#systemsmanager-Type-InstanceInformation-ActivationId](https://docs.aws.amazon.com/systems-manager/latest/APIReference/API_InstanceInformation.html#systemsmanager-Type-InstanceInformation-ActivationId)).

```

$Filters = @{
 Key="AgentVersion"
 Values="2.2.800.0"
}
Get-SSMInstanceInformation -Region us-east-1 -Filter $Filters

```

Output:

```

ActivationId :
AgentVersion : 2.2.800.0
AssociationOverview :
 Amazon.SimpleSystemsManagement.Model.InstanceAggregatedAssociationOverview
AssociationStatus : Success
ComputerName : EXAMPLE-EXAMPLE.WORKGROUP
IamRole :
InstanceId : i-EXAMPLEb0792d98ce
IPAddress : 10.0.0.01
IsLatestVersion : False
LastAssociationExecutionDate : 8/16/2018 12:02:50 AM
LastPingDateTime : 8/16/2018 7:40:27 PM
LastSuccessfulAssociationExecutionDate : 8/16/2018 12:02:50 AM
Name :
PingStatus : Online
PlatformName : Microsoft Windows Server 2016 Datacenter
PlatformType : Windows
PlatformVersion : 10.0.14393
RegistrationDate : 1/1/0001 12:00:00 AM
ResourceType : EC2Instance

```

```

ActivationId :
AgentVersion : 2.2.800.0
AssociationOverview :
 Amazon.SimpleSystemsManagement.Model.InstanceAggregatedAssociationOverview
AssociationStatus : Success
ComputerName : EXAMPLE-EXAMPLE.WORKGROUP
IamRole :
InstanceId : i-EXAMPLEac7501d023
IPAddress : 10.0.0.02
IsLatestVersion : False
LastAssociationExecutionDate : 8/16/2018 12:00:20 AM
LastPingDateTime : 8/16/2018 7:40:35 PM
LastSuccessfulAssociationExecutionDate : 8/16/2018 12:00:20 AM
Name :
PingStatus : Online
PlatformName : Microsoft Windows Server 2016 Datacenter
PlatformType : Windows
PlatformVersion : 10.0.14393
RegistrationDate : 1/1/0001 12:00:00 AM
ResourceType : EC2Instance

```

Esempio 3: questo esempio mostra come utilizzare il `InstanceInformationFilterList` parametro - per filtrare i risultati solo in base alle istanze **PlatformTypes** di AWS Systems Manager nella regione **us-east-1** con **Windows** o **Linux**. Puoi trovare un elenco di valori `InstanceInformationFilterList` chiave validi nell'argomento di riferimento dell' `InstanceInformationFilter` API ([https://docs.aws.amazon.com/systems-manager/latest/APIReference/API\\_InstanceInformationFilter.html](https://docs.aws.amazon.com/systems-manager/latest/APIReference/API_InstanceInformationFilter.html)).

```

$Filters = @{
 Key="PlatformTypes"
 ValueSet=("Windows","Linux")
}
Get-SSMInstanceInformation -Region us-east-1 -InstanceInformationFilterList
$Filters

```

Output:

```

ActivationId :
AgentVersion : 2.2.800.0
AssociationOverview :
 Amazon.SimpleSystemsManagement.Model.InstanceAggregatedAssociationOverview
AssociationStatus : Success

```

```

ComputerName : EXAMPLE-EXAMPLE.WORKGROUP
IamRole :
InstanceId : i-EXAMPLEb0792d98ce
IPAddress : 10.0.0.27
IsLatestVersion : False
LastAssociationExecutionDate : 8/16/2018 12:02:50 AM
LastPingDateTime : 8/16/2018 7:40:27 PM
LastSuccessfulAssociationExecutionDate : 8/16/2018 12:02:50 AM
Name :
PingStatus : Online
PlatformName : Ubuntu Server 18.04 LTS
PlatformType : Linux
PlatformVersion : 18.04
RegistrationDate : 1/1/0001 12:00:00 AM
ResourceType : EC2Instance

ActivationId :
AgentVersion : 2.2.800.0
AssociationOverview :
 Amazon.SimpleSystemsManagement.Model.InstanceAggregatedAssociationOverview
AssociationStatus : Success
ComputerName : EXAMPLE-EXAMPLE.WORKGROUP
IamRole :
InstanceId : i-EXAMPLEac7501d023
IPAddress : 10.0.0.100
IsLatestVersion : False
LastAssociationExecutionDate : 8/16/2018 12:00:20 AM
LastPingDateTime : 8/16/2018 7:40:35 PM
LastSuccessfulAssociationExecutionDate : 8/16/2018 12:00:20 AM
Name :
PingStatus : Online
PlatformName : Microsoft Windows Server 2016 Datacenter
PlatformType : Windows
PlatformVersion : 10.0.14393
RegistrationDate : 1/1/0001 12:00:00 AM
ResourceType : EC2Instance

```

Esempio 4: questo esempio elenca le istanze e le esportazioni InstanceId gestite da ssm LastPingDateTime e PlatformName in un file csv. PingStatus

```

Get-SSMInstanceInformation | Select-Object InstanceId, PingStatus,
 LastPingDateTime, PlatformName | Export-Csv Instance-details.csv -
NoTypeInformation

```

- Per i dettagli sull'API, vedere [DescribeInstanceInformation](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeInstancePatchStates** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeInstancePatchStates`.

### CLI

#### AWS CLI

Per ottenere gli stati di riepilogo delle patch per le istanze

Questo esempio `describe-instance-patch-states` viene recuperato lo stato del riepilogo della patch per un'istanza.

```
aws ssm describe-instance-patch-states \
 --instance-ids "i-1234567890abcdef0"
```

Output:

```
{
 "InstancePatchStates": [
 {
 "InstanceId": "i-1234567890abcdef0",
 "PatchGroup": "my-patch-group",
 "BaselineId": "pb-0713accee01234567",
 "SnapshotId": "521c3536-930c-4aa9-950e-01234567abcd",
 "CriticalNonCompliantCount": 2,
 "SecurityNonCompliantCount": 2,
 "OtherNonCompliantCount": 1,
 "InstalledCount": 123,
 "InstalledOtherCount": 334,
 "InstalledPendingRebootCount": 0,
 "InstalledRejectedCount": 0,
 "MissingCount": 1,
 "FailedCount": 2,
 "UnreportedNotApplicableCount": 11,
 }
]
}
```



```

 "NotApplicableCount": 2063,
 "OperationStartTime": "2021-05-03T11:00:56-07:00",
 "OperationEndTime": "2021-05-03T11:01:09-07:00",
 "Operation": "Scan",
 "LastNoRebootInstallOperationTime": "2020-06-14T12:17:41-07:00",
 "RebootOption": "RebootIfNeeded"
 }
]
}

```

Per ulteriori informazioni, consulta [Informazioni sulla conformità delle patch](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [DescribeInstancePatchStates](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio ottiene gli stati di riepilogo delle patch per un'istanza.

```
Get-SSMInstancePatchState -InstanceId "i-08ee91c0b17045407"
```

Esempio 2: questo esempio ottiene gli stati di riepilogo delle patch per due istanze.

```
Get-SSMInstancePatchState -InstanceId "i-08ee91c0b17045407","i-09a618aec652973a9"
```

- Per i dettagli sull'API, vedere [DescribeInstancePatchStates](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio ottiene gli stati di riepilogo delle patch per un'istanza.

```
Get-SSMInstancePatchState -InstanceId "i-08ee91c0b17045407"
```

Esempio 2: questo esempio ottiene gli stati di riepilogo delle patch per due istanze.

```
Get-SSMInstancePatchState -InstanceId "i-08ee91c0b17045407","i-09a618aec652973a9"
```

- Per i dettagli sull'API, vedere [DescribeInstancePatchStates](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeInstancePatchStatesForPatchGroup** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeInstancePatchStatesForPatchGroup`.

### CLI

#### AWS CLI

Esempio 1: per ottenere gli stati dell'istanza per un gruppo di patch

L'esempio seguente `describe-instance-patch-states-for-patch-group` recupera i dettagli sugli stati di riepilogo delle patch per istanza per il gruppo di patch specificato.

```
aws ssm describe-instance-patch-states-for-patch-group \
 --patch-group "Production"
```

Output:

```
{
 "InstancePatchStates": [
 {
 "InstanceId": "i-02573cafcfEXAMPLE",
 "PatchGroup": "Production",
 "BaselineId": "pb-0c10e65780EXAMPLE",
 "SnapshotId": "a3f5ff34-9bc4-4d2c-a665-4d1c1EXAMPLE",
 "OwnerInformation": "",
 "InstalledCount": 32,
 "InstalledOtherCount": 1,
 "InstalledPendingRebootCount": 0,
 "InstalledRejectedCount": 0,
 "MissingCount": 2,
 "FailedCount": 0,
 "UnreportedNotApplicableCount": 2671,
 "NotApplicableCount": 400,
 "OperationStartTime": "2021-08-04T11:03:50.590000-07:00",
 "OperationEndTime": "2021-08-04T11:04:21.555000-07:00",
 "Operation": "Scan",
 }
]
}
```

```

 "RebootOption": "NoReboot",
 "CriticalNonCompliantCount": 0,
 "SecurityNonCompliantCount": 1,
 "OtherNonCompliantCount": 0
 },
 {
 "InstanceId": "i-0471e04240EXAMPLE",
 "PatchGroup": "Production",
 "BaselineId": "pb-09ca3fb51fEXAMPLE",
 "SnapshotId": "05d8ffb0-1bbe-4812-ba2d-d9b7bEXAMPLE",
 "OwnerInformation": "",
 "InstalledCount": 32,
 "InstalledOtherCount": 1,
 "InstalledPendingRebootCount": 0,
 "InstalledRejectedCount": 0,
 "MissingCount": 2,
 "FailedCount": 0,
 "UnreportedNotApplicableCount": 2671,
 "NotApplicableCount": 400,
 "OperationStartTime": "2021-08-04T22:06:20.340000-07:00",
 "OperationEndTime": "2021-08-04T22:07:11.220000-07:00",
 "Operation": "Scan",
 "RebootOption": "NoReboot",
 "CriticalNonCompliantCount": 0,
 "SecurityNonCompliantCount": 1,
 "OtherNonCompliantCount": 0
 }
]
}

```

Esempio 2: come ottenere gli stati delle istanze per un gruppo di patch con più di cinque patch mancanti

L'esempio seguente `describe-instance-patch-states-for-patch-group` recupera i dettagli sugli stati di riepilogo delle patch per il gruppo di patch specificato per le istanze con più di cinque patch mancanti.

```

aws ssm describe-instance-patch-states-for-patch-group \
 --filters Key=MissingCount,Type=GreaterThan,Values=5 \
 --patch-group "Production"

```

Output:

```
{
 "InstancePatchStates": [
 {
 "InstanceId": "i-02573cafcfEXAMPLE",
 "PatchGroup": "Production",
 "BaselineId": "pb-0c10e65780EXAMPLE",
 "SnapshotId": "a3f5ff34-9bc4-4d2c-a665-4d1c1EXAMPLE",
 "OwnerInformation": "",
 "InstalledCount": 46,
 "InstalledOtherCount": 4,
 "InstalledPendingRebootCount": 1,
 "InstalledRejectedCount": 1,
 "MissingCount": 7,
 "FailedCount": 0,
 "UnreportedNotApplicableCount": 232,
 "NotApplicableCount": 654,
 "OperationStartTime": "2021-08-04T11:03:50.590000-07:00",
 "OperationEndTime": "2021-08-04T11:04:21.555000-07:00",
 "Operation": "Scan",
 "RebootOption": "NoReboot",
 "CriticalNonCompliantCount": 0,
 "SecurityNonCompliantCount": 1,
 "OtherNonCompliantCount": 1
 }
]
}
```

Esempio 3: come ottenere gli stati delle istanze per un gruppo di patch con meno di dieci istanze che richiedono un riavvio

L'esempio seguente `describe-instance-patch-states-for-patch-group` recupera i dettagli sugli stati di riepilogo delle patch per il gruppo di patch specificato per le istanze con meno di dieci istanze che richiedono un riavvio.

```
aws ssm describe-instance-patch-states-for-patch-group \
 --filters Key=InstalledPendingRebootCount,Type=LessThan,Values=10 \
 --patch-group "Production"
```

Output:

```
{
 "InstancePatchStates": [
```

```

 {
 "InstanceId": "i-02573cafcfEXAMPLE",
 "BaselineId": "pb-0c10e65780EXAMPLE",
 "SnapshotId": "a3f5ff34-9bc4-4d2c-a665-4d1c1EXAMPLE",
 "PatchGroup": "Production",
 "OwnerInformation": "",
 "InstalledCount": 32,
 "InstalledOtherCount": 1,
 "InstalledPendingRebootCount": 4,
 "InstalledRejectedCount": 0,
 "MissingCount": 2,
 "FailedCount": 0,
 "UnreportedNotApplicableCount": 846,
 "NotApplicableCount": 212,
 "OperationStartTime": "2021-08-04T11:03:50.590000-07:00",
 "OperationEndTime": "2021-08-06T11:04:21.555000-07:00",
 "Operation": "Scan",
 "RebootOption": "NoReboot",
 "CriticalNonCompliantCount": 0,
 "SecurityNonCompliantCount": 1,
 "OtherNonCompliantCount": 0
 }
]
}

```

Per ulteriori informazioni, consulta [Comprensione dei valori dello stato di conformità delle patch](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [DescribeInstancePatchStatesForPatchGroup](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: Questo esempio ottiene gli stati del riepilogo delle patch per istanza per un gruppo di patch.

```
Get-SSMInstancePatchStatesForPatchGroup -PatchGroup "Production"
```

- Per i dettagli sull'API, vedere [DescribeInstancePatchStatesForPatchGroup](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: Questo esempio ottiene gli stati del riepilogo delle patch per istanza per un gruppo di patch.

```
Get-SSMInstancePatchStatesForPatchGroup -PatchGroup "Production"
```

- Per i dettagli sull'API, vedere [DescribeInstancePatchStatesForPatchGroup](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeInstancePatches** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeInstancePatches`.

### CLI

#### AWS CLI

Esempio 1: per ottenere i dettagli sullo stato della patch per un'istanza

L'esempio seguente `describe-instance-patches` recupera i dettagli delle patch per l'istanza specificata.

```
aws ssm describe-instance-patches \
 --instance-id "i-1234567890abcdef0"
```

Output:

```
{
 "Patches": [
 {
 "Title": "2019-01 Security Update for Adobe Flash Player for Windows
Server 2016 for x64-based Systems (KB4480979)",
 "KBId": "KB4480979",
 "Classification": "SecurityUpdates",
 "Severity": "Critical",
```

```

 "State": "Installed",
 "InstalledTime": "2019-01-09T00:00:00+00:00"
 },
 {
 "Title": "",
 "KBId": "KB4481031",
 "Classification": "",
 "Severity": "",
 "State": "InstalledOther",
 "InstalledTime": "2019-02-08T00:00:00+00:00"
 },
 ...
],
"NextToken": "--token string truncated--"
}

```

Esempio 2: come ottenere un elenco di patch nello Stato mancante per un'istanza

L'esempio seguente `describe-instance-patches` recupera informazioni sulle patch che si trovano nello stato Missing per l'istanza specificata.

```

aws ssm describe-instance-patches \
 --instance-id "i-1234567890abcdef0" \
 --filters Key=State,Values=Missing

```

Output:

```

{
 "Patches": [
 {
 "Title": "Windows Malicious Software Removal Tool x64 - February 2019 (KB890830)",
 "KBId": "KB890830",
 "Classification": "UpdateRollups",
 "Severity": "Unspecified",
 "State": "Missing",
 "InstalledTime": "1970-01-01T00:00:00+00:00"
 },
 ...
],
 "NextToken": "--token string truncated--"
}

```

Per ulteriori informazioni, consulta [Informazioni sugli stati di conformità delle patch](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 3: per ottenere un elenco delle patch installate a partire da una specificata `InstalledTime` per un'istanza

L'esempio seguente `describe-instance-patches` recupera le informazioni sulle patch installate a partire da un determinato periodo di tempo per l'istanza specificata combinando l'uso di `--filters` e `--query`.

```
aws ssm describe-instance-patches \
 --instance-id "i-1234567890abcdef0" \
 --filters Key=State,Values=Installed \
 --query "Patches[?InstalledTime >= `2023-01-01T16:00:00`]"
```

Output:

```
{
 "Patches": [
 {
 "Title": "2023-03 Cumulative Update for Windows Server 2019 (1809)
for x64-based Systems (KB5023702)",
 "KBId": "KB5023702",
 "Classification": "SecurityUpdates",
 "Severity": "Critical",
 "State": "Installed",
 "InstalledTime": "2023-03-16T11:00:00+00:00"
 },
 ...
],
 "NextToken": "--token string truncated--"
}
```

- Per i dettagli sull'API, vedi [DescribeInstancePatches](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio ottiene i dettagli sulla conformità delle patch per un'istanza.



```
Get-SSMInstancePatch -InstanceId "i-08ee91c0b17045407"
```

- Per i dettagli sull'API, vedere [DescribeInstancePatches](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio ottiene i dettagli sulla conformità delle patch per un'istanza.

```
Get-SSMInstancePatch -InstanceId "i-08ee91c0b17045407"
```

- Per i dettagli sull'API, vedere [DescribeInstancePatches](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeMaintenanceWindowExecutionTaskInvocations** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeMaintenanceWindowExecutionTaskInvocations`.

### CLI

#### AWS CLI

Per eseguire le invocazioni di attività specifiche per l'esecuzione di un'operazione in una finestra di manutenzione

L'esempio seguente `describe-maintenance-window-execution-task-invocations` elenca le invocazioni per l'attività specificata eseguite come parte dell'esecuzione della finestra di manutenzione specificata.

```
aws ssm describe-maintenance-window-execution-task-invocations \
 --window-execution-id "518d5565-5969-4cca-8f0e-da3b2a638355" \
 --task-id "ac0c6ae1-daa3-4a89-832e-d384503b6586"
```

Output:

```
{
 "WindowExecutionTaskInvocationIdentities": [
 {
 "Status": "SUCCESS",
 "Parameters": "{\\"documentName\\":\\"AWS-RunShellScript\\",
\\"instanceIds\\":[\\"i-0000293ffd8c57862\\"],\\"parameters\\":{\\"commands\\":[\\"df\\"]}},
\\"maxConcurrency\\":\\"1\\",\\"maxErrors\\":\\"1\\"}",
 "InvocationId": "e274b6e1-fe56-4e32-bd2a-8073c6381d8b",
 "StartTime": 1487692834.723,
 "EndTime": 1487692834.871,
 "WindowExecutionId": "518d5565-5969-4cca-8f0e-da3b2a638355",
 "TaskExecutionId": "ac0c6ae1-daa3-4a89-832e-d384503b6586"
 }
]
}
```

Per ulteriori informazioni, vedere [View Information About Tasks and Task Executions \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindowExecutionTaskInvocations](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca le invocazioni per un'attività eseguita nell'ambito di un'esecuzione di una finestra di manutenzione.

```
Get-SSMMaintenanceWindowExecutionTaskInvocationList -TaskId "ac0c6ae1-
daa3-4a89-832e-d384503b6586" -WindowExecutionId "518d5565-5969-4cca-8f0e-
da3b2a638355"
```

Output:

```
EndTime : 2/21/2017 4:00:34 PM
ExecutionId :
InvocationId : e274b6e1-fe56-4e32-bd2a-8073c6381d8b
OwnerInformation :
Parameters : {"documentName":"AWS-RunShellScript","instanceIds":
["i-0000293ffd8c57862"],"parameters":{"commands":["df"]},"maxConcurrency":"1",
 "maxErrors":"1"}
```

```

StartTime : 2/21/2017 4:00:34 PM
Status : FAILED
StatusDetails : The instance IDs list contains an invalid entry.
TaskExecutionId : ac0c6ae1-daa3-4a89-832e-d384503b6586
WindowExecutionId : 518d5565-5969-4cca-8f0e-da3b2a638355
WindowTargetId :

```

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindowExecutionTaskInvocations](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca le invocazioni per un'attività eseguita nell'ambito di un'esecuzione di una finestra di manutenzione.

```

Get-SSMMaintenanceWindowExecutionTaskInvocationList -TaskId "ac0c6ae1-
daa3-4a89-832e-d384503b6586" -WindowExecutionId "518d5565-5969-4cca-8f0e-
da3b2a638355"

```

## Output:

```

EndTime : 2/21/2017 4:00:34 PM
ExecutionId :
InvocationId : e274b6e1-fe56-4e32-bd2a-8073c6381d8b
OwnerInformation :
Parameters : {"documentName":"AWS-RunShellScript","instanceIds":
["i-0000293ffd8c57862"],"parameters":{"commands":["df"]},"maxConcurrency":"1",
 "maxErrors":"1"}
StartTime : 2/21/2017 4:00:34 PM
Status : FAILED
StatusDetails : The instance IDs list contains an invalid entry.
TaskExecutionId : ac0c6ae1-daa3-4a89-832e-d384503b6586
WindowExecutionId : 518d5565-5969-4cca-8f0e-da3b2a638355
WindowTargetId :

```

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindowExecutionTaskInvocations](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di `DescribeMaintenanceWindowExecutionTasks` con una CLI

I seguenti esempi di codice mostrano come usare `DescribeMaintenanceWindowExecutionTasks`.

### CLI

#### AWS CLI

Per elencare tutte le attività associate all'esecuzione di una finestra di manutenzione

L'esempio seguente `ssm describe-maintenance-window-execution-tasks` elenca le attività associate all'esecuzione della finestra di manutenzione specificata.

```
aws ssm describe-maintenance-window-execution-tasks \
 --window-execution-id "518d5565-5969-4cca-8f0e-da3b2EXAMPLE"
```

Output:

```
{
 "WindowExecutionTaskIdentities": [
 {
 "Status": "SUCCESS",
 "TaskArn": "AWS-RunShellScript",
 "StartTime": 1487692834.684,
 "TaskType": "RUN_COMMAND",
 "EndTime": 1487692835.005,
 "WindowExecutionId": "518d5565-5969-4cca-8f0e-da3b2EXAMPLE",
 "TaskExecutionId": "ac0c6ae1-daa3-4a89-832e-d3845EXAMPLE"
 }
]
}
```

Per ulteriori informazioni, vedere [View Information About Tasks and Task Executions \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindowExecutionTasks](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca le attività associate all'esecuzione di una finestra di manutenzione.

```
Get-SSMMaintenanceWindowExecutionTaskList -WindowExecutionId
"518d5565-5969-4cca-8f0e-da3b2a638355"
```

Output:

```
EndTime : 2/21/2017 4:00:35 PM
StartTime : 2/21/2017 4:00:34 PM
Status : SUCCESS
TaskArn : AWS-RunShellScript
TaskExecutionId : ac0c6ae1-daa3-4a89-832e-d384503b6586
TaskType : RUN_COMMAND
WindowExecutionId : 518d5565-5969-4cca-8f0e-da3b2a638355
```

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindowExecutionTasks](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca le attività associate all'esecuzione di una finestra di manutenzione.

```
Get-SSMMaintenanceWindowExecutionTaskList -WindowExecutionId
"518d5565-5969-4cca-8f0e-da3b2a638355"
```

Output:

```
EndTime : 2/21/2017 4:00:35 PM
StartTime : 2/21/2017 4:00:34 PM
Status : SUCCESS
TaskArn : AWS-RunShellScript
TaskExecutionId : ac0c6ae1-daa3-4a89-832e-d384503b6586
TaskType : RUN_COMMAND
WindowExecutionId : 518d5565-5969-4cca-8f0e-da3b2a638355
```

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindowExecutionTasks](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeMaintenanceWindowExecutions** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeMaintenanceWindowExecutions`.

### CLI

#### AWS CLI

Esempio 1: per elencare tutte le esecuzioni per una finestra di manutenzione

L'esempio seguente `describe-maintenance-window-executions` elenca tutte le esecuzioni per la finestra di manutenzione specificata.

```
aws ssm describe-maintenance-window-executions \
 --window-id "mw-ab12cd34eEXAMPLE"
```

Output:

```
{
 "WindowExecutions": [
 {
 "WindowId": "mw-ab12cd34eEXAMPLE",
 "WindowExecutionId": "6027b513-64fe-4cf0-be7d-1191aEXAMPLE",
 "Status": "IN_PROGRESS",
 "StartTime": "2021-08-04T11:00:00.000000-07:00"
 },
 {
 "WindowId": "mw-ab12cd34eEXAMPLE",
 "WindowExecutionId": "ff75b750-4834-4377-8f61-b3cadEXAMPLE",
 "Status": "SUCCESS",
 "StartTime": "2021-08-03T11:00:00.000000-07:00",
 "EndTime": "2021-08-03T11:37:21.450000-07:00"
 },
 {
```

```

 "WindowId": "mw-ab12cd34eEXAMPLE",
 "WindowExecutionId": "9fac7dd9-ff21-42a5-96ad-bbc4bEXAMPLE",
 "Status": "FAILED",
 "StatusDetails": "One or more tasks in the orchestration failed.",
 "StartTime": "2021-08-02T11:00:00.000000-07:00",
 "EndTime": "2021-08-02T11:22:36.190000-07:00"
 }
]
 }
}

```

Esempio 2: come elencare tutte le esecuzioni relative a una finestra di manutenzione prima di una data specificata

L'esempio seguente `describe-maintenance-window-executions` elenca tutte le esecuzioni per la finestra di manutenzione specificata prima della data specificata.

```

aws ssm describe-maintenance-window-executions \
 --window-id "mw-ab12cd34eEXAMPLE" \
 --filters "Key=ExecutedBefore,Values=2021-08-03T00:00:00Z"

```

Output:

```

{
 "WindowExecutions": [
 {
 "WindowId": "mw-ab12cd34eEXAMPLE",
 "WindowExecutionId": "9fac7dd9-ff21-42a5-96ad-bbc4bEXAMPLE",
 "Status": "FAILED",
 "StatusDetails": "One or more tasks in the orchestration failed.",
 "StartTime": "2021-08-02T11:00:00.000000-07:00",
 "EndTime": "2021-08-02T11:22:36.190000-07:00"
 }
]
}

```

Esempio 3: come elencare tutte le esecuzioni per una finestra di manutenzione dopo una data specificata

L'esempio seguente `describe-maintenance-window-executions` elenca tutte le esecuzioni per la finestra di manutenzione specificata dopo la data specificata.

```

aws ssm describe-maintenance-window-executions \

```

```
--window-id "mw-ab12cd34eEXAMPLE" \
--filters "Key=ExecutedAfter,Values=2021-08-04T00:00:00Z"
```

Output:

```
{
 "WindowExecutions": [
 {
 "WindowId": "mw-ab12cd34eEXAMPLE",
 "WindowExecutionId": "6027b513-64fe-4cf0-be7d-1191aEXAMPLE",
 "Status": "IN_PROGRESS",
 "StartTime": "2021-08-04T11:00:00.000000-07:00"
 }
]
}
```

Per ulteriori informazioni, vedere [Visualizzare le informazioni sulle attività e sulle esecuzioni delle attività \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindowExecutions](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca tutte le esecuzioni per una finestra di manutenzione.

```
Get-SSMMaintenanceWindowExecutionList -WindowId "mw-03eb9db42890fb82d"
```

Output:

```
EndTime : 2/20/2017 6:30:17 PM
StartTime : 2/20/2017 6:30:16 PM
Status : FAILED
StatusDetails : One or more tasks in the orchestration failed.
WindowExecutionId : 6f3215cf-4101-4fa0-9b7b-9523269599c7
WindowId : mw-03eb9db42890fb82d
```

Esempio 2: questo esempio elenca tutte le esecuzioni per una finestra di manutenzione prima di una data specificata.



```
$option1 = @{"Key="ExecutedBefore";Values=@"2016-11-04T05:00:00Z"}
Get-SSMMaintenanceWindowExecutionList -WindowId "mw-03eb9db42890fb82d" -Filter
$option1
```

Esempio 3: questo esempio elenca tutte le esecuzioni per una finestra di manutenzione dopo una data specificata.

```
$option1 = @{"Key="ExecutedAfter";Values=@"2016-11-04T05:00:00Z"}
Get-SSMMaintenanceWindowExecutionList -WindowId "mw-03eb9db42890fb82d" -Filter
$option1
```

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindowExecutions](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca tutte le esecuzioni per una finestra di manutenzione.

```
Get-SSMMaintenanceWindowExecutionList -WindowId "mw-03eb9db42890fb82d"
```

### Output:

```
EndTime : 2/20/2017 6:30:17 PM
StartTime : 2/20/2017 6:30:16 PM
Status : FAILED
StatusDetails : One or more tasks in the orchestration failed.
WindowExecutionId : 6f3215cf-4101-4fa0-9b7b-9523269599c7
WindowId : mw-03eb9db42890fb82d
```

Esempio 2: questo esempio elenca tutte le esecuzioni per una finestra di manutenzione prima di una data specificata.

```
$option1 = @{"Key="ExecutedBefore";Values=@"2016-11-04T05:00:00Z"}
Get-SSMMaintenanceWindowExecutionList -WindowId "mw-03eb9db42890fb82d" -Filter
$option1
```

Esempio 3: questo esempio elenca tutte le esecuzioni per una finestra di manutenzione dopo una data specificata.

```
$option1 = @{"Key="ExecutedAfter";Values=@"2016-11-04T05:00:00Z"}
Get-SSMMaintenanceWindowExecutionList -WindowId "mw-03eb9db42890fb82d" -Filter
$option1
```

```
Get-SSMMaintenanceWindowExecutionList -WindowId "mw-03eb9db42890fb82d" -Filter $option1
```

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindowExecutions](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeMaintenanceWindowTargets** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeMaintenanceWindowTargets`.

### CLI

#### AWS CLI

Esempio 1: elencare tutti gli obiettivi per una finestra di manutenzione

L'esempio seguente `describe-maintenance-window-targets` elenca tutte le destinazioni per una finestra di manutenzione.

```
aws ssm describe-maintenance-window-targets \
 --window-id "mw-06cf17cbefEXAMPLE"
```

Output:

```
{
 "Targets": [
 {
 "ResourceType": "INSTANCE",
 "OwnerInformation": "Single instance",
 "WindowId": "mw-06cf17cbefEXAMPLE",
 "Targets": [
 {
 "Values": [
 "i-0000293ffdEXAMPLE"
],
 "Key": "InstanceIds"
 }
]
 }
],
```

```

 "WindowTargetId": "350d44e6-28cc-44e2-951f-4b2c9EXAMPLE"
 },
 {
 "ResourceType": "INSTANCE",
 "OwnerInformation": "Two instances in a list",
 "WindowId": "mw-06cf17cbefEXAMPLE",
 "Targets": [
 {
 "Values": [
 "i-0000293ffdEXAMPLE",
 "i-0cb2b964d3EXAMPLE"
],
 "Key": "InstanceIds"
 }
],
 "WindowTargetId": "e078a987-2866-47be-bedd-d9cf4EXAMPLE"
 }
]
}

```

Esempio 2: come elencare tutte le destinazioni di una finestra di manutenzione che corrispondono a un determinato valore delle informazioni dello specifico proprietario

Questo esempio `describe-maintenance-window-targets` elenca tutti gli obiettivi di una finestra di manutenzione con un valore specifico.

```

aws ssm describe-maintenance-window-targets \
 --window-id "mw-0ecb1226ddEXAMPLE" \
 --filters "Key=OwnerInformation,Values=CostCenter1"

```

Output:

```

{
 "Targets": [
 {
 "WindowId": "mw-0ecb1226ddEXAMPLE",
 "WindowTargetId": "da89dcc3-7f9c-481d-ba2b-edcb7d0057f9",
 "ResourceType": "INSTANCE",
 "Targets": [
 {
 "Key": "tag:Environment",
 "Values": [
 "Prod"
]
 }
]
 }
]
}

```

```

]
 }
],
 "OwnerInformation": "CostCenter1",
 "Name": "ProdTarget1"
 }
]
}

```

Per ulteriori informazioni, vedere [View Information About Maintenance Windows \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindowTargets](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca tutti gli obiettivi per una finestra di manutenzione.

```
Get-SSMMaintenanceWindowTarget -WindowId "mw-06cf17cbefcb4bf4f"
```

Output:

```

OwnerInformation : Single instance
ResourceType : INSTANCE
Targets : {InstanceIds}
WindowId : mw-06cf17cbefcb4bf4f
WindowTargetId : 350d44e6-28cc-44e2-951f-4b2c985838f6

OwnerInformation : Two instances in a list
ResourceType : INSTANCE
Targets : {InstanceIds}
WindowId : mw-06cf17cbefcb4bf4f
WindowTargetId : e078a987-2866-47be-bedd-d9cf49177d3a

```

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindowTargets](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca tutti gli obiettivi per una finestra di manutenzione.

```
Get-SSMMaintenanceWindowTarget -WindowId "mw-06cf17cbefcb4bf4f"
```

Output:

```
OwnerInformation : Single instance
ResourceType : INSTANCE
Targets : {InstanceIds}
WindowId : mw-06cf17cbefcb4bf4f
WindowTargetId : 350d44e6-28cc-44e2-951f-4b2c985838f6

OwnerInformation : Two instances in a list
ResourceType : INSTANCE
Targets : {InstanceIds}
WindowId : mw-06cf17cbefcb4bf4f
WindowTargetId : e078a987-2866-47be-bedd-d9cf49177d3a
```

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindowTargets](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeMaintenanceWindowTasks** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeMaintenanceWindowTasks`.

### CLI

#### AWS CLI

Esempio 1: per elencare tutte le attività per una finestra di manutenzione

L'esempio seguente `describe-maintenance-window-tasks` elenca tutte le attività per la finestra di manutenzione specificata.

```
aws ssm describe-maintenance-window-tasks \
 --window-id "mw-06cf17cbefEXAMPLE"
```

Output:

```

{
 "Tasks": [
 {
 "WindowId": "mw-06cf17cbefEXAMPLE",
 "WindowTaskId": "018b31c3-2d77-4b9e-bd48-c91edEXAMPLE",
 "TaskArn": "AWS-RestartEC2Instance",
 "TaskParameters": {},
 "Type": "AUTOMATION",
 "Description": "Restarting EC2 Instance for maintenance",
 "MaxConcurrency": "1",
 "MaxErrors": "1",
 "Name": "My-Automation-Example-Task",
 "Priority": 0,
 "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
 "Targets": [
 {
 "Key": "WindowTargetIds",
 "Values": [
 "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
]
 }
]
 },
 {
 "WindowId": "mw-06cf17cbefEXAMPLE",
 "WindowTaskId": "1943dee0-0a17-4978-9bf4-3cc2fEXAMPLE",
 "TaskArn": "AWS-DisableS3BucketPublicReadWrite",
 "TaskParameters": {},
 "Type": "AUTOMATION",
 "Description": "Automation task to disable read/write access on public S3 buckets",
 "MaxConcurrency": "10",
 "MaxErrors": "5",
 "Name": "My-Disable-S3-Public-Read-Write-Access-Automation-Task",
 "Priority": 0,
 "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
 "Targets": [
 {
 "Key": "WindowTargetIds",
 "Values": [
 "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
]
 }
]
 }
]
}

```

```

]
 }
]
}

```

Esempio 2: elencare tutte le attività per una finestra di manutenzione che richiama il documento AWS- command RunPowerShellScript

L'esempio seguente `describe-maintenance-window-tasks` elenca tutte le attività per la finestra di manutenzione specificata che invoca il documento di comando AWS-RunPowerShellScript.

```

aws ssm describe-maintenance-window-tasks \
 --window-id "mw-ab12cd34eEXAMPLE" \
 --filters "Key=TaskArn,Values=AWS-RunPowerShellScript"

```

Output:

```

{
 "Tasks": [
 {
 "WindowId": "mw-ab12cd34eEXAMPLE",
 "WindowTaskId": "0d36e6b4-3a4f-411e-adcb-3558eEXAMPLE",
 "TaskArn": "AWS-RunPowerShellScript",
 "Type": "RUN_COMMAND",
 "Targets": [
 {
 "Key": "WindowTargetIds",
 "Values": [
 "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
]
 }
],
 "TaskParameters": {},
 "Priority": 1,
 "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
 "MaxConcurrency": "1",
 "MaxErrors": "1",
 "Name": "MyTask"
 }
]
}

```

```
 }
]
}
```

Esempio 3: come elencare tutte le attività per una finestra di manutenzione con una priorità di 3

L'esempio seguente `describe-maintenance-window-tasks` elenca tutte le attività per la finestra di manutenzione specificata che hanno un valore `Priority` di 3.

```
aws ssm describe-maintenance-window-tasks \
 --window-id "mw-ab12cd34eEXAMPLE" \
 --filters "Key=Priority,Values=3"
```

Output:

```
{
 "Tasks": [
 {
 "WindowId": "mw-ab12cd34eEXAMPLE",
 "WindowTaskId": "0d36e6b4-3a4f-411e-adcb-3558eEXAMPLE",
 "TaskArn": "AWS-RunPowerShellScript",
 "Type": "RUN_COMMAND",
 "Targets": [
 {
 "Key": "WindowTargetIds",
 "Values": [
 "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
]
 }
],
 "TaskParameters": {},
 "Priority": 3,
 "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
 "MaxConcurrency": "1",
 "MaxErrors": "1",
 "Name": "MyRunCommandTask"
 },
 {
 "WindowId": "mw-ab12cd34eEXAMPLE",
 "WindowTaskId": "ee45feff-ad65-4a6c-b478-5cab8EXAMPLE",
```



```

 "TaskArn": "AWS-RestartEC2Instance",
 "Type": "AUTOMATION",
 "Targets": [
 {
 "Key": "WindowTargetIds",
 "Values": [
 "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
]
 }
],
 "TaskParameters": {},
 "Priority": 3,
 "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
 "MaxConcurrency": "10",
 "MaxErrors": "5",
 "Name": "My-Automation-Task",
 "Description": "A description for my Automation task"
 }
]
}

```

Esempio 4: come elencare tutte le attività per una finestra di manutenzione con priorità pari a 1 e utilizzare Run Command

Questo esempio `describe-maintenance-window-tasks` elenca tutte le attività per la finestra di manutenzione specificata che hanno un valore `Priority` di 1 e un utilizzo di `Run Command`.

```

aws ssm describe-maintenance-window-tasks \
 --window-id "mw-ab12cd34eEXAMPLE" \
 --filters "Key=Priority,Values=1" "Key=TaskType,Values=RUN_COMMAND"

```

Output:

```

{
 "Tasks": [
 {
 "WindowId": "mw-ab12cd34eEXAMPLE",
 "WindowTaskId": "0d36e6b4-3a4f-411e-adcb-3558eEXAMPLE",
 "TaskArn": "AWS-RunPowerShellScript",
 "Type": "RUN_COMMAND",

```

```

 "Targets": [
 {
 "Key": "WindowTargetIds",
 "Values": [
 "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
]
 }
],
 "TaskParameters": {},
 "Priority": 1,
 "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
 "MaxConcurrency": "1",
 "MaxErrors": "1",
 "Name": "MyRunCommandTask"
 }
]
}

```

Per ulteriori informazioni, vedere [Visualizzare le informazioni sulle finestre di manutenzione \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindowTasks](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca tutte le attività per una finestra di manutenzione.

```
Get-SSMMaintenanceWindowTaskList -WindowId "mw-06cf17cbefcb4bf4f"
```

Output:

```

LoggingInfo :
MaxConcurrency : 1
MaxErrors : 1
Priority : 10
ServiceRoleArn : arn:aws:iam::123456789012:role/MaintenanceWindowsRole
Targets : {InstanceIds}
TaskArn : AWS-RunShellScript

```

```
TaskParameters : {[commands,
 Amazon.SimpleSystemsManagement.Model.MaintenanceWindowTaskParameterValueExpression]}
Type : RUN_COMMAND
WindowId : mw-06cf17cbefcb4bf4f
WindowTaskId : a23e338d-ff30-4398-8aa3-09cd052ebf17
```

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindowTasks](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca tutte le attività per una finestra di manutenzione.

```
Get-SSMMaintenanceWindowTaskList -WindowId "mw-06cf17cbefcb4bf4f"
```

Output:

```
LoggingInfo :
MaxConcurrency : 1
MaxErrors : 1
Priority : 10
ServiceRoleArn : arn:aws:iam::123456789012:role/MaintenanceWindowsRole
Targets : {InstanceIds}
TaskArn : AWS-RunShellScript
TaskParameters : {[commands,
 Amazon.SimpleSystemsManagement.Model.MaintenanceWindowTaskParameterValueExpression]}
Type : RUN_COMMAND
WindowId : mw-06cf17cbefcb4bf4f
WindowTaskId : a23e338d-ff30-4398-8aa3-09cd052ebf17
```

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindowTasks](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribeMaintenanceWindows** con una CLI

I seguenti esempi di codice mostrano come usare `DescribeMaintenanceWindows`.

## CLI

### AWS CLI

Esempio 1: per elencare tutte le finestre di manutenzione

L'output seguente elenca tutte le finestre di manutenzione del tuo AWS account nella regione corrente.

```
aws ssm describe-maintenance-windows
```

Output:

```
{
 "WindowIdentities": [
 {
 "WindowId": "mw-0ecb1226ddEXAMPLE",
 "Name": "MyMaintenanceWindow-1",
 "Enabled": true,
 "Duration": 2,
 "Cutoff": 1,
 "Schedule": "rate(180 minutes)",
 "NextExecutionTime": "2020-02-12T23:19:20.596Z"
 },
 {
 "WindowId": "mw-03eb9db428EXAMPLE",
 "Name": "MyMaintenanceWindow-2",
 "Enabled": true,
 "Duration": 3,
 "Cutoff": 1,
 "Schedule": "rate(7 days)",
 "NextExecutionTime": "2020-02-17T23:22:00.956Z"
 }
]
}
```

Esempio 2: come elencare tutte le finestre di manutenzione abilitate

L'esempio seguente `describe-maintenance-windows` elenca tutte le finestre di manutenzione abilitate.

```
aws ssm describe-maintenance-windows \
```

```
--filters "Key=Enabled,Values=true"
```

Esempio 3: come elencare le finestre di manutenzione che corrispondono a un nome specifico

Questo esempio `describe-maintenance-windows` elenca tutte le finestre di manutenzione con il nome specificato.

```
aws ssm describe-maintenance-windows \
 --filters "Key=Name,Values=MyMaintenanceWindow"
```

Per ulteriori informazioni, vedere [View Information About Maintenance Windows \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindows](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca tutte le finestre di manutenzione dell'account.

```
Get-SSMMaintenanceWindowList
```

Output:

```
Cutoff : 1
Duration : 4
Enabled : True
Name : My-First-Maintenance-Window
WindowId : mw-06d59c1a07c022145
```

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindows](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca tutte le finestre di manutenzione dell'account.

```
Get-SSMMaintenanceWindowList
```

Output:

```
Cutoff : 1
Duration : 4
Enabled : True
Name : My-First-Maintenance-Window
WindowId : mw-06d59c1a07c022145
```

- Per i dettagli sull'API, vedere [DescribeMaintenanceWindows](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Usare **DescribeOpsItems** con un AWS SDK o CLI

I seguenti esempi di codice mostrano come usare `DescribeOpsItems`.

### CLI

#### AWS CLI

Per elencare un set di OpsItems

L'`describe-ops-items`esempio seguente mostra un elenco di tutti i dati aperti OpsItems nel tuo AWS account.

```
aws ssm describe-ops-items \
 --ops-item-filters "Key=Status,Values=Open,Operator=Equal"
```

Output:

```
{
 "OpsItemSummaries": [
 {
 "CreatedBy": "arn:aws:sts::111222333444:assumed-role/OpsItem-CWE-Role/fbf77cbe264a33509569f23e4EXAMPLE",
 "CreatedTime": "2020-03-14T17:02:46.375000-07:00",
 "LastModifiedBy": "arn:aws:sts::111222333444:assumed-role/OpsItem-CWE-Role/fbf77cbe264a33509569f23e4EXAMPLE",
 "LastModifiedTime": "2020-03-14T17:02:46.375000-07:00",
 "Source": "SSM",
```

```

 "Status": "Open",
 "OpsItemId": "oi-7cfc5EXAMPLE",
 "Title": "SSM Maintenance Window execution failed",
 "OperationalData": {
 "/aws/dedup": {
 "Value": "{\"dedupString\":\"SSMOpsItems-SSM-maintenance-
window-execution-failed\"}",
 "Type": "SearchableString"
 },
 "/aws/resources": {
 "Value": "[{\"arn\":\"arn:aws:ssm:us-
east-2:111222333444:maintenancewindow/mw-034093d322EXAMPLE\"}]",
 "Type": "SearchableString"
 }
 },
 "Category": "Availability",
 "Severity": "3"
 },
 {
 "CreatedBy": "arn:aws:sts::111222333444:assumed-role/OpsItem-CWE-
Role/fbf77cbe264a33509569f23e4EXAMPLE",
 "CreatedTime": "2020-02-26T11:43:15.426000-08:00",
 "LastModifiedBy": "arn:aws:sts::111222333444:assumed-role/OpsItem-
CWE-Role/fbf77cbe264a33509569f23e4EXAMPLE",
 "LastModifiedTime": "2020-02-26T11:43:15.426000-08:00",
 "Source": "EC2",
 "Status": "Open",
 "OpsItemId": "oi-6f966EXAMPLE",
 "Title": "EC2 instance stopped",
 "OperationalData": {
 "/aws/automations": {
 "Value": "[{ \"automationType\": \"AWS:SSM:Automation\",
 \"automationId\": \"AWS-RestartEC2Instance\" }]",
 "Type": "SearchableString"
 },
 "/aws/dedup": {
 "Value": "{\"dedupString\":\"SSMOpsItems-EC2-instance-stopped
\"}",
 "Type": "SearchableString"
 },
 "/aws/resources": {
 "Value": "[{\"arn\":\"arn:aws:ec2:us-
east-2:111222333444:instance/i-0beccfb02EXAMPLE\"}]",
 "Type": "SearchableString"
 }
 }
 }

```

```

 }
 },
 "Category": "Availability",
 "Severity": "3"
}
]
}

```

Per ulteriori informazioni, vedere [Lavorare con OpsItems](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [DescribeOpsItems](#) in AWS CLI Command Reference.

## Java

### SDK per Java 2.x

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```

/**
 * Describes AWS SSM OpsItems asynchronously.
 *
 * @param key The key to filter OpsItems by (e.g., OPS_ITEM_ID).
 *
 * This method initiates an asynchronous request to describe SSM OpsItems.
 * If the request is successful, it prints the title and status of each
OpsItem.
 * If an exception occurs, it handles the error appropriately.
 */
public void describeOpsItems(String key) {
 OpsItemFilter filter = OpsItemFilter.builder()
 .key(OpsItemFilterKey.OPS_ITEM_ID)
 .values(key)
 .operator(OpsItemFilterOperator.EQUAL)
 .build();

 DescribeOpsItemsRequest itemsRequest = DescribeOpsItemsRequest.builder()
 .maxResults(10)

```



```

 .opsItemFilters(filter)
 .build();

 CompletableFuture<Void> future = CompletableFuture.runAsync(() -> {
 getAsyncClient().describeOpsItems(itemsRequest)
 .thenAccept(itemsResponse -> {
 List<OpsItemSummary> items =
itemsResponse.opsItemSummaries();
 for (OpsItemSummary item : items) {
 System.out.println("The item title is " +
item.title() + " and the status is " + item.status().toString());
 }
 })
 .exceptionally(ex -> {
 throw new CompletionException(ex);
 }).join();
 }).exceptionally(ex -> {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
 if (cause instanceof SsmException) {
 throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
 } else {
 throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
 }
 });

 try {
 future.join();
 } catch (CompletionException ex) {
 throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
ex.getCause() : ex;
 }
}

```

- Per i dettagli sulle API, consulta la [DescribeOpsItems](#) sezione AWS SDK for Java 2.x API Reference.

## JavaScript

### SDK per JavaScript (v3)

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
import {
 OpsItemFilterOperator,
 OpsItemFilterKey,
 paginateDescribeOpsItems,
 SSMClient,
} from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Describe SSM OpsItems.
 * @param {{ opsItemId: string }}
 */
export const main = async ({ opsItemId }) => {
 const client = new SSMClient({});
 try {
 const describeOpsItemsPaginated = [];
 for await (const page of paginateDescribeOpsItems(
 { client },
 {
 OpsItemFilters: {
 Key: OpsItemFilterKey.OPSITEM_ID,
 Operator: OpsItemFilterOperator.EQUAL,
 Values: opsItemId,
 },
 },
)) {
 describeOpsItemsPaginated.push(...page.OpsItemSummaries);
 }
 console.log("Here are the ops items:");
 console.log(describeOpsItemsPaginated);
 return { OpsItemSummaries: describeOpsItemsPaginated };
 } catch (caught) {
```

```

 if (caught instanceof Error && caught.name === "MissingParameter") {
 console.warn(`${caught.message}. Did you provide this value?`);
 }
 throw caught;
}
};

```

- Per i dettagli sulle API, consulta la [DescribeOpsItems](#) sezione AWS SDK per JavaScript API Reference.

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```

class OpsItemWrapper:
 """Encapsulates AWS Systems Manager OpsItem actions."""

 def __init__(self, ssm_client):
 """
 :param ssm_client: A Boto3 Systems Manager client.
 """
 self.ssm_client = ssm_client
 self.id = None

 @classmethod
 def from_client(cls):
 """
 :return: A OpsItemWrapper instance.
 """
 ssm_client = boto3.client("ssm")
 return cls(ssm_client)

 def describe(self):

```

```
"""
Describe an OpsItem.
"""
try:
 paginator = self.ssm_client.get_paginator("describe_ops_items")
 ops_items = []
 for page in paginator.paginate(
 OpsItemFilters=[
 {"Key": "OpsItemId", "Values": [self.id], "Operator":
"Equal"}
]
):
 ops_items.extend(page["OpsItemSummaries"])

 for item in ops_items:
 print(
 f"The item title is {item['Title']} and the status is
{item['Status']}"
)
 return len(ops_items) > 0
except ClientError as err:
 logger.error(
 "Couldn't describe ops item %s. Here's why: %s: %s",
 self.id,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise
```

- Per i dettagli sulle API, vedi [DescribeOpsItems](#) in AWS SDK for Python (Boto3) API Reference.

## SAP ABAP

## SDK per SAP ABAP

 Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```

TRY.
 " Create filter for OpsItem ID
 DATA(lt_filters) = VALUE /aws1/cl_ssmopsitemfilter=>tt_opsitemfilters(
 (NEW /aws1/cl_ssmopsitemfilter(
 iv_key = 'OpsItemId'
 it_values = VALUE /aws1/
cl_ssmopsitemfiltvals_w=>tt_opsitemfiltervalues(
 (NEW /aws1/cl_ssmopsitemfiltvals_w(iv_value =
iv_ops_item_id))
)
 iv_operator = 'Equal'
))
).

 " Use paginator to get all results
 DATA(lo_paginator) = lo_ssm->get_paginator().
 DATA(lo_iterator) = lo_paginator->describeopsitems(
 it_opsitemfilters = lt_filters).

 rv_found = abap_false.

 WHILE lo_iterator->has_next().
 DATA(lo_result) = CAST /aws1/cl_ssmdescropsitemsrsp(lo_iterator-
>get_next()).
 LOOP AT lo_result->get_opsitemsummaries() INTO DATA(lo_item).
 DATA(lv_title) = lo_item->get_title().
 DATA(lv_status) = lo_item->get_status().
 MESSAGE |The OpsItem title is { lv_title } and the status is
{ lv_status }| TYPE 'I'.
 rv_found = abap_true.
 ENDLOOP.
 ENDWHILE.

```

```
CATCH /aws1/cx_ssminternalservererr.
 MESSAGE 'Internal server error occurred.' TYPE 'I'.
ENDTRY.
```

- Per i dettagli sulle API, consulta [DescribeOpsItems](#) la sezione AWS SDK for SAP ABAP API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Usare **DescribeParameters** con un AWS SDK o CLI

I seguenti esempi di codice mostrano come usare `DescribeParameters`.

### CLI

#### AWS CLI

Esempio 1: per elencare tutti i parametri

L'`describe-parameters` seguente elenca tutti i parametri dell' AWS account corrente e della regione.

```
aws ssm describe-parameters
```

Output:

```
{
 "Parameters": [
 {
 "Name": "MySecureStringParameter",
 "Type": "SecureString",
 "KeyId": "alias/aws/ssm",
 "LastModifiedDate": 1582155479.205,
 "LastModifiedUser": "arn:aws:sts::111222333444:assumed-role/Admin/
Richard-Roe-Managed",
 "Description": "This is a SecureString parameter",
 "Version": 2,
 "Tier": "Advanced",
 "Policies": [

```

```

 {
 "PolicyText": "{\"Type\":\"Expiration\",\"Version\":\"1.0\",
\\\"Attributes\\\":{\\\"Timestamp\\\":\\\"2020-07-07T22:30:00Z\\\"}}\",
 "PolicyType": "Expiration",
 "PolicyStatus": "Pending"
 },
 {
 "PolicyText": "{\"Type\":\"ExpirationNotification\",\"Version
\\\":\\\"1.0\\\",\\\"Attributes\\\":{\\\"Before\\\":\\\"12\\\",\\\"Unit\\\":\\\"Hours\\\"}}\",
 "PolicyType": "ExpirationNotification",
 "PolicyStatus": "Pending"
 }
]
},
{
 "Name": "MyStringListParameter",
 "Type": "StringList",
 "LastModifiedDate": 1582154764.222,
 "LastModifiedUser": "arn:aws:iam::111222333444:user/Mary-Major",
 "Description": "This is a StringList parameter",
 "Version": 1,
 "Tier": "Standard",
 "Policies": []
},
{
 "Name": "MyStringParameter",
 "Type": "String",
 "LastModifiedDate": 1582154711.976,
 "LastModifiedUser": "arn:aws:iam::111222333444:user/Alejandro-
Rosalez",
 "Description": "This is a String parameter",
 "Version": 1,
 "Tier": "Standard",
 "Policies": []
},
{
 "Name": "latestAmi",
 "Type": "String",
 "LastModifiedDate": 1580862415.521,
 "LastModifiedUser": "arn:aws:sts::111222333444:assumed-role/lambda-
ssm-role/Automation-UpdateSSM-Param",
 "Version": 3,
 "Tier": "Standard",
 "Policies": []
}

```

```
 }
]
}
```

Esempio 2: come elencare tutti i parametri che corrispondono a metadati specifici

Questo esempio `describe-parameters` elenca tutti i parametri che corrispondono a un filtro.

```
aws ssm describe-parameters --filters «Key=Type, Values=» StringList
```

Output:

```
{
 "Parameters": [
 {
 "Name": "MyStringListParameter",
 "Type": "StringList",
 "LastModifiedDate": 1582154764.222,
 "LastModifiedUser": "arn:aws:iam::111222333444:user/Mary-Major",
 "Description": "This is a StringList parameter",
 "Version": 1,
 "Tier": "Standard",
 "Policies": []
 }
]
}
```

Per ulteriori informazioni, consulta [Ricerca dei parametri di Systems Manager](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, consulta la sezione Command Reference. [DescribeParameters](#) AWS CLI



## Java

### SDK per Java 2.x

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ssm.SsmClient;
import software.amazon.awssdk.services.ssm.model.GetParameterRequest;
import software.amazon.awssdk.services.ssm.model.GetParameterResponse;
import software.amazon.awssdk.services.ssm.model.SsmException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
 * started.html
 */
public class GetParameter {
 public static void main(String[] args) {
 final String usage = ""

 Usage:
 <paraName>

 Where:
 paraName - The name of the parameter.
 "";

 if (args.length != 1) {
 System.out.println(usage);
 System.exit(1);
 }

 String paraName = args[0];
```

```
 Region region = Region.US_EAST_1;
 SsmClient ssmClient = SsmClient.builder()
 .region(region)
 .build();

 getParaValue(ssmClient, paraName);
 ssmClient.close();
 }

 public static void getParaValue(SsmClient ssmClient, String paraName) {
 try {
 GetParameterRequest parameterRequest = GetParameterRequest.builder()
 .name(paraName)
 .build();

 GetParameterResponse parameterResponse =
 ssmClient.getParameter(parameterRequest);
 System.out.println("The parameter value is " +
 parameterResponse.parameter().value());

 } catch (SsmException e) {
 System.err.println(e.getMessage());
 System.exit(1);
 }
 }
}
```

- Per i dettagli sulle API, consulta la [DescribeParameters](#) sezione AWS SDK for Java 2.x API Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca tutti i parametri.

```
Get-SSMParameterList
```

Output:

```
Description :
```

```
KeyId :
LastModifiedDate : 3/3/2017 6:58:23 PM
LastModifiedUser : arn:aws:iam::123456789012:user/admin
Name : Welcome
Type : String
```

- Per i dettagli sull'API, vedere [DescribeParameters](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca tutti i parametri.

```
Get-SSMParameterList
```

Output:

```
Description :
KeyId :
LastModifiedDate : 3/3/2017 6:58:23 PM
LastModifiedUser : arn:aws:iam::123456789012:user/admin
Name : Welcome
Type : String
```

- Per i dettagli sull'API, vedere [DescribeParameters](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

## Rust

### SDK per Rust

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
async fn show_parameters(client: &Client) -> Result<(), Error> {
 let resp = client.describe_parameters().send().await?;
```

```
for param in resp.parameters() {
 println!("{}", param.name().unwrap_or_default());
}

Ok(())
}
```

- Per i dettagli sulle API, consulta [DescribeParameters](#) la sezione AWS SDK for Rust API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribePatchBaselines** con una CLI

I seguenti esempi di codice mostrano come usare `DescribePatchBaselines`.

### CLI

#### AWS CLI

Esempio 1: per elencare tutte le baseline delle patch

L'`describe-patch-baselines` seguente recupera i dettagli di tutte le baseline delle patch nell'account dell'utente nella regione corrente.

```
aws ssm describe-patch-baselines
```

Output:

```
{
 "BaselineIdentities": [
 {
 "BaselineName": "AWS-SuseDefaultPatchBaseline",
 "DefaultBaseline": true,
 "BaselineDescription": "Default Patch Baseline for Suse Provided by
AWS.",
 "BaselineId": "arn:aws:ssm:us-east-2:733109147000:patchbaseline/
pb-0123fdb36e334a3b2",
 }
]
}
```

```

 "OperatingSystem": "SUSE"
 },
 {
 "BaselineName": "AWS-DefaultPatchBaseline",
 "DefaultBaseline": false,
 "BaselineDescription": "Default Patch Baseline Provided by AWS.",
 "BaselineId": "arn:aws:ssm:us-east-2:733109147000:patchbaseline/
pb-020d361a05defe4ed",
 "OperatingSystem": "WINDOWS"
 },
 ...
 {
 "BaselineName": "MyWindowsPatchBaseline",
 "DefaultBaseline": true,
 "BaselineDescription": "My patch baseline for EC2 instances for
Windows Server",
 "BaselineId": "pb-0ad00e0dd7EXAMPLE",
 "OperatingSystem": "WINDOWS"
 }
]
}

```

Esempio 2: per elencare tutte le baseline delle patch fornite da AWS

L'`describe-patch-baselines` seguente elenca tutte le baseline delle patch fornite da AWS

```
aws ssm describe-patch-baselines \
 --filters "Key=OWNER,Values=[AWS]"
```

Esempio 3: come elencare tutte le baseline delle patch possedute

L'esempio seguente `describe-patch-baselines` elenca tutte le baseline delle patch personalizzate create nell'account nella regione corrente.

```
aws ssm describe-patch-baselines \
 --filters "Key=OWNER,Values=[Self]"
```

Per ulteriori informazioni, consulta [Informazioni sulle baseline delle patch predefinite e personalizzate](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [DescribePatchBaselines](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca tutte le baseline delle patch.

```
Get-SSMPatchBaseline
```

Output:

BaselineDescription	BaselineId
-----	-----
Default Patch Baseline Provided by AWS.	arn:aws:ssm:us-west-2:123456789012:patchbaseline/pb-04fb4ae6142167966 AWS-DefaultP...
Baseline containing all updates approved for production systems	
pb-045f10b4f382baeda	
Production-B...	
Baseline containing all updates approved for production systems	
pb-0a2f1059b670ebd31	
Production-B...	

Esempio 2: questo esempio elenca tutte le linee di base delle patch fornite da AWS. La sintassi utilizzata in questo esempio richiede la PowerShell versione 3 o successiva.

```
$filter1 = @{"Key"="OWNER";Values=@("AWS")}
```

Output:

```
Get-SSMPatchBaseline -Filter $filter1
```

Esempio 3: questo esempio elenca tutte le baseline delle patch con l'utente come proprietario. La sintassi utilizzata in questo esempio richiede la PowerShell versione 3 o successiva.

```
$filter1 = @{"Key"="OWNER";Values=@("Self")}
```

Output:

```
Get-SSMPatchBaseline -Filter $filter1
```

Esempio 4: con PowerShell la versione 2, è necessario utilizzare New-Object per creare ogni tag.

```
$filter1 = New-Object
 Amazon.SimpleSystemsManagement.Model.PatchOrchestratorFilter
$filter1.Key = "OWNER"
$filter1.Values = "AWS"

Get-SSMPatchBaseline -Filter $filter1
```

Output:

BaselineDescription	BaselineId	BaselineName	DefaultBaseline
-----	-----	-----	e
Default Patch Baseline Provided by AWS.	arn:aws:ssm:us-west-2:123456789012:patchbaseline/pb-04fb4ae6142167966	AWS-DefaultPatchBaseline	True

- Per i dettagli sull'API, vedere [DescribePatchBaselines](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca tutte le baseline delle patch.

```
Get-SSMPatchBaseline
```

Output:

BaselineDescription	BaselineId	BaselineName
-----	-----	-----
Default Patch Baseline Provided by AWS.	arn:aws:ssm:us-west-2:123456789012:patchbaseline/pb-04fb4ae6142167966	AWS-DefaultP...
Baseline containing all updates approved for production systems	pb-045f10b4f382baeda	Production-B...

```
Baseline containing all updates approved for production systems
pb-0a2f1059b670ebd31
Production-B...
```

Esempio 2: questo esempio elenca tutte le linee di base delle patch fornite da AWS. La sintassi utilizzata in questo esempio richiede la PowerShell versione 3 o successiva.

```
$filter1 = @{{Key="OWNER";Values=@("AWS")}}
```

Output:

```
Get-SSMPatchBaseline -Filter $filter1
```

Esempio 3: questo esempio elenca tutte le baseline delle patch con l'utente come proprietario. La sintassi utilizzata in questo esempio richiede la PowerShell versione 3 o successiva.

```
$filter1 = @{{Key="OWNER";Values=@("Self")}}
```

Output:

```
Get-SSMPatchBaseline -Filter $filter1
```

Esempio 4: con PowerShell la versione 2, è necessario utilizzare New-Object per creare ogni tag.

```
$filter1 = New-Object
Amazon.SimpleSystemsManagement.Model.PatchOrchestratorFilter
$filter1.Key = "OWNER"
$filter1.Values = "AWS"

Get-SSMPatchBaseline -Filter $filter1
```

Output:

BaselineDescription	BaselineId	BaselineName	DefaultBaseline
-----	-----	-----	e
-----	-----	-----	-----



```
Default Patch Baseline Provided by AWS. arn:aws:ssm:us-west-2:123456789012:patchbaseline/pb-04fb4ae6142167966 AWS-DefaultPatchBaseline True
```

- Per i dettagli sull'API, vedere [DescribePatchBaselines](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribePatchGroupState** con una CLI

I seguenti esempi di codice mostrano come usare `DescribePatchGroupState`.

### CLI

#### AWS CLI

Per ottenere lo stato di un gruppo di patch

L'esempio seguente `describe-patch-group-state` recupera il riepilogo di alto livello sulla conformità delle patch per un gruppo di patch.

```
aws ssm describe-patch-group-state \
 --patch-group "Production"
```

Output:

```
{
 "Instances": 21,
 "InstancesWithCriticalNonCompliantPatches": 1,
 "InstancesWithFailedPatches": 2,
 "InstancesWithInstalledOtherPatches": 3,
 "InstancesWithInstalledPatches": 21,
 "InstancesWithInstalledPendingRebootPatches": 2,
 "InstancesWithInstalledRejectedPatches": 1,
 "InstancesWithMissingPatches": 3,
 "InstancesWithNotApplicablePatches": 4,
 "InstancesWithOtherNonCompliantPatches": 1,
 "InstancesWithSecurityNonCompliantPatches": 1,
```

```
"InstancesWithUnreportedNotApplicablePatches": 2
}
```

Per ulteriori informazioni, vedere Informazioni sui gruppi di patch < <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-patchgroups.html> >\_\_ e [Comprensione dei valori dello stato di conformità delle patch](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [DescribePatchGroupState](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio ottiene il riepilogo di alto livello sulla conformità delle patch per un gruppo di patch.

```
Get-SSMPatchGroupState -PatchGroup "Production"
```

Output:

```
Instances : 4
InstancesWithFailedPatches : 1
InstancesWithInstalledOtherPatches : 4
InstancesWithInstalledPatches : 3
InstancesWithMissingPatches : 0
InstancesWithNotApplicablePatches : 0
```

- Per i dettagli sull'API, vedere [DescribePatchGroupState](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio ottiene il riepilogo di alto livello sulla conformità delle patch per un gruppo di patch.

```
Get-SSMPatchGroupState -PatchGroup "Production"
```

Output:

```
Instances : 4
```

```
InstancesWithFailedPatches : 1
InstancesWithInstalledOtherPatches : 4
InstancesWithInstalledPatches : 3
InstancesWithMissingPatches : 0
InstancesWithNotApplicablePatches : 0
```

- Per i dettagli sull'API, vedere [DescribePatchGroupState](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **DescribePatchGroups** con una CLI

I seguenti esempi di codice mostrano come usare `DescribePatchGroups`.

### CLI

#### AWS CLI

Per visualizzare le registrazioni dei gruppi di patch

L'esempio seguente `describe-patch-groups` elenca le registrazioni dei gruppi di patch.

```
aws ssm describe-patch-groups
```

Output:

```
{
 "Mappings": [
 {
 "PatchGroup": "Production",
 "BaselineIdentity": {
 "BaselineId": "pb-0123456789abcdef0",
 "BaselineName": "ProdPatching",
 "OperatingSystem": "WINDOWS",
 "BaselineDescription": "Patches for Production",
 "DefaultBaseline": false
 }
 },
 {
```

```

 "PatchGroup": "Development",
 "BaselineIdentity": {
 "BaselineId": "pb-0713accee01234567",
 "BaselineName": "DevPatching",
 "OperatingSystem": "WINDOWS",
 "BaselineDescription": "Patches for Development",
 "DefaultBaseline": true
 },
 ...
]
}

```

Per ulteriori informazioni, vedere [Create a Patch Group < https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-group-tagging.html >](https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-group-tagging.html) e [Add a Patch Group to a Patch Baseline](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [DescribePatchGroups](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca le registrazioni dei gruppi di patch.

```
Get-SSMPatchGroup
```

Output:

BaselineIdentity	PatchGroup
-----	-----
Amazon.SimpleSystemsManagement.Model.PatchBaselineIdentity	Production

- Per i dettagli sull'API, vedere [DescribePatchGroups](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca le registrazioni dei gruppi di patch.

```
Get-SSMPatchGroup
```

**Output:**

BaselineIdentity	PatchGroup
-----	-----
Amazon.SimpleSystemsManagement.Model.PatchBaselineIdentity	Production

- Per i dettagli sull'API, vedere [DescribePatchGroups](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

**Utilizzo di `GetAutomationExecution` con una CLI**

I seguenti esempi di codice mostrano come usare `GetAutomationExecution`.

**CLI****AWS CLI**

Per visualizzare i dettagli sull'esecuzione di un'automazione

L'esempio seguente `get-automation-execution` visualizza informazioni dettagliate sull'esecuzione di un'automazione.

```
aws ssm get-automation-execution \
 --automation-execution-id 73c8eef8-f4ee-4a05-820c-e354fEXAMPLE
```

**Output:**

```
{
 "AutomationExecution": {
 "AutomationExecutionId": "73c8eef8-f4ee-4a05-820c-e354fEXAMPLE",
 "DocumentName": "AWS-StartEC2Instance",
 "DocumentVersion": "1",
 "ExecutionStartTime": 1583737233.748,
 "ExecutionEndTime": 1583737234.719,
 "AutomationExecutionStatus": "Success",
 "StepExecutions": [
```

```

 {
 "StepName": "startInstances",
 "Action": "aws:changeInstanceState",
 "ExecutionStartTime": 1583737234.134,
 "ExecutionEndTime": 1583737234.672,
 "StepStatus": "Success",
 "Inputs": {
 "DesiredState": "\"running\"",
 "InstanceIds": "[\"i-0cb99161f6EXAMPLE\"]"
 },
 "Outputs": {
 "InstanceStates": [
 "running"
]
 },
 "StepExecutionId": "95e70479-cf20-4d80-8018-7e4e2EXAMPLE",
 "OverriddenParameters": {}
 }
],
 "StepExecutionsTruncated": false,
 "Parameters": {
 "AutomationAssumeRole": [
 ""
],
 "InstanceId": [
 "i-0cb99161f6EXAMPLE"
]
 },
 "Outputs": {},
 "Mode": "Auto",
 "ExecutedBy": "arn:aws:sts::29884EXAMPLE:assumed-role/mw_service_role/OrchestrationService",
 "Targets": [],
 "ResolvedTargets": {
 "ParameterValues": [],
 "Truncated": false
 }
}
}

```

Per ulteriori informazioni, vedere [Walkthrough: Patch a Linux AMI \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [GetAutomationExecution](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio visualizza i dettagli di un'esecuzione di automazione.

```
Get-SSMAutomationExecution -AutomationExecutionId "4105a4fc-f944-11e6-9d32-8fb2db27a909"
```

Output:

```
AutomationExecutionId : 4105a4fc-f944-11e6-9d32-8fb2db27a909
AutomationExecutionStatus : Failed
DocumentName : AWS-UpdateLinuxAmi
DocumentVersion : 1
ExecutionEndTime : 2/22/2017 9:17:08 PM
ExecutionStartTime : 2/22/2017 9:17:02 PM
FailureMessage : Step launchInstance failed maximum allowed times. You
 are not authorized to perform this operation. Encoded
 authorization failure message:
 B_V2QyyN7NhSZQYpmVzpEc4oSnj2GLTNYnXUHsTbqJkNMdGubmbtthLmZyaiUYek0RIrA42-
 fv1x-04q5Fjff6glh
 Yb6TI5b0GQeeNrpwNvpDzm0-
 PSR1swlAbg9fdM9BcNjyrznspUkWpuKu9EC10u6v30XU1KC9nZ7mPlWMFZNkSioQqpWWEvMw-
 GZktsQzm67q0hUhBN0LWYhbS
 pkfiqzY-5nw3S0obx30fhd3EJa50_-
 GjV_a0nFXQJa70ik40bF0rEh3MtCSbrQT6--DvFy_FQ8TKvkIXadyVskeJI84X0F5WmA60f1pi5GI08i-
 nRfZS6oDeU

 gELBjjoFKD8s3L2aI0B6umWVxnQ0jqhQRxwJ53b54sZJ2PW3v_mtg9-q0CK0ezS3xfh_y0ilaUG0AZG-
 xjQFuvU_JZedWpla3xi-MZsmbIAifBI
 (Service: AmazonEC2; Status Code: 403; Error Code:
 UnauthorizedOperation; Request ID:
 6a002f94-ba37-43fd-99e6-39517715fce5)
Outputs : {[createImage.ImageId,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
Parameters : {[AutomationAssumeRole,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]], [InstanceIamRole,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]], [SourceAmiId,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
```

```
StepExecutions : {launchInstance, updateOSSoftware, stopInstance,
 createImage...}
```

Esempio 2: questo esempio elenca i dettagli della fase per l'ID di esecuzione dell'automazione specificato

```
Get-SSMAutomationExecution -AutomationExecutionId e1d2bad3-4567-8901-
ae23-456c7c8901be | Select-Object -ExpandProperty StepExecutions | Select-Object
 StepName, Action, StepStatus, ValidNextSteps
```

Output:

StepName	Action	StepStatus	ValidNextSteps
-----	-----	-----	-----
LaunchInstance	aws:runInstances	Success	
{OSCompatibilityCheck}			
OSCompatibilityCheck	aws:runCommand	Success	{RunPreUpdateScript}
RunPreUpdateScript	aws:runCommand	Success	{UpdateEC2Config}
UpdateEC2Config	aws:runCommand	Cancelled	{}
UpdateSSMAgent	aws:runCommand	Pending	{}
UpdateAWSPVDriver	aws:runCommand	Pending	{}
UpdateAWSEnaNetworkDriver	aws:runCommand	Pending	{}
UpdateAWSNVMe	aws:runCommand	Pending	{}
InstallWindowsUpdates	aws:runCommand	Pending	{}
RunPostUpdateScript	aws:runCommand	Pending	{}
RunSysprepGeneralize	aws:runCommand	Pending	{}
StopInstance	aws:changeInstanceState	Pending	{}
CreateImage	aws:createImage	Pending	{}
TerminateInstance	aws:changeInstanceState	Pending	{}

- Per i dettagli sull'API, vedere [GetAutomationExecution](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: questo esempio visualizza i dettagli di un'esecuzione di automazione.

```
Get-SSMAutomationExecution -AutomationExecutionId "4105a4fc-
f944-11e6-9d32-8fb2db27a909"
```

Output:



```

AutomationExecutionId : 4105a4fc-f944-11e6-9d32-8fb2db27a909
AutomationExecutionStatus : Failed
DocumentName : AWS-UpdateLinuxAmi
DocumentVersion : 1
ExecutionEndTime : 2/22/2017 9:17:08 PM
ExecutionStartTime : 2/22/2017 9:17:02 PM
FailureMessage : Step launchInstance failed maximum allowed times. You
 are not authorized to perform this operation. Encoded
 authorization failure message:
 B_V2QyyN7NhSZQYpmVzpEc4oSnj2GLTNYnXUHsTbqJkNMdGubmbtthLmZyaiUYek0RIrA42-
 fv1x-04q5Fjff6glh
 Yb6TI5b0GQeeNrpwNvpDzm0-
 PSR1swlAbg9fdM9BcNjyrznspUkWpuKu9EC10u6v30XU1KC9nZ7mPlWMFZNkSioQqpWWEvMw-
 GZktsQzm67q0hUhBNOLWYhbS
 pkfiqzY-5nw3S0obx30fhd3EJa50_-
 GjV_a0nFXQJa70ik40bF0rEh3MtCSbrQT6--DvFy_FQ8TKvkIXadyVskeJI84X0F5WmA60f1pi5GI08i-
 nRfZS6oDeU

 gELBjjoFKD8s3L2aI0B6umWVxnQ0jqhQRxwJ53b54sZJ2PW3v_mtg9-q0CK0ezS3xfh_y0ilaUG0AZG-
 xjQFuvU_JZedWpla3xi-MZsmbIAifBI
 (Service: AmazonEC2; Status Code: 403; Error Code:
 UnauthorizedOperation; Request ID:
 6a002f94-ba37-43fd-99e6-39517715fce5)
Outputs : {[createImage.ImageId,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
Parameters : {[AutomationAssumeRole,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]], [InstanceIamRole,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]], [SourceAmiId,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
StepExecutions : {launchInstance, updateOSSoftware, stopInstance,
 createImage...}

```

Esempio 2: questo esempio elenca i dettagli della fase per l'ID di esecuzione dell'automazione specificato

```

Get-SSMAutomationExecution -AutomationExecutionId e1d2bad3-4567-8901-
ae23-456c7c8901be | Select-Object -ExpandProperty StepExecutions | Select-Object
StepName, Action, StepStatus, ValidNextSteps

```

Output:

StepName	Action	StepStatus	ValidNextSteps
-----	-----	-----	-----
LaunchInstance	aws:runInstances	Success	
{OSCompatibilityCheck}			
OSCompatibilityCheck	aws:runCommand	Success	{RunPreUpdateScript}
RunPreUpdateScript	aws:runCommand	Success	{UpdateEC2Config}
UpdateEC2Config	aws:runCommand	Cancelled	{}
UpdateSSMAgent	aws:runCommand	Pending	{}
UpdateAWSPVDriver	aws:runCommand	Pending	{}
UpdateAWSEnaNetworkDriver	aws:runCommand	Pending	{}
UpdateAWSNVMe	aws:runCommand	Pending	{}
InstallWindowsUpdates	aws:runCommand	Pending	{}
RunPostUpdateScript	aws:runCommand	Pending	{}
RunSysprepGeneralize	aws:runCommand	Pending	{}
StopInstance	aws:changeInstanceState	Pending	{}
CreateImage	aws:createImage	Pending	{}
TerminateInstance	aws:changeInstanceState	Pending	{}

- Per i dettagli sull'API, vedere [GetAutomationExecution](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **GetCommandInvocation** con una CLI

I seguenti esempi di codice mostrano come usare `GetCommandInvocation`.

### CLI

#### AWS CLI

Per visualizzare i dettagli di una invocazione di comando

L'esempio seguente `get-command-invocation` elenca tutte le invocazioni del comando specificato sull'istanza specificata.

```
aws ssm get-command-invocation \
 --command-id "ef7fd8-9b57-4151-a15c-db9a12345678" \
 --instance-id "i-1234567890abcdef0"
```

## Output:

```
{
 "CommandId": "ef7fd8-9b57-4151-a15c-db9a12345678",
 "InstanceId": "i-1234567890abcdef0",
 "Comment": "b48291dd-ba76-43e0-b9df-13e11ddaac26:6960febb-2907-4b59-8e1a-d6ce8EXAMPLE",
 "DocumentName": "AWS-UpdateSSMAgent",
 "DocumentVersion": "",
 "PluginName": "aws:updateSsmAgent",
 "ResponseCode": 0,
 "ExecutionStartDateTime": "2020-02-19T18:18:03.419Z",
 "ExecutionElapsedTime": "PT0.091S",
 "ExecutionEndDateTime": "2020-02-19T18:18:03.419Z",
 "Status": "Success",
 "StatusDetails": "Success",
 "StandardOutputContent": "Updating amazon-ssm-agent from 2.3.842.0 to latest\nSuccessfully downloaded https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/ssm-agent-manifest.json\namazon-ssm-agent 2.3.842.0 has already been installed, update skipped\n",
 "StandardOutputUrl": "",
 "StandardErrorContent": "",
 "StandardErrorUrl": "",
 "CloudWatchOutputConfig": {
 "CloudWatchLogGroupName": "",
 "CloudWatchOutputEnabled": false
 }
}
```

Per ulteriori informazioni, consulta [Informazioni sugli stati dei comandi](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [GetCommandInvocation](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio visualizza i dettagli di un comando eseguito su un'istanza.

```
Get-SSMCommandInvocationDetail -InstanceId "i-0cb2b964d3e14fd9f" -CommandId "b8eac879-0541-439d-94ec-47a80d554f44"
```

**Output:**

```
CommandId : b8eac879-0541-439d-94ec-47a80d554f44
Comment : IP config
DocumentName : AWS-RunShellScript
ExecutionElapsedTime : PT0.004S
ExecutionEndDateTime : 2017-02-22T20:13:16.651Z
ExecutionStartDateTime : 2017-02-22T20:13:16.651Z
InstanceId : i-0cb2b964d3e14fd9f
PluginName : aws:runShellScript
ResponseCode : 0
StandardErrorContent :
StandardErrorUrl :
StandardOutputContent :
StandardOutputUrl :
Status : Success
StatusDetails : Success
```

- Per i dettagli sull'API, vedere [GetCommandInvocation](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

**Strumenti per V5 PowerShell**

Esempio 1: questo esempio visualizza i dettagli di un comando eseguito su un'istanza.

```
Get-SSMCommandInvocationDetail -InstanceId "i-0cb2b964d3e14fd9f" -CommandId
"b8eac879-0541-439d-94ec-47a80d554f44"
```

**Output:**

```
CommandId : b8eac879-0541-439d-94ec-47a80d554f44
Comment : IP config
DocumentName : AWS-RunShellScript
ExecutionElapsedTime : PT0.004S
ExecutionEndDateTime : 2017-02-22T20:13:16.651Z
ExecutionStartDateTime : 2017-02-22T20:13:16.651Z
InstanceId : i-0cb2b964d3e14fd9f
PluginName : aws:runShellScript
ResponseCode : 0
StandardErrorContent :
StandardErrorUrl :
StandardOutputContent :
StandardOutputUrl :
```

```
Status : Success
StatusDetails : Success
```

- Per i dettagli sull'API, vedere [GetCommandInvocation](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **GetConnectionStatus** con una CLI

I seguenti esempi di codice mostrano come usare `GetConnectionStatus`.

### CLI

#### AWS CLI

Per visualizzare lo stato della connessione di un'istanza gestita

Questo esempio `get-connection-status` restituisce lo stato della connessione dell'istanza gestita specificata.

```
aws ssm get-connection-status \
 --target i-1234567890abcdef0
```

Output:

```
{
 "Target": "i-1234567890abcdef0",
 "Status": "connected"
}
```

- Per i dettagli sull'API, vedi [GetConnectionStatus](#) in AWS CLI Command Reference.

### PowerShell

#### Strumenti per PowerShell V4

Esempio 1: questo esempio recupera lo stato della connessione di Session Manager per un'istanza per determinare se è connessa e pronta a ricevere connessioni a Session Manager.

```
Get-SSMConnectionStatus -Target i-0a1caf234f12d3dc4
```

Output:

Status	Target
-----	-----
Connected	i-0a1caf234f12d3dc4

- Per i dettagli sull'API, vedere [GetConnectionStatus](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio recupera lo stato della connessione di Session Manager per un'istanza per determinare se è connessa e pronta a ricevere connessioni a Session Manager.

```
Get-SSMConnectionStatus -Target i-0a1caf234f12d3dc4
```

Output:

Status	Target
-----	-----
Connected	i-0a1caf234f12d3dc4

- Per i dettagli sull'API, vedere [GetConnectionStatus](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **GetDefaultPatchBaseline** con una CLI

I seguenti esempi di codice mostrano come usare `GetDefaultPatchBaseline`.

### CLI

#### AWS CLI

Esempio 1: per visualizzare la baseline delle patch di Windows predefinita

L'esempio seguente `get-default-patch-baseline` recupera i dettagli per la baseline delle patch predefinita per Windows Server.

```
aws ssm get-default-patch-baseline
```

Output:

```
{
 "BaselineId": "pb-0713accee01612345",
 "OperatingSystem": "WINDOWS"
}
```

Esempio 2: come visualizzare la baseline delle patch predefinita per Amazon Linux

L'esempio seguente `get-default-patch-baseline` recupera i dettagli per la baseline delle patch predefinita per Amazon Linux.

```
aws ssm get-default-patch-baseline \
 --operating-system AMAZON_LINUX
```

Output:

```
{
 "BaselineId": "pb-047c6eb9c8fc12345",
 "OperatingSystem": "AMAZON_LINUX"
}
```

Per ulteriori informazioni, vedere Informazioni sulle baseline delle patch predefinite e personalizzate < <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-baselines.html> >\_\_ e [Impostare una baseline di patch esistente come predefinita](#) nella Guida per l'utente di Systems Manager. AWS

- Per i dettagli sulle API, vedere in Command Reference. [GetDefaultPatchBaseline](#) AWS CLI

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio visualizza la baseline delle patch predefinita.

```
Get-SSMDefaultPatchBaseline
```

Output:

```
arn:aws:ssm:us-west-2:123456789012:patchbaseline/pb-04fb4ae6142167966
```

- Per i dettagli sull'API, vedere [GetDefaultPatchBaseline](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: questo esempio visualizza la baseline delle patch predefinita.

```
Get-SSMDefaultPatchBaseline
```

Output:

```
arn:aws:ssm:us-west-2:123456789012:patchbaseline/pb-04fb4ae6142167966
```

- Per i dettagli sull'API, vedere [GetDefaultPatchBaseline](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **GetDeployablePatchSnapshotForInstance** con una CLI

I seguenti esempi di codice mostrano come usare `GetDeployablePatchSnapshotForInstance`.

CLI

AWS CLI

Per recuperare l'istantanea corrente per la baseline delle patch, un'istanza utilizza

L'esempio seguente `get-deployable-patch-snapshot-for-instance` recupera i dettagli dello snapshot corrente per la baseline delle patch specificata utilizzata da un'istanza. Questo comando deve essere eseguito dall'istanza utilizzando le credenziali dell'istanza. Per



assicurarti che utilizzi le credenziali dell'istanza, esegui `aws configure` e specifica solo la Regione dell'istanza. Lascia i campi `Access Key` e `Secret Key` vuoti.

Suggerimento: Utilizza `uuidgen` per generare un `snapshot-id`.

```
aws ssm get-deployable-patch-snapshot-for-instance \
 --instance-id "i-1234567890abcdef0" \
 --snapshot-id "521c3536-930c-4aa9-950e-01234567abcd"
```

Output:

```
{
 "InstanceId": "i-1234567890abcdef0",
 "SnapshotId": "521c3536-930c-4aa9-950e-01234567abcd",
 "Product": "AmazonLinux2018.03",
 "SnapshotDownloadUrl": "https://patch-baseline-snapshot-us-east-1.s3.amazonaws.com/ed85194ef27214f5984f28b4d664d14f7313568fea7d4b6ac6c10ad1f729d7e7-773304212436/AMAZON_LINUX-521c3536-930c-4aa9-950e-01234567abcd?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20190215T164031Z&X-Amz-SignedHeaders=host&X-Amz-Expires=86400&X-Amz-Credential=AKIAJ5C56P35AEBRX2QQ%2F20190215%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Signature=efaaaf6e3878e77f48a6697e015efdbda9c426b09c5822055075c062f6ad2149"
}
```

Per ulteriori informazioni, consulta [Nome parametro: Snapshot ID](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [GetDeployablePatchSnapshotForInstance](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio visualizza l'istantanea corrente per la baseline delle patch utilizzata da un'istanza. Questo comando deve essere eseguito dall'istanza utilizzando le credenziali dell'istanza. Per garantire che utilizzi le credenziali dell'istanza, l'esempio passa un oggetto **Amazon.Runtime.InstanceProfileAWSCredentials** al parametro `Credentials`.

```
$credentials = [Amazon.Runtime.InstanceProfileAWSCredentials]::new()
```

```
Get-SSMDeployablePatchSnapshotForInstance -SnapshotId "4681775b-098f-4435-
a956-0ef33373ac11" -InstanceId "i-0cb2b964d3e14fd9f" -Credentials $credentials
```

Output:

```
InstanceId SnapshotDownloadUrl

i-0cb2b964d3e14fd9f https://patch-baseline-snapshot-us-west-2.s3-us-
west-2.amazonaws.com/853d0d3db0f0cafe...1692/4681775b-098f-4435...
```

Esempio 2: Questo esempio mostra come ottenere il massimo SnapshotDownloadUrl. Questo comando deve essere eseguito dall'istanza utilizzando le credenziali dell'istanza. Per assicurarsi che utilizzi le credenziali dell'istanza, l'esempio configura la PowerShell sessione per l'utilizzo di un **Amazon.Runtime.InstanceProfileAWSCredentials** oggetto.

```
Set-AWSCredential -Credential
([Amazon.Runtime.InstanceProfileAWSCredentials]::new())
(Get-SSMDeployablePatchSnapshotForInstance -SnapshotId "4681775b-098f-4435-
a956-0ef33373ac11" -InstanceId "i-0cb2b964d3e14fd9f").SnapshotDownloadUrl
```

Output:

```
https://patch-baseline-snapshot-us-west-2.s3-us-
west-2.amazonaws.com/853d0d3db0f0cafe...
```

- Per i dettagli sull'API, vedere [GetDeployablePatchSnapshotForInstance](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio visualizza l'istantanea corrente per la baseline delle patch utilizzata da un'istanza. Questo comando deve essere eseguito dall'istanza utilizzando le credenziali dell'istanza. Per garantire che utilizzi le credenziali dell'istanza, l'esempio passa un oggetto **Amazon.Runtime.InstanceProfileAWSCredentials** al parametro Credentials.

```
$credentials = [Amazon.Runtime.InstanceProfileAWSCredentials]::new()
Get-SSMDeployablePatchSnapshotForInstance -SnapshotId "4681775b-098f-4435-
a956-0ef33373ac11" -InstanceId "i-0cb2b964d3e14fd9f" -Credentials $credentials
```

Output:

InstanceId	SnapshotDownloadUrl
-----	-----
i-0cb2b964d3e14fd9f	https://patch-baseline-snapshot-us-west-2.s3-us-west-2.amazonaws.com/853d0d3db0f0cafe...1692/4681775b-098f-4435...

Esempio 2: Questo esempio mostra come ottenere il massimo SnapshotDownloadUrl. Questo comando deve essere eseguito dall'istanza utilizzando le credenziali dell'istanza. Per assicurarsi che utilizzi le credenziali dell'istanza, l'esempio configura la PowerShell sessione per l'utilizzo di un **Amazon.Runtime.InstanceProfileAWSCredentials** oggetto.

```
Set-AWSCredential -Credential
([Amazon.Runtime.InstanceProfileAWSCredentials]::new())
(Get-SSMDeployablePatchSnapshotForInstance -SnapshotId "4681775b-098f-4435-
a956-0ef33373ac11" -InstanceId "i-0cb2b964d3e14fd9f").SnapshotDownloadUrl
```

Output:

```
https://patch-baseline-snapshot-us-west-2.s3-us-
west-2.amazonaws.com/853d0d3db0f0cafe...
```

- Per i dettagli sull'API, vedere [GetDeployablePatchSnapshotForInstance](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **GetDocument** con una CLI

I seguenti esempi di codice mostrano come usare `GetDocument`.

### CLI

#### AWS CLI

Per ottenere il contenuto del documento

L'esempio seguente `get-document` visualizza il contenuto di un documento Systems Manager.

```
aws ssm get-document \
 --name "AWS-RunShellScript"
```

Output:

```
{
 "Name": "AWS-RunShellScript",
 "DocumentVersion": "1",
 "Status": "Active",
 "Content": "{\n \"schemaVersion\": \"1.2\", \n \"description\": \"Run\na shell script or specify the commands to run.\", \n \"parameters\": {\n \"commands\": {\n \"type\": \"StringList\", \n \"description\": \"(Required) Specify a shell script or a command to run.\", \n \"minItems\": 1, \n \"displayType\": \"textarea\" \n }, \n \"workingDirectory\": {\n \"type\": \"String\", \n \"default\": \"\", \n \"description\": \"(Optional) The\npath to the working directory on your instance.\", \n \"maxChars\n\": 4096 \n }, \n \"executionTimeout\": {\n \"type\":\n\"String\", \n \"default\": \"3600\", \n \"description\n\": \"(Optional) The time in seconds for a command to complete before it is\nconsidered to have failed. Default is 3600 (1 hour). Maximum is 172800 (48\nhours).\", \n \"allowedPattern\": \"([1-9][0-9]{0,4})|(1[0-6][0-9]{4})|(17[0-1][0-9]{3})|(172[0-7][0-9]{2})|(172800)\" \n }, \n \"runtimeConfig\": {\n \"aws:runShellScript\": {\n \"properties\n\": [\n {\n \"id\": \"0.aws:runShellScript\n\", \n \"runCommand\": \"{{ commands }}\", \n \"workingDirectory\": \"{{ workingDirectory }}\", \n \"timeoutSeconds\": \"{{ executionTimeout }}\" \n } \n] \n } \n }, \n \"DocumentType\": \"Command\", \n \"DocumentFormat\": \"JSON\"\n}"
```

Per ulteriori informazioni, consulta [Documenti di AWS Systems Manager](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [GetDocument](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio restituisce il contenuto di un documento.

```
Get-SSMDocument -Name "RunShellScript"
```

Output:

```
Content

{...
```

Esempio 2: questo esempio visualizza il contenuto completo di un documento.

```
(Get-SSMDocument -Name "RunShellScript").Content
{
 "schemaVersion":"2.0",
 "description":"Run an updated script",
 "parameters":{
 "commands":{
 "type":"StringList",
 "description":"(Required) Specify a shell script or a command to run.",
 "minItems":1,
 "displayType":"textarea"
 }
 },
 "mainSteps":[
 {
 "action":"aws:runShellScript",
 "name":"runShellScript",
 "inputs":{
 "commands":"{{ commands }}"
 }
 },
 {
 "action":"aws:runPowerShellScript",
 "name":"runPowerShellScript",
 "inputs":{
 "commands":"{{ commands }}"
 }
 }
]
}
```

```
}
]
}
```

- Per i dettagli sull'API, vedere [GetDocument](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio restituisce il contenuto di un documento.

```
Get-SSMDocument -Name "RunShellScript"
```

Output:

```
Content

{...
```

Esempio 2: questo esempio visualizza il contenuto completo di un documento.

```
(Get-SSMDocument -Name "RunShellScript").Content
{
 "schemaVersion":"2.0",
 "description":"Run an updated script",
 "parameters":{
 "commands":{
 "type":"StringList",
 "description":"(Required) Specify a shell script or a command to run.",
 "minItems":1,
 "displayType":"textarea"
 }
 },
 "mainSteps":[
 {
 "action":"aws:runShellScript",
 "name":"runShellScript",
 "inputs":{
 "commands":"{{ commands }}"
 }
 },
 {
 "action":"aws:runPowerShellScript",
```

```
 "name": "runPowerShellScript",
 "inputs": {
 "commands": "{{ commands }}"
 }
 }
]
```

- Per i dettagli sull'API, vedere [GetDocument](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **GetInventory** con una CLI

I seguenti esempi di codice mostrano come usare `GetInventory`.

### CLI

#### AWS CLI

Per visualizzare l'inventario

Questo esempio ottiene i metadati personalizzati per l'inventario.

Comando:

```
aws ssm get-inventory
```

Output:

```
{
 "Entities": [
 {
 "Data": {
 "AWS:InstanceInformation": {
 "Content": [
 {
 "ComputerName": "ip-172-31-44-222.us-
west-2.compute.internal",
```

```

 "InstanceId": "i-0cb2b964d3e14fd9f",
 "IpAddress": "172.31.44.222",
 "AgentType": "amazon-ssm-agent",
 "ResourceType": "EC2Instance",
 "AgentVersion": "2.0.672.0",
 "PlatformVersion": "2016.09",
 "PlatformName": "Amazon Linux AMI",
 "PlatformType": "Linux"
 },
 "TypeName": "AWS:InstanceInformation",
 "SchemaVersion": "1.0",
 "CaptureTime": "2017-02-20T18:03:58Z"
},
{
 "Id": "i-0cb2b964d3e14fd9f"
}
]
}

```

- Per i dettagli sull'API, vedi [GetInventory](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio ottiene i metadati personalizzati per l'inventario.

```
Get-SSMInventory
```

Output:

```

Data
 Id

--
{[AWS:InstanceInformation,
 Amazon.SimpleSystemsManagement.Model.InventoryResultItem]} i-0cb2b964d3e14fd9f

```

- Per i dettagli sull'API, vedere [GetInventory](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).



## Strumenti per V5 PowerShell

Esempio 1: questo esempio ottiene i metadati personalizzati per l'inventario.

```
Get-SSMInventory
```

Output:

```
Data
 Id

 --
{[AWS:InstanceInformation,
 Amazon.SimpleSystemsManagement.Model.InventoryResultItem]} i-0cb2b964d3e14fd9f
```

- Per i dettagli sull'API, vedere [GetInventory](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **GetInventorySchema** con una CLI

I seguenti esempi di codice mostrano come usare `GetInventorySchema`.

### CLI

#### AWS CLI

Per visualizzare lo schema dell'inventario

Questo esempio restituisce un elenco di nomi di tipi di inventario per l'account.

Comando:

```
aws ssm get-inventory-schema
```

Output:

```
{
 "Schemas": [
```

```

{
 "TypeName": "AWS:AWSComponent",
 "Version": "1.0",
 "Attributes": [
 {
 "Name": "Name",
 "DataType": "STRING"
 },
 {
 "Name": "ApplicationType",
 "DataType": "STRING"
 },
 {
 "Name": "Publisher",
 "DataType": "STRING"
 },
 {
 "Name": "Version",
 "DataType": "STRING"
 },
 {
 "Name": "InstalledTime",
 "DataType": "STRING"
 },
 {
 "Name": "Architecture",
 "DataType": "STRING"
 },
 {
 "Name": "URL",
 "DataType": "STRING"
 }
],
 ...
],
 "NextToken": "--token string truncated--"
}

```

Come visualizzare lo schema di inventario per un tipo di inventario specifico

Questo esempio restituisce lo schema di inventario per un tipo di inventario AWS:AWS Component.

Comando:

```
aws ssm get-inventory-schema --type-name "AWS:AWSComponent"
```

- Per i dettagli sull'API, vedi [GetInventorySchema](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio restituisce un elenco di nomi dei tipi di inventario per l'account.

```
Get-SSMInventorySchema
```

- Per i dettagli sull'API, vedere [GetInventorySchema](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio restituisce un elenco di nomi dei tipi di inventario per l'account.

```
Get-SSMInventorySchema
```

- Per i dettagli sull'API, vedere [GetInventorySchema](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **GetMaintenanceWindow** con una CLI

I seguenti esempi di codice mostrano come usare `GetMaintenanceWindow`.

### CLI

#### AWS CLI

Per ottenere le informazioni su una finestra di manutenzione

L'esempio seguente `get-maintenance-window` recupera i dettagli sulla finestra di manutenzione specificata.

```
aws ssm get-maintenance-window \
 --window-id "mw-03eb9db428EXAMPLE"
```

Output:

```
{
 "AllowUnassociatedTargets": true,
 "CreateDate": 1515006912.957,
 "Cutoff": 1,
 "Duration": 6,
 "Enabled": true,
 "ModifiedDate": 2020-01-01T10:04:04.099Z,
 "Name": "My-Maintenance-Window",
 "Schedule": "rate(3 days)",
 "WindowId": "mw-03eb9db428EXAMPLE",
 "NextExecutionTime": "2020-02-25T00:08:15.099Z"
}
```

Per ulteriori informazioni, vedere [Visualizzare le informazioni sulle finestre di manutenzione \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [GetMaintenanceWindow](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio ottiene dettagli su una finestra di manutenzione.

```
Get-SSMMaintenanceWindow -WindowId "mw-03eb9db42890fb82d"
```

Output:

```
AllowUnassociatedTargets : False
CreateDate : 2/20/2017 6:14:05 PM
Cutoff : 1
Duration : 2
Enabled : True
```

```
ModifiedDate : 2/20/2017 6:14:05 PM
Name : TestMaintWin
Schedule : cron(0 */30 * * * ? *)
WindowId : mw-03eb9db42890fb82d
```

- Per i dettagli sull'API, vedere [GetMaintenanceWindow](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio ottiene dettagli su una finestra di manutenzione.

```
Get-SSMMaintenanceWindow -WindowId "mw-03eb9db42890fb82d"
```

Output:

```
AllowUnassociatedTargets : False
CreatedDate : 2/20/2017 6:14:05 PM
Cutoff : 1
Duration : 2
Enabled : True
ModifiedDate : 2/20/2017 6:14:05 PM
Name : TestMaintWin
Schedule : cron(0 */30 * * * ? *)
WindowId : mw-03eb9db42890fb82d
```

- Per i dettagli sull'API, vedere [GetMaintenanceWindow](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta.

[L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **GetMaintenanceWindowExecution** con una CLI

I seguenti esempi di codice mostrano come usare `GetMaintenanceWindowExecution`.

### CLI

#### AWS CLI

Per ottenere informazioni sull'esecuzione di un'attività in una finestra di manutenzione

L'esempio seguente `get-maintenance-window-execution` elenca le informazioni su un'attività eseguita come parte dell'esecuzione della finestra di manutenzione specificata.

```
aws ssm get-maintenance-window-execution \
 --window-execution-id "518d5565-5969-4cca-8f0e-da3b2EXAMPLE"
```

Output:

```
{
 "Status": "SUCCESS",
 "TaskIds": [
 "ac0c6ae1-daa3-4a89-832e-d3845EXAMPLE"
],
 "StartTime": 1487692834.595,
 "EndTime": 1487692835.051,
 "WindowExecutionId": "518d5565-5969-4cca-8f0e-da3b2EXAMPLE",
}
```

Per ulteriori informazioni, vedere [View Information About Tasks and Task Executions \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [GetMaintenanceWindowExecution](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca le informazioni su un'attività eseguita nell'ambito di un'esecuzione di una finestra di manutenzione.

```
Get-SSMMaintenanceWindowExecution -WindowExecutionId "518d5565-5969-4cca-8f0e-da3b2a638355"
```

Output:

```
EndTime : 2/21/2017 4:00:35 PM
StartTime : 2/21/2017 4:00:34 PM
Status : FAILED
StatusDetails : One or more tasks in the orchestration failed.
TaskIds : {ac0c6ae1-daa3-4a89-832e-d384503b6586}
```

```
WindowExecutionId : 518d5565-5969-4cca-8f0e-da3b2a638355
```

- Per i dettagli sull'API, vedere [GetMaintenanceWindowExecution](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca le informazioni su un'attività eseguita nell'ambito di un'esecuzione di una finestra di manutenzione.

```
Get-SSMMaintenanceWindowExecution -WindowExecutionId "518d5565-5969-4cca-8f0e-da3b2a638355"
```

### Output:

```
EndTime : 2/21/2017 4:00:35 PM
StartTime : 2/21/2017 4:00:34 PM
Status : FAILED
StatusDetails : One or more tasks in the orchestration failed.
TaskIds : {ac0c6ae1-daa3-4a89-832e-d384503b6586}
WindowExecutionId : 518d5565-5969-4cca-8f0e-da3b2a638355
```

- Per i dettagli sull'API, vedere [GetMaintenanceWindowExecution](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **GetMaintenanceWindowExecutionTask** con una CLI

I seguenti esempi di codice mostrano come usare `GetMaintenanceWindowExecutionTask`.

### CLI

#### AWS CLI

Per ottenere informazioni sull'esecuzione di un'attività in una finestra di manutenzione

L'esempio seguente `get-maintenance-window-execution-task` elenca le informazioni su un'attività che fa parte dell'esecuzione della finestra di manutenzione specificata.

```
aws ssm get-maintenance-window-execution-task \
 --window-execution-id "518d5565-5969-4cca-8f0e-da3b2EXAMPLE" \
 --task-id "ac0c6ae1-daa3-4a89-832e-d3845EXAMPLE"
```

Output:

```
{
 "WindowExecutionId": "518d5565-5969-4cca-8f0e-da3b2EXAMPLE",
 "TaskExecutionId": "ac0c6ae1-daa3-4a89-832e-d3845EXAMPLE",
 "TaskArn": "AWS-RunPatchBaseline",
 "ServiceRole": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
 "Type": "RUN_COMMAND",
 "TaskParameters": [
 {
 "BaselineOverride": {
 "Values": [
 ""
]
 },
 "InstallOverrideList": {
 "Values": [
 ""
]
 },
 "Operation": {
 "Values": [
 "Scan"
]
 },
 "RebootOption": {
 "Values": [
 "RebootIfNeeded"
]
 },
 "SnapshotId": {
 "Values": [
 "{{ aws:ORCHESTRATION_ID }}"
]
 },
 "aws:InstanceId": {
 "Values": [
 "i-02573cafcfEXAMPLE",

```



```

 "i-0471e04240EXAMPLE",
 "i-07782c72faEXAMPLE"
]
}
}
],
"Priority": 1,
"MaxConcurrency": "1",
"MaxErrors": "3",
"Status": "SUCCESS",
"StartTime": "2021-08-04T11:45:35.088000-07:00",
"EndTime": "2021-08-04T11:53:09.079000-07:00"
}

```

Per ulteriori informazioni, vedere [Visualizzare le informazioni sulle attività e sulle esecuzioni delle attività \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [GetMaintenanceWindowExecutionTask](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca le informazioni su un'attività che faceva parte dell'esecuzione di una finestra di manutenzione.

```
Get-SSMMaintenanceWindowExecutionTask -TaskId "ac0c6ae1-daa3-4a89-832e-d384503b6586" -WindowExecutionId "518d5565-5969-4cca-8f0e-da3b2a638355"
```

### Output:

```

EndTime : 2/21/2017 4:00:35 PM
MaxConcurrency : 1
MaxErrors : 1
Priority : 10
ServiceRole : arn:aws:iam::123456789012:role/MaintenanceWindowsRole
StartTime : 2/21/2017 4:00:34 PM
Status : FAILED
StatusDetails : The maximum error count was exceeded.
TaskArn : AWS-RunShellScript
TaskExecutionId : ac0c6ae1-daa3-4a89-832e-d384503b6586

```

```
TaskParameters :
 {Amazon.Runtime.Internal.Util.AlwaysSendDictionary`2[System.String,Amazon.SimpleSystemsM
 meterValueExpression]}
Type : RUN_COMMAND
WindowExecutionId : 518d5565-5969-4cca-8f0e-da3b2a638355
```

- Per i dettagli sull'API, vedere [GetMaintenanceWindowExecutionTask](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca le informazioni su un'attività che faceva parte dell'esecuzione di una finestra di manutenzione.

```
Get-SSMMaintenanceWindowExecutionTask -TaskId "ac0c6ae1-daa3-4a89-832e-
d384503b6586" -WindowExecutionId "518d5565-5969-4cca-8f0e-da3b2a638355"
```

### Output:

```
EndTime : 2/21/2017 4:00:35 PM
MaxConcurrency : 1
MaxErrors : 1
Priority : 10
ServiceRole : arn:aws:iam::123456789012:role/MaintenanceWindowsRole
StartTime : 2/21/2017 4:00:34 PM
Status : FAILED
StatusDetails : The maximum error count was exceeded.
TaskArn : AWS-RunShellScript
TaskExecutionId : ac0c6ae1-daa3-4a89-832e-d384503b6586
TaskParameters :
 {Amazon.Runtime.Internal.Util.AlwaysSendDictionary`2[System.String,Amazon.SimpleSystemsM
 meterValueExpression]}
Type : RUN_COMMAND
WindowExecutionId : 518d5565-5969-4cca-8f0e-da3b2a638355
```

- Per i dettagli sull'API, vedere [GetMaintenanceWindowExecutionTask](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Usare **GetParameter** con un AWS SDK o CLI

I seguenti esempi di codice mostrano come usare `GetParameter`.

### CLI

#### AWS CLI

Esempio 1: per visualizzare il valore di un parametro

L'esempio seguente `get-parameter` elenca il valore per il singolo parametro specificato.

```
aws ssm get-parameter \
 --name "MyStringParameter"
```

Output:

```
{
 "Parameter": {
 "Name": "MyStringParameter",
 "Type": "String",
 "Value": "Veni",
 "Version": 1,
 "LastModifiedDate": 1530018761.888,
 "ARN": "arn:aws:ssm:us-east-2:111222333444:parameter/MyStringParameter"
 "DataType": "text"
 }
}
```

Per ulteriori informazioni, consulta [Utilizzo dell'Archivio parametri](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 2: per decrittografare il valore di un parametro `SecureString`

L'esempio seguente `get-parameter` decrittografa il valore del parametro specificato `SecureString`.

```
aws ssm get-parameter \
 --name "MySecureStringParameter" \
 --with-decryption
```

Output:

```
{
 "Parameter": {
 "Name": "MySecureStringParameter",
 "Type": "SecureString",
 "Value": "16679b88-310b-4895-a943-e0764EXAMPLE",
 "Version": 2,
 "LastModifiedDate": 1582155479.205,
 "ARN": "arn:aws:ssm:us-east-2:111222333444:parameter/MySecureStringParameter",
 "DataType": "text"
 }
}
```

Per ulteriori informazioni, consulta [Utilizzo dell'Archivio parametri](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 3: come visualizzare il valore di un parametro utilizzando le etichette

L'esempio seguente `get-parameter` elenca il valore per il singolo parametro specificato con un'etichetta specificata.

```
aws ssm get-parameter \
 --name "MyParameter:label"
```

Output:

```
{
 "Parameter": {
 "Name": "MyParameter",
 "Type": "String",
 "Value": "parameter version 2",
 "Version": 2,
 "Selector": ":label",
 "LastModifiedDate": "2021-07-12T09:49:15.865000-07:00",
 "ARN": "arn:aws:ssm:us-west-2:786973925828:parameter/MyParameter",
 "DataType": "text"
 }
}
```

Per ulteriori informazioni, consulta [Utilizzo delle versioni dei parametri](#) nella Guida per l'utente di AWS Systems Manager.

## Esempio 4: come visualizzare il valore di un parametro utilizzando le versioni

L'esempio seguente `get-parameter` elenca il valore per la versione a parametro singolo specificata.

```
aws ssm get-parameter \
 --name "MyParameter:2"
```

Output:

```
{
 "Parameter": {
 "Name": "MyParameter",
 "Type": "String",
 "Value": "parameter version 2",
 "Version": 2,
 "Selector": ":2",
 "LastModifiedDate": "2021-07-12T09:49:15.865000-07:00",
 "ARN": "arn:aws:ssm:us-west-2:786973925828:parameter/MyParameter",
 "DataType": "text"
 }
}
```

Per ulteriori informazioni, consulta [Utilizzo delle versioni dei parametri](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [GetParameter](#) in AWS CLI Command Reference.

## Rust

### SDK per Rust

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
pub async fn list_path(&self, path: &str) -> Result<Vec<Parameter>, EC2Error>
{
 let maybe_params: Vec<Result<Parameter, _>> = TryFlatMap::new(
 <Vec<Result<Parameter, _>>, EC2Error>>
```

```

 self.inner
 .get_parameters_by_path()
 .path(path)
 .into_paginator()
 .send(),
)
 .flat_map(|item| item.parameters.unwrap_or_default())
 .collect()
 .await;
// Fail on the first error
let params = maybe_params
 .into_iter()
 .collect::

```

- Per i dettagli sulle API, consulta [GetParameter](#) la sezione AWS SDK for Rust API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **GetParameterHistory** con una CLI

I seguenti esempi di codice mostrano come usare `GetParameterHistory`.

### CLI

#### AWS CLI

Per ottenere una cronologia dei valori per un parametro

L'esempio seguente `get-parameter-history` elenca la cronologia delle modifiche per il parametro specificato, incluso il relativo valore.

```
aws ssm get-parameter-history \
 --name "MyStringParameter"
```

Output:

```
{
 "Parameters": [
 {
 "Name": "MyStringParameter",
 "Type": "String",
 "LastModifiedDate": 1582154711.976,
 "LastModifiedUser": "arn:aws:iam::111222333444:user/Mary-Major",
 "Description": "This is the first version of my String parameter",
 "Value": "Veni",
 "Version": 1,
 "Labels": [],
 "Tier": "Standard",
 "Policies": []
 },
 {
 "Name": "MyStringParameter",
 "Type": "String",
 "LastModifiedDate": 1582156093.471,
 "LastModifiedUser": "arn:aws:iam::111222333444:user/Mary-Major",
 "Description": "This is the second version of my String parameter",
 "Value": "Vidi",
 "Version": 2,
 "Labels": [],
 "Tier": "Standard",
 "Policies": []
 },
 {
 "Name": "MyStringParameter",
 "Type": "String",
 "LastModifiedDate": 1582156117.545,
 "LastModifiedUser": "arn:aws:iam::111222333444:user/Mary-Major",
 "Description": "This is the third version of my String parameter",
 "Value": "Vici",
 "Version": 3,
 "Labels": [],
 "Tier": "Standard",
 "Policies": []
 }
]
}
```

Per ulteriori informazioni, consulta [Utilizzo delle versioni dei parametri](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [GetParameterHistory](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca la cronologia dei valori di un parametro.

```
Get-SSMParameterHistory -Name "Welcome"
```

Output:

```
Description :
KeyId :
LastModifiedDate : 3/3/2017 6:55:25 PM
LastModifiedUser : arn:aws:iam::123456789012:user/admin
Name : Welcome
Type : String
Value : helloWorld
```

- Per i dettagli sull'API, vedere [GetParameterHistory](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca la cronologia dei valori di un parametro.

```
Get-SSMParameterHistory -Name "Welcome"
```

Output:

```
Description :
KeyId :
LastModifiedDate : 3/3/2017 6:55:25 PM
LastModifiedUser : arn:aws:iam::123456789012:user/admin
Name : Welcome
Type : String
Value : helloWorld
```

- Per i dettagli sull'API, vedere [GetParameterHistory](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).



Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **GetParameters** con una CLI

I seguenti esempi di codice mostrano come usare `GetParameters`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- [Creazione di un servizio contenitore per istanze di macchine virtuali](#)

### CLI

#### AWS CLI

Esempio 1: come elencare i valori di un parametro

L'esempio seguente `get-parameters` elenca i valori dei tre parametri specificati.

```
aws ssm get-parameters \
 --names "MyStringParameter" "MyStringListParameter" "MyInvalidParameterName"
```

Output:

```
{
 "Parameters": [
 {
 "Name": "MyStringListParameter",
 "Type": "StringList",
 "Value": "alpha,beta,gamma",
 "Version": 1,
 "LastModifiedDate": 1582154764.222,
 "ARN": "arn:aws:ssm:us-east-2:111222333444:parameter/
MyStringListParameter"
 "DataType": "text"
 },
 {
 "Name": "MyStringParameter",
 "Type": "String",
 "Value": "Vici",
 }
]
}
```

```

 "Version": 3,
 "LastModifiedDate": 1582156117.545,
 "ARN": "arn:aws:ssm:us-east-2:111222333444:parameter/
MyStringParameter"
 "DataType": "text"
 }
],
 "InvalidParameters": [
 "MyInvalidParameterName"
]
}

```

Per ulteriori informazioni, consulta [Utilizzo dell'Archivio parametri](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 2: come elencare i nomi e i valori di più parametri utilizzando l'opzione ``--query``

L'esempio seguente `get-parameters` elenca i nomi e i valori dei parametri specificati.

```

aws ssm get-parameters \
 --names MyStringParameter MyStringListParameter \
 --query "Parameters[*].{Name:Name,Value:Value}"

```

Output:

```

[
 {
 "Name": "MyStringListParameter",
 "Value": "alpha,beta,gamma"
 },
 {
 "Name": "MyStringParameter",
 "Value": "Vidi"
 }
]

```

Per ulteriori informazioni, consulta [Utilizzo dell'Archivio parametri](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 3: come visualizzare il valore di un parametro utilizzando le etichette

L'esempio seguente `get-parameter` elenca il valore per il singolo parametro specificato con un'etichetta specificata.

```
aws ssm get-parameter \
 --name "MyParameter:label"
```

Output:

```
{
 "Parameters": [
 {
 "Name": "MyLabelParameter",
 "Type": "String",
 "Value": "parameter by label",
 "Version": 1,
 "Selector": ":label",
 "LastModifiedDate": "2021-07-12T09:49:15.865000-07:00",
 "ARN": "arn:aws:ssm:us-west-2:786973925828:parameter/MyParameter",
 "DataType": "text"
 },
 {
 "Name": "MyVersionParameter",
 "Type": "String",
 "Value": "parameter by version",
 "Version": 2,
 "Selector": ":2",
 "LastModifiedDate": "2021-03-24T16:20:28.236000-07:00",
 "ARN": "arn:aws:ssm:us-west-2:786973925828:parameter/unlabel-param",
 "DataType": "text"
 }
],
 "InvalidParameters": []
}
```

Per ulteriori informazioni, consulta [Utilizzo delle versioni dei parametri](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [GetParameters](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca i valori di un parametro.

```
Get-SSMParameterValue -Name "Welcome"
```

Output:

```
InvalidParameters Parameters

{} {Welcome}
```

Esempio 2: questo esempio elenca i dettagli del valore.

```
(Get-SSMParameterValue -Name "Welcome").Parameters
```

Output:

```
Name Type Value
---- -
Welcome String Good day, Sunshine!
```

- Per i dettagli sull'API, vedere [GetParameters](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca i valori di un parametro.

```
Get-SSMParameterValue -Name "Welcome"
```

Output:

```
InvalidParameters Parameters

{} {Welcome}
```

Esempio 2: questo esempio elenca i dettagli del valore.

```
(Get-SSMParameterValue -Name "Welcome").Parameters
```

Output:

```
Name Type Value
```

```

Welcome String Good day, Sunshine!
```

- Per i dettagli sull'API, vedere [GetParameters](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **GetPatchBaseline** con una CLI

I seguenti esempi di codice mostrano come usare `GetPatchBaseline`.

### CLI

#### AWS CLI

Visualizzazione di una baseline delle patch

Nell'esempio seguente `get-patch-baseline` vengono recuperati i dettagli per la baseline delle patch specificata.

```
aws ssm get-patch-baseline \
 --baseline-id "pb-0123456789abcdef0"
```

Output:

```
{
 "BaselineId": "pb-0123456789abcdef0",
 "Name": "WindowsPatching",
 "OperatingSystem": "WINDOWS",
 "GlobalFilters": {
 "PatchFilters": []
 },
 "ApprovalRules": {
 "PatchRules": [
 {
 "PatchFilterGroup": {
 "PatchFilters": [
 {
 "Key": "PRODUCT",
```

```

 "Values": [
 "WindowsServer2016"
]
 },
 "ComplianceLevel": "CRITICAL",
 "ApproveAfterDays": 0,
 "EnableNonSecurity": false
}
],
},
"ApprovedPatches": [],
"ApprovedPatchesComplianceLevel": "UNSPECIFIED",
"ApprovedPatchesEnableNonSecurity": false,
"RejectedPatches": [],
"RejectedPatchesAction": "ALLOW_AS_DEPENDENCY",
"PatchGroups": [
 "QA",
 "DEV"
],
"CreateDate": 1550244180.465,
"ModifiedDate": 1550244180.465,
"Description": "Patches for Windows Servers",
"Sources": []
}

```

Per ulteriori informazioni, consulta [informazioni baseline delle patch](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [GetPatchBaseline](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio mostra i dettagli di una baseline delle patch.

```
Get-SSMPatchBaselineDetail -BaselineId "pb-03da896ca3b68b639"
```

Output:

```
ApprovalRules : Amazon.SimpleSystemsManagement.Model.PatchRuleGroup
```

```
ApprovedPatches : {}
BaselineId : pb-03da896ca3b68b639
CreatedDate : 3/3/2017 5:02:19 PM
Description : Baseline containing all updates approved for production systems
GlobalFilters : Amazon.SimpleSystemsManagement.Model.PatchFilterGroup
ModifiedDate : 3/3/2017 5:02:19 PM
Name : Production-Baseline
PatchGroups : {}
RejectedPatches : {}
```

- Per i dettagli sull'API, vedere [GetPatchBaseline](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio mostra i dettagli di una baseline delle patch.

```
Get-SSMPatchBaselineDetail -BaselineId "pb-03da896ca3b68b639"
```

#### Output:

```
ApprovalRules : Amazon.SimpleSystemsManagement.Model.PatchRuleGroup
ApprovedPatches : {}
BaselineId : pb-03da896ca3b68b639
CreatedDate : 3/3/2017 5:02:19 PM
Description : Baseline containing all updates approved for production systems
GlobalFilters : Amazon.SimpleSystemsManagement.Model.PatchFilterGroup
ModifiedDate : 3/3/2017 5:02:19 PM
Name : Production-Baseline
PatchGroups : {}
RejectedPatches : {}
```

- Per i dettagli sull'API, vedere [GetPatchBaseline](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

### Utilizzo di **GetPatchBaselineForPatchGroup** con una CLI

I seguenti esempi di codice mostrano come usare `GetPatchBaselineForPatchGroup`.

## CLI

### AWS CLI

Per visualizzare la baseline delle patch per un gruppo di patch

L'esempio seguente `get-patch-baseline-for-patch-group` recupera i dettagli relativi alla baseline delle patch per il gruppo di patch specificato.

```
aws ssm get-patch-baseline-for-patch-group \
 --patch-group "DEV"
```

Output:

```
{
 "PatchGroup": "DEV",
 "BaselineId": "pb-0123456789abcdef0",
 "OperatingSystem": "WINDOWS"
}
```

Per ulteriori informazioni, vedere [Create a Patch Group < https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-group-tagging.html >](https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-group-tagging.html) e [Add a Patch Group to a Patch Baseline](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [GetPatchBaselineForPatchGroup](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio mostra la baseline delle patch per un gruppo di patch.

```
Get-SSMPatchBaselineForPatchGroup -PatchGroup "Production"
```

Output:

BaselineId	PatchGroup
pb-045f10b4f382baeda	Production



- Per i dettagli sull'API, vedere [GetPatchBaselineForPatchGroup](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio mostra la baseline delle patch per un gruppo di patch.

```
Get-SSMPatchBaselineForPatchGroup -PatchGroup "Production"
```

Output:

BaselineId	PatchGroup
-----	-----
pb-045f10b4f382baeda	Production

- Per i dettagli sull'API, vedere [GetPatchBaselineForPatchGroup](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **ListAssociationVersions** con una CLI

I seguenti esempi di codice mostrano come usare `ListAssociationVersions`.

### CLI

#### AWS CLI

Per recuperare tutte le versioni di un'associazione per un determinato ID di associazione

L'esempio seguente `list-association-versions` elenca tutte le versioni delle associazioni specificate.

```
aws ssm list-association-versions \
 --association-id "8dfe3659-4309-493a-8755-0123456789ab"
```

Output:

```
{
 "AssociationVersions": [

```

```
{
 "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
 "AssociationVersion": "1",
 "CreateDate": 1550505536.726,
 "Name": "AWS-UpdateSSMAgent",
 "Parameters": {
 "allowDowngrade": [
 "false"
],
 "version": [
 ""
]
 },
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
 "i-1234567890abcdef0"
]
 }
],
 "ScheduleExpression": "cron(0 00 12 ? * SUN *)",
 "AssociationName": "UpdateSSMAgent"
}
]
```

Per ulteriori informazioni, consulta [Utilizzo delle associazioni in Systems Manager](#) nella AWS Guida per l'utente di Systems Manager.

- Per i dettagli sull'API, vedi [ListAssociationVersions](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio recupera tutte le versioni dell'associazione fornita.

```
Get-SSMAssociationVersionList -AssociationId 123a45a0-c678-9012-3456-78901234db5e
```

Output:

```
AssociationId : 123a45a0-c678-9012-3456-78901234db5e
```

```

AssociationName :
AssociationVersion : 2
ComplianceSeverity :
CreatedDate : 3/12/2019 9:21:01 AM
DocumentVersion :
MaxConcurrency :
MaxErrors :
Name : AWS-GatherSoftwareInventory
OutputLocation :
Parameters : {}
ScheduleExpression :
Targets : {InstanceIds}

AssociationId : 123a45a0-c678-9012-3456-78901234db5e
AssociationName : test-case-1234567890
AssociationVersion : 1
ComplianceSeverity :
CreatedDate : 3/2/2019 8:53:29 AM
DocumentVersion :
MaxConcurrency :
MaxErrors :
Name : AWS-GatherSoftwareInventory
OutputLocation :
Parameters : {}
ScheduleExpression : rate(30minutes)
Targets : {InstanceIds}

```

- Per i dettagli sull'API, vedere [ListAssociationVersions](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio recupera tutte le versioni dell'associazione fornita.

```
Get-SSMAssociationVersionList -AssociationId 123a45a0-c678-9012-3456-78901234db5e
```

Output:

```

AssociationId : 123a45a0-c678-9012-3456-78901234db5e
AssociationName :
AssociationVersion : 2
ComplianceSeverity :
CreatedDate : 3/12/2019 9:21:01 AM

```

```

DocumentVersion :
MaxConcurrency :
MaxErrors :
Name : AWS-GatherSoftwareInventory
OutputLocation :
Parameters : {}
ScheduleExpression :
Targets : {InstanceIds}

AssociationId : 123a45a0-c678-9012-3456-78901234db5e
AssociationName : test-case-1234567890
AssociationVersion : 1
ComplianceSeverity :
CreatedDate : 3/2/2019 8:53:29 AM
DocumentVersion :
MaxConcurrency :
MaxErrors :
Name : AWS-GatherSoftwareInventory
OutputLocation :
Parameters : {}
ScheduleExpression : rate(30minutes)
Targets : {InstanceIds}

```

- Per i dettagli sull'API, vedere [ListAssociationVersions](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **ListAssociations** con una CLI

I seguenti esempi di codice mostrano come usare `ListAssociations`.

### CLI

#### AWS CLI

Esempio 1: per elencare le associazioni per un'istanza specifica

Il seguente esempio di elenco di associazioni elenca tutte le associazioni con `UpdateSSMAgent`. `AssociationName`

```
aws ssm list-associations /
 --association-filter-list "key=AssociationName,value=UpdateSSMAgent"
```

Output:

```
{
 "Associations": [
 {
 "Name": "AWS-UpdateSSMAgent",
 "InstanceId": "i-1234567890abcdef0",
 "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
 "AssociationVersion": "1",
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
 "i-016648b75dd622dab"
]
 }
],
 "Overview": {
 "Status": "Pending",
 "DetailedStatus": "Associated",
 "AssociationStatusAggregatedCount": {
 "Pending": 1
 }
 },
 "ScheduleExpression": "cron(0 00 12 ? * SUN *)",
 "AssociationName": "UpdateSSMAgent"
 }
]
}
```

Per ulteriori informazioni, consulta [Utilizzo delle associazioni in Systems Manager](#) nella Guida per l'utente di Systems Manager.

Esempio 2: come elencare le associazioni per un documento specifico

Il seguente esempio di associazioni di elenchi elenca tutte le associazioni per il documento specificato.

```
aws ssm list-associations /
```

```
--association-filter-list "key=Name,value=AWS-UpdateSSMAgent"
```

Output:

```
{
 "Associations": [
 {
 "Name": "AWS-UpdateSSMAgent",
 "InstanceId": "i-1234567890abcdef0",
 "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
 "AssociationVersion": "1",
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
 "i-1234567890abcdef0"
]
 }
],
 "LastExecutionDate": 1550505828.548,
 "Overview": {
 "Status": "Success",
 "DetailedStatus": "Success",
 "AssociationStatusAggregatedCount": {
 "Success": 1
 }
 },
 "ScheduleExpression": "cron(0 00 12 ? * SUN *)",
 "AssociationName": "UpdateSSMAgent"
 },
 {
 "Name": "AWS-UpdateSSMAgent",
 "InstanceId": "i-9876543210abcdef0",
 "AssociationId": "fbc07ef7-b985-4684-b82b-0123456789ab",
 "AssociationVersion": "1",
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
 "i-9876543210abcdef0"
]
 }
]
 }
],
}
```

```

 "LastExecutionDate": 1550507531.0,
 "Overview": {
 "Status": "Success",
 "AssociationStatusAggregatedCount": {
 "Success": 1
 }
 }
 }
]
}

```

Per ulteriori informazioni, consulta [Utilizzo delle associazioni in Systems Manager](#) nella Guida per l'utente di Systems Manager.

- Per i dettagli sull'API, vedere in Command Reference. [ListAssociations](#) AWS CLI

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca tutte le associazioni per un'istanza. La sintassi utilizzata da questo esempio richiede la PowerShell versione 3 o successiva.

```

$filter1 = @{"Key"="InstanceId";Value=@"i-0000293ffd8c57862"}
Get-SSMAssociationList -AssociationFilterList $filter1

```

Output:

```

AssociationId : d8617c07-2079-4c18-9847-1655fc2698b0
DocumentVersion :
InstanceId : i-0000293ffd8c57862
LastExecutionDate : 2/20/2015 8:31:11 AM
Name : AWS-UpdateSSMAgent
Overview : Amazon.SimpleSystemsManagement.Model.AssociationOverview
ScheduleExpression :
Targets : {InstanceIds}

```

Esempio 2: questo esempio elenca tutte le associazioni per un documento di configurazione. La sintassi utilizzata in questo esempio richiede la PowerShell versione 3 o successiva.

```

$filter2 = @{"Key"="Name";Value=@"AWS-UpdateSSMAgent"}

```

```
Get-SSMAssociationList -AssociationFilterList $filter2
```

**Output:**

```
AssociationId : d8617c07-2079-4c18-9847-1655fc2698b0
DocumentVersion :
InstanceId : i-0000293ffd8c57862
LastExecutionDate : 2/20/2015 8:31:11 AM
Name : AWS-UpdateSSMAgent
Overview : Amazon.SimpleSystemsManagement.Model.AssociationOverview
ScheduleExpression :
Targets : {InstanceIds}
```

Esempio 3: con PowerShell la versione 2, è necessario utilizzare New-Object per creare ciascun filtro.

```
$filter1 = New-Object Amazon.SimpleSystemsManagement.Model.AssociationFilter
$filter1.Key = "InstanceId"
$filter1.Value = "i-0000293ffd8c57862"

Get-SSMAssociationList -AssociationFilterList $filter1
```

**Output:**

```
AssociationId : d8617c07-2079-4c18-9847-1655fc2698b0
DocumentVersion :
InstanceId : i-0000293ffd8c57862
LastExecutionDate : 2/20/2015 8:31:11 AM
Name : AWS-UpdateSSMAgent
Overview : Amazon.SimpleSystemsManagement.Model.AssociationOverview
ScheduleExpression :
Targets : {InstanceIds}
```

- Per i dettagli sull'API, vedere [ListAssociations](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

**Strumenti per V5 PowerShell**

Esempio 1: questo esempio elenca tutte le associazioni per un'istanza. La sintassi utilizzata da questo esempio richiede la PowerShell versione 3 o successiva.

```
$filter1 = @{"Key"="InstanceId";Value=@"i-0000293ffd8c57862"}
```



```
Get-SSMAssociationList -AssociationFilterList $filter1
```

**Output:**

```
AssociationId : d8617c07-2079-4c18-9847-1655fc2698b0
DocumentVersion :
InstanceId : i-0000293ffd8c57862
LastExecutionDate : 2/20/2015 8:31:11 AM
Name : AWS-UpdateSSMAgent
Overview : Amazon.SimpleSystemsManagement.Model.AssociationOverview
ScheduleExpression :
Targets : {InstanceIds}
```

Esempio 2: questo esempio elenca tutte le associazioni per un documento di configurazione. La sintassi utilizzata in questo esempio richiede la PowerShell versione 3 o successiva.

```
$filter2 = @{"Key"="Name";Value=@"AWS-UpdateSSMAgent"}
Get-SSMAssociationList -AssociationFilterList $filter2
```

**Output:**

```
AssociationId : d8617c07-2079-4c18-9847-1655fc2698b0
DocumentVersion :
InstanceId : i-0000293ffd8c57862
LastExecutionDate : 2/20/2015 8:31:11 AM
Name : AWS-UpdateSSMAgent
Overview : Amazon.SimpleSystemsManagement.Model.AssociationOverview
ScheduleExpression :
Targets : {InstanceIds}
```

Esempio 3: con PowerShell la versione 2, è necessario utilizzare New-Object per creare ciascun filtro.

```
$filter1 = New-Object Amazon.SimpleSystemsManagement.Model.AssociationFilter
$filter1.Key = "InstanceId"
$filter1.Value = "i-0000293ffd8c57862"

Get-SSMAssociationList -AssociationFilterList $filter1
```

**Output:**

```
AssociationId : d8617c07-2079-4c18-9847-1655fc2698b0
DocumentVersion :
InstanceId : i-0000293ffd8c57862
LastExecutionDate : 2/20/2015 8:31:11 AM
Name : AWS-UpdateSSMAgent
Overview : Amazon.SimpleSystemsManagement.Model.AssociationOverview
ScheduleExpression :
Targets : {InstanceIds}
```

- Per i dettagli sull'API, vedere [ListAssociations](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Usare **ListCommandInvocations** con un AWS SDK o CLI

I seguenti esempi di codice mostrano come usare `ListCommandInvocations`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- [Informazioni di base](#)

### CLI

#### AWS CLI

Come elencare le invocazioni di un comando specifico

L'esempio seguente `list-command-invocations` elenca tutte le invocazioni di un comando.

```
aws ssm list-command-invocations \
 --command-id "ef7fd8-9b57-4151-a15c-db9a12345678" \
 --details
```

Output:

```

{
 "CommandInvocations": [
 {
 "CommandId": "ef7fd8-9b57-4151-a15c-db9a12345678",
 "InstanceId": "i-02573cafcfEXAMPLE",
 "InstanceName": "",
 "Comment": "b48291dd-ba76-43e0-b9df-13e11ddaac26:6960febb-2907-4b59-8e1a-d6ce8EXAMPLE",
 "DocumentName": "AWS-UpdateSSMAgent",
 "DocumentVersion": "",
 "RequestedDateTime": 1582136283.089,
 "Status": "Success",
 "StatusDetails": "Success",
 "StandardOutputUrl": "",
 "StandardErrorUrl": "",
 "CommandPlugins": [
 {
 "Name": "aws:updateSsmAgent",
 "Status": "Success",
 "StatusDetails": "Success",
 "ResponseCode": 0,
 "ResponseStartDateTime": 1582136283.419,
 "ResponseFinishDateTime": 1582136283.51,
 "Output": "Updating amazon-ssm-agent from 2.3.842.0 to latest\nSuccessfully downloaded https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/ssm-agent-manifest.json\namazon-ssm-agent 2.3.842.0 has already been installed, update skipped\n",
 "StandardOutputUrl": "",
 "StandardErrorUrl": "",
 "OutputS3Region": "us-east-2",
 "OutputS3BucketName": "",
 "OutputS3KeyPrefix": ""
 }
],
 "ServiceRole": "",
 "NotificationConfig": {
 "NotificationArn": "",
 "NotificationEvents": [],
 "NotificationType": ""
 },
 "CloudWatchOutputConfig": {
 "CloudWatchLogGroupName": "",
 "CloudWatchOutputEnabled": false
 }
 }
]
}

```

```

 }
 },
 {
 "CommandId": "ef7fd8d8-9b57-4151-a15c-db9a12345678",
 "InstanceId": "i-0471e04240EXAMPLE",
 "InstanceName": "",
 "Comment": "b48291dd-ba76-43e0-b9df-13e11ddaac26:6960febb-2907-4b59-8e1a-d6ce8EXAMPLE",
 "DocumentName": "AWS-UpdateSSMAgent",
 "DocumentVersion": "",
 "RequestedDateTime": 1582136283.02,
 "Status": "Success",
 "StatusDetails": "Success",
 "StandardOutputUrl": "",
 "StandardErrorUrl": "",
 "CommandPlugins": [
 {
 "Name": "aws:updateSsmAgent",
 "Status": "Success",
 "StatusDetails": "Success",
 "ResponseCode": 0,
 "ResponseStartDateTime": 1582136283.812,
 "ResponseFinishDateTime": 1582136295.031,
 "Output": "Updating amazon-ssm-agent from 2.3.672.0 to
latest\nSuccessfully downloaded https://s3.us-east-2.amazonaws.com/amazon-
ssm-us-east-2/ssm-agent-manifest.json\nSuccessfully downloaded https://s3.us-
east-2.amazonaws.com/amazon-ssm-us-east-2/amazon-ssm-agent-updater/2.3.842.0/
amazon-ssm-agent-updater-snap-amd64.tar.gz\nSuccessfully downloaded https://
s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/amazon-ssm-agent/2.3.672.0/
amazon-ssm-agent-snap-amd64.tar.gz\nSuccessfully downloaded https://s3.us-
east-2.amazonaws.com/amazon-ssm-us-east-2/amazon-ssm-agent/2.3.842.0/amazon-ssm-
agent-snap-amd64.tar.gz\nInitiating amazon-ssm-agent update to 2.3.842.0\namazon-
ssm-agent updated successfully to 2.3.842.0",
 "StandardOutputUrl": "",
 "StandardErrorUrl": "",
 "OutputS3Region": "us-east-2",
 "OutputS3BucketName": "",
 "OutputS3KeyPrefix": "8bee3135-398c-4d31-99b6-e42d2EXAMPLE/
i-0471e04240EXAMPLE/awsupdateSsmAgent"
 }
],
 "ServiceRole": "",
 "NotificationConfig": {
 "NotificationArn": "",

```

```

 "NotificationEvents": [],
 "NotificationType": ""
 },
 "CloudWatchOutputConfig": {
 "CloudWatchLogGroupName": "",
 "CloudWatchOutputEnabled": false
 }
}
]
}

```

Per ulteriori informazioni, consulta [Informazioni sugli stati dei comandi](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [ListCommandInvocations](#) in AWS CLI Command Reference.

## JavaScript

### SDK per JavaScript (v3)

#### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```

import { paginateListCommandInvocations, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * List SSM command invocations on an instance.
 * @param {{ instanceId: string }}
 */
export const main = async ({ instanceId }) => {
 const client = new SSMClient({});
 try {
 const listCommandInvocationsPaginated = [];
 // The paginate function is a wrapper around the base command.
 const paginator = paginateListCommandInvocations(
 { client },
 {
 InstanceId: instanceId,
 }
);
 }
};

```

```

 },
);
 for await (const page of paginator) {
 listCommandInvocationsPaginated.push(...page.CommandInvocations);
 }
 console.log("Here is the list of command invocations:");
 console.log(listCommandInvocationsPaginated);
 return { CommandInvocations: listCommandInvocationsPaginated };
} catch (caught) {
 if (caught instanceof Error && caught.name === "ValidationError") {
 console.warn(`${caught.message}. Did you provide a valid instance ID?`);
 }
 throw caught;
}
};

```

- Per i dettagli sulle API, consulta la [ListCommandInvocations](#) sezione AWS SDK per JavaScript API Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca tutte le invocazioni di un comando.

```
Get-SSMCommandInvocation -CommandId "b8eac879-0541-439d-94ec-47a80d554f44" -
Detail $true
```

Output:

```

CommandId : b8eac879-0541-439d-94ec-47a80d554f44
CommandPlugins : {aws:runShellScript}
Comment : IP config
DocumentName : AWS-RunShellScript
InstanceId : i-0cb2b964d3e14fd9f
InstanceName :
NotificationConfig : Amazon.SimpleSystemsManagement.Model.NotificationConfig
RequestedDateTime : 2/22/2017 8:13:16 PM
ServiceRole :
StandardErrorUrl :
StandardOutputUrl :

```

```
Status : Success
StatusDetails : Success
TraceOutput :
```

Esempio 2: Questo esempio elenca l'invocazione del comando id CommandPlugins e1eb2e3c-ed4c-5123-45c1-234f5612345f

```
Get-SSMCommandInvocation -CommandId e1eb2e3c-ed4c-5123-45c1-234f5612345f -Detail:
$true | Select-Object -ExpandProperty CommandPlugins
```

Output:

```
Name : aws:runPowerShellScript
Output : Completed 17.7 KiB/17.7 KiB (40.1 KiB/s) with 1 file(s)
 remainingdownload: s3://dd-aess-r-ctmer/KUM0.png to ..\..\programdata\KUM0.png
 kumo available

OutputS3BucketName :
OutputS3KeyPrefix :
OutputS3Region : eu-west-1
ResponseCode : 0
ResponseFinishDateTime : 4/3/2019 11:53:23 AM
ResponseStartDateTime : 4/3/2019 11:53:21 AM
StandardErrorUrl :
StandardOutputUrl :
Status : Success
StatusDetails : Success
```

- AWS Strumenti per PowerShell Per i dettagli sull'API, vedere in [Cmdlet Reference \(V4\)](#).  
[ListCommandInvocations](#)

## Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca tutte le invocazioni di un comando.

```
Get-SSMCommandInvocation -CommandId "b8eac879-0541-439d-94ec-47a80d554f44" -
Detail $true
```

Output:

```
CommandId : b8eac879-0541-439d-94ec-47a80d554f44
```

```

CommandPlugins : {aws:runShellScript}
Comment : IP config
DocumentName : AWS-RunShellScript
InstanceId : i-0cb2b964d3e14fd9f
InstanceName :
NotificationConfig : Amazon.SimpleSystemsManagement.Model.NotificationConfig
RequestedDateTime : 2/22/2017 8:13:16 PM
ServiceRole :
StandardErrorUrl :
StandardOutputUrl :
Status : Success
StatusDetails : Success
TraceOutput :

```

Esempio 2: Questo esempio elenca l'invocazione del comando id CommandPlugins e1eb2e3c-ed4c-5123-45c1-234f5612345f

```

Get-SSMCommandInvocation -CommandId e1eb2e3c-ed4c-5123-45c1-234f5612345f -Detail:
$true | Select-Object -ExpandProperty CommandPlugins

```

Output:

```

Name : aws:runPowerShellScript
Output : Completed 17.7 KiB/17.7 KiB (40.1 KiB/s) with 1 file(s)
 remainingdownload: s3://dd-aess-r-ctmer/KUM0.png to ..\..\programdata\KUM0.png
 kumo available

OutputS3BucketName :
OutputS3KeyPrefix :
OutputS3Region : eu-west-1
ResponseCode : 0
ResponseFinishDateTime : 4/3/2019 11:53:23 AM
ResponseStartDateTime : 4/3/2019 11:53:21 AM
StandardErrorUrl :
StandardOutputUrl :
Status : Success
StatusDetails : Success

```

- AWS Strumenti per PowerShell Per i dettagli sull'API, vedere in [Cmdlet Reference \(V5\)](#).  
[ListCommandInvocations](#)



## Python

### SDK per Python (Boto3)

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
class DocumentWrapper:
 """Encapsulates AWS Systems Manager Document actions."""

 def __init__(self, ssm_client):
 """
 :param ssm_client: A Boto3 Systems Manager client.
 """
 self.ssm_client = ssm_client
 self.name = None

 @classmethod
 def from_client(cls):
 ssm_client = boto3.client("ssm")
 return cls(ssm_client)

 def list_command_invocations(self, instance_id):
 """
 Lists the commands for an instance.

 :param instance_id: The ID of the instance.
 :return: The list of commands.
 """
 try:
 paginator = self.ssm_client.get_paginator("list_command_invocations")
 command_invocations = []
 for page in paginator.paginate(InstanceId=instance_id):
 command_invocations.extend(page["CommandInvocations"])
 num_of_commands = len(command_invocations)
 print(
 f"{num_of_commands} command invocation(s) found for instance {instance_id}."
)
```

```

)

 if num_of_commands > 10:
 print("Displaying the first 10 commands:")
 num_of_commands = 10
 date_format = "%A, %d %B %Y %I:%M%p"
 for command in command_invocations[:num_of_commands]:
 print(
 f" The time of command invocation is
{command['RequestedDateTime'].strftime(date_format)}"
)
 except ClientError as err:
 logger.error(
 "Couldn't list commands for %s. Here's why: %s: %s",
 instance_id,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise

```

- Per i dettagli sulle API, vedi [ListCommandInvocations](#) in AWS SDK for Python (Boto3) API Reference.

## SAP ABAP

### SDK per SAP ABAP

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

#### TRY.

```

" Use paginator to get all results
DATA(lo_paginator) = lo_ssm->get_paginator().
DATA(lo_iterator) = lo_paginator->listcommandinvocations(
 iv_instanceid = iv_instance_id).

```

```

DATA lv_count TYPE i VALUE 0.

WHILE lo_iterator->has_next().
 DATA(lo_result) = CAST /aws1/cl_ssmlistcmdinvcsresult(lo_iterator-
>get_next()).
 LOOP AT lo_result->get_commandinvocations() INTO DATA(lo_invocation).
 lv_count = lv_count + 1.
 DATA(lv_requested_datetime) = lo_invocation-
>get_requesteditime().
 MESSAGE |Command invocation requested at: { lv_requested_datetime }|
TYPE 'I'.
 ENDLLOOP.
ENDWHILE.

MESSAGE |{ lv_count } command invocation(s) found for instance
{ iv_instance_id }.| TYPE 'I'.
CATCH /aws1/cx_ssminvalidinstanceid.
 MESSAGE 'Invalid instance ID.' TYPE 'I'.
CATCH /aws1/cx_ssminvalidcommandid.
 MESSAGE 'Invalid command ID.' TYPE 'I'.
ENDTRY.

```

- Per i dettagli sulle API, consulta [ListCommandInvocations](#) la sezione AWS SDK for SAP ABAP API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **ListCommands** con una CLI

I seguenti esempi di codice mostrano come usare `ListCommands`.

### CLI

#### AWS CLI

Esempio 1: per ottenere lo stato di un comando specifico

L'esempio seguente `list-commands` recupera e visualizza lo stato del comando specificato.

```
aws ssm list-commands \
```

```
--command-id "0831e1a8-a1ac-4257-a1fd-c831bEXAMPLE"
```

Esempio 2: come ottenere lo stato dei comandi richiesti dopo una data specifica

L'esempio seguente `list-commands` recupera i dettagli dei comandi richiesti dopo la data specificata.

```
aws ssm list-commands \
 --filter "key=InvokedAfter,value=2020-02-01T00:00:00Z"
```

Esempio 3: elencare tutti i comandi richiesti in un account AWS

L'esempio seguente `list-commands` elenca tutti i comandi richiesti dagli utenti nell'AWS account corrente e nella regione.

```
aws ssm list-commands
```

Output:

```
{
 "Commands": [
 {
 "CommandId": "8bee3135-398c-4d31-99b6-e42d2EXAMPLE",
 "DocumentName": "AWS-UpdateSSMAgent",
 "DocumentVersion": "",
 "Comment": "b48291dd-ba76-43e0-b9df-13e11ddaac26:6960febb-2907-4b59-8e1a-d6ce8EXAMPLE",
 "ExpiresAfter": "2020-02-19T11:28:02.500000-08:00",
 "Parameters": {},
 "InstanceIds": [
 "i-028ea792daEXAMPLE",
 "i-02feef8c46EXAMPLE",
 "i-038613f3f0EXAMPLE",
 "i-03a530a2d4EXAMPLE",
 "i-083b678d37EXAMPLE",
 "i-0dee81debaEXAMPLE"
],
 "Targets": [],
 "RequestedDateTime": "2020-02-19T10:18:02.500000-08:00",
 "Status": "Success",
 "StatusDetails": "Success",
 "OutputS3BucketName": ""
 }
]
}
```

```

 "OutputS3KeyPrefix": "",
 "MaxConcurrency": "50",
 "MaxErrors": "100%",
 "TargetCount": 6,
 "CompletedCount": 6,
 "ErrorCount": 0,
 "DeliveryTimedOutCount": 0,
 "ServiceRole": "",
 "NotificationConfig": {
 "NotificationArn": "",
 "NotificationEvents": [],
 "NotificationType": ""
 },
 "CloudWatchOutputConfig": {
 "CloudWatchLogGroupName": "",
 "CloudWatchOutputEnabled": false
 }
 }
}
{
 "CommandId": "e9ade581-c03d-476b-9b07-26667EXAMPLE",
 "DocumentName": "AWS-FindWindowsUpdates",
 "DocumentVersion": "1",
 "Comment": "",
 "ExpiresAfter": "2020-01-24T12:37:31.874000-08:00",
 "Parameters": {
 "KbArticleIds": [
 ""
],
 "UpdateLevel": [
 "All"
]
 },
 "InstanceIds": [],
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
 "i-00ec29b21eEXAMPLE",
 "i-09911ddd90EXAMPLE"
]
 }
],
 "RequestedDateTime": "2020-01-24T11:27:31.874000-08:00",
 "Status": "Success",

```

```

 "StatusDetails": "Success",
 "OutputS3BucketName": "my-us-east-2-bucket",
 "OutputS3KeyPrefix": "my-rc-output",
 "MaxConcurrency": "50",
 "MaxErrors": "0",
 "TargetCount": 2,
 "CompletedCount": 2,
 "ErrorCount": 0,
 "DeliveryTimedOutCount": 0,
 "ServiceRole": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
 "NotificationConfig": {
 "NotificationArn": "arn:aws:sns:us-east-2:111222333444:my-us-
east-2-notification-arn",
 "NotificationEvents": [
 "All"
],
 "NotificationType": "Invocation"
 },
 "CloudWatchOutputConfig": {
 "CloudWatchLogGroupName": "",
 "CloudWatchOutputEnabled": false
 }
 }
}
{
 "CommandId": "d539b6c3-70e8-4853-80e5-0ce4fEXAMPLE",
 "DocumentName": "AWS-RunPatchBaseline",
 "DocumentVersion": "1",
 "Comment": "",
 "ExpiresAfter": "2020-01-24T12:21:04.350000-08:00",
 "Parameters": {
 "InstallOverrideList": [
 ""
],
 "Operation": [
 "Install"
],
 "RebootOption": [
 "RebootIfNeeded"
],
 "SnapshotId": [
 ""
]
 },

```

```

 "InstanceIds": [],
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
 "i-00ec29b21eEXAMPLE",
 "i-09911ddd90EXAMPLE"
]
 }
],
 "RequestedDateTime": "2020-01-24T11:11:04.350000-08:00",
 "Status": "Success",
 "StatusDetails": "Success",
 "OutputS3BucketName": "my-us-east-2-bucket",
 "OutputS3KeyPrefix": "my-rc-output",
 "MaxConcurrency": "50",
 "MaxErrors": "0",
 "TargetCount": 2,
 "CompletedCount": 2,
 "ErrorCount": 0,
 "DeliveryTimedOutCount": 0,
 "ServiceRole": "arn:aws:iam::111222333444:role/aws-service-role/ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
 "NotificationConfig": {
 "NotificationArn": "arn:aws:sns:us-east-2:111222333444:my-us-east-2-notification-arn",
 "NotificationEvents": [
 "All"
],
 "NotificationType": "Invocation"
 },
 "CloudWatchOutputConfig": {
 "CloudWatchLogGroupName": "",
 "CloudWatchOutputEnabled": false
 }
 }
]
}

```

Per ulteriori informazioni, consulta [Eseguire comandi utilizzando Systems Manager Run Command](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [ListCommands](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca tutti i comandi richiesti.

```
Get-SSMCommand
```

Output:

```
CommandId : 4b75a163-d39a-4d97-87c9-98ae52c6be35
Comment : Apply association with id at update time: 4cc73e42-
d5ae-4879-84f8-57e09c0efcd0
CompletedCount : 1
DocumentName : AWS-RefreshAssociation
ErrorCount : 0
ExpiresAfter : 2/24/2017 3:19:08 AM
InstanceIds : {i-0cb2b964d3e14fd9f}
MaxConcurrency : 50
MaxErrors : 0
NotificationConfig : Amazon.SimpleSystemsManagement.Model.NotificationConfig
OutputS3BucketName :
OutputS3KeyPrefix :
OutputS3Region :
Parameters : {[associationIds,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
RequestedDateTime : 2/24/2017 3:18:08 AM
ServiceRole :
Status : Success
StatusDetails : Success
TargetCount : 1
Targets : {}
```

Esempio 2: questo esempio ottiene lo stato di un comando specifico.

```
Get-SSMCommand -CommandId "4b75a163-d39a-4d97-87c9-98ae52c6be35"
```

Esempio 3: questo esempio recupera tutti i comandi SSM richiamati dopo il 01/04/2019 T00:00:00Z



```
Get-SSMCommand -Filter @{Key="InvokedAfter";Value="2019-04-01T00:00:00Z"} |
 Select-Object CommandId, DocumentName, Status, RequestedDateTime | Sort-Object -
 Property RequestedDateTime -Descending
```

### Output:

CommandId RequestedDateTime ----- -----	DocumentName -----	Status -----
edb1b23e-456a-7adb-aef8-90e-012ac34f 4/16/2019 5:45:23 AM	AWS-RunPowerShellScript	Cancelled
1a2dc3fb-4567-890d-a1ad-234b5d6bc7d9 4/6/2019 9:19:42 AM	AWS-ConfigureAWSPackage	Success
12c3456c-7e90-4f12-1232-1234f5b67893 4/2/2019 4:13:07 AM	KT-Retrieve-Cloud-Type-Win	Failed
fe123b45-240c-4123-a2b3-234bdd567ecf 4/1/2019 2:27:31 PM	AWS-RunInspecChecks	Failed
1eb23aa4-567d-4123-12a3-4c1c2ab34561 4/1/2019 1:05:55 PM	AWS-RunPowerShellScript	Success
1c2f3bb4-ee12-4bc1-1a23-12345eea123e 4/1/2019 11:13:09 AM	AWS-RunInspecChecks	Failed

- Per i dettagli sull'API, vedere [ListCommands](#) in Cmdlet Reference (V4). AWS Strumenti per PowerShell

### Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca tutti i comandi richiesti.

```
Get-SSMCommand
```

### Output:

```
CommandId : 4b75a163-d39a-4d97-87c9-98ae52c6be35
Comment : Apply association with id at update time: 4cc73e42-
d5ae-4879-84f8-57e09c0efcd0
CompletedCount : 1
DocumentName : AWS-RefreshAssociation
ErrorCount : 0
ExpiresAfter : 2/24/2017 3:19:08 AM
```

```

InstanceId : {i-0cb2b964d3e14fd9f}
MaxConcurrency : 50
MaxErrors : 0
NotificationConfig : Amazon.SimpleSystemsManagement.Model.NotificationConfig
OutputS3BucketName :
OutputS3KeyPrefix :
OutputS3Region :
Parameters : {[associationIds,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
RequestedDateTime : 2/24/2017 3:18:08 AM
ServiceRole :
Status : Success
StatusDetails : Success
TargetCount : 1
Targets : {}

```

Esempio 2: questo esempio ottiene lo stato di un comando specifico.

```
Get-SSMCommand -CommandId "4b75a163-d39a-4d97-87c9-98ae52c6be35"
```

Esempio 3: questo esempio recupera tutti i comandi SSM richiamati dopo il 01/04/2019 T00:00:00Z

```

Get-SSMCommand -Filter @{Key="InvokedAfter";Value="2019-04-01T00:00:00Z"} |
 Select-Object CommandId, DocumentName, Status, RequestedDateTime | Sort-Object -
 Property RequestedDateTime -Descending

```

Output:

CommandId RequestedDateTime ----- -----	DocumentName -----	Status -----
edb1b23e-456a-7adb-aef8-90e-012ac34f 4/16/2019 5:45:23 AM	AWS-RunPowerShellScript	Cancelled
1a2dc3fb-4567-890d-a1ad-234b5d6bc7d9 4/6/2019 9:19:42 AM	AWS-ConfigureAWSPackage	Success
12c3456c-7e90-4f12-1232-1234f5b67893 4/2/2019 4:13:07 AM	KT-Retrieve-Cloud-Type-Win	Failed
fe123b45-240c-4123-a2b3-234bdd567ecf 4/1/2019 2:27:31 PM	AWS-RunInspecChecks	Failed

1eb23aa4-567d-4123-12a3-4c1c2ab34561	AWS-RunPowerShellScript	Success
4/1/2019 1:05:55 PM		
1c2f3bb4-ee12-4bc1-1a23-12345eea123e	AWS-RunInspectionChecks	Failed
4/1/2019 11:13:09 AM		

- Per i dettagli sull'API, vedere [ListCommands](#) in Cmdlet Reference (V5). AWS Strumenti per PowerShell

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **ListComplianceItems** con una CLI

I seguenti esempi di codice mostrano come usare `ListComplianceItems`.

### CLI

#### AWS CLI

Per elencare gli elementi di conformità per un'istanza specifica

Questo esempio elenca tutti gli elementi di conformità per l'istanza specificata.

Comando:

```
aws ssm list-compliance-items --resource-ids "i-1234567890abcdef0" --resource-types "ManagedInstance"
```

Output:

```
{
 "ComplianceItems": [
 {
 "ComplianceType": "Association",
 "ResourceType": "ManagedInstance",
 "ResourceId": "i-1234567890abcdef0",
 "Id": "8dfe3659-4309-493a-8755-0123456789ab",
 "Title": "",
 "Status": "COMPLIANT",
 }
]
}
```

```

 "Severity": "UNSPECIFIED",
 "ExecutionSummary": {
 "ExecutionTime": 1550408470.0
 },
 "Details": {
 "DocumentName": "AWS-GatherSoftwareInventory",
 "DocumentVersion": "1"
 }
 },
 {
 "ComplianceType": "Association",
 "ResourceType": "ManagedInstance",
 "ResourceId": "i-1234567890abcdef0",
 "Id": "e4c2ed6d-516f-41aa-aa2a-0123456789ab",
 "Title": "",
 "Status": "COMPLIANT",
 "Severity": "UNSPECIFIED",
 "ExecutionSummary": {
 "ExecutionTime": 1550508475.0
 },
 "Details": {
 "DocumentName": "AWS-UpdateSSMAgent",
 "DocumentVersion": "1"
 }
 },
 ...
],
"NextToken": "--token string truncated--"
}

```

Come elencare gli elementi di conformità per un'istanza e un ID di associazione specifici

Questo esempio elenca tutti gli elementi di conformità per l'ID di istanza e associazione specificati.

Comando:

```

aws ssm list-compliance-items --resource-ids "i-1234567890abcdef0" --resource-
types "ManagedInstance" --
filters "Key=ComplianceType,Values=Association,Type=EQUAL" "Key=Id,Values=e4c2ed6d-516f-4
aa2a-0123456789ab,Type=EQUAL"

```

Come elencare gli elementi di conformità per un'istanza dopo una data e un'ora specifiche

Questo esempio elenca tutti gli elementi di conformità per un'istanza dopo la data e l'ora specificate.

Comando:

```
aws ssm list-compliance-items --resource-ids "i-1234567890abcdef0" --resource-
types "ManagedInstance" --
filters "Key=ExecutionTime,Values=2019-02-18T16:00:00Z,Type=GREATER_THAN"
```

- Per i dettagli sull'API, vedi [ListComplianceItems](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca l'elenco degli elementi di conformità per l'ID e il tipo di risorsa specificati, filtrando il tipo di conformità utilizzando "Associazione"

```
Get-SSMComplianceItemList -ResourceId i-1a2caf345f67d0dc2 -ResourceType
ManagedInstance -Filter @{Key="ComplianceType";Values="Association"}
```

Output:

```
ComplianceType : Association
Details : {[DocumentName, AWS-GatherSoftwareInventory],
 [DocumentVersion, 1]}
ExecutionSummary :
 Amazon.SimpleSystemsManagement.Model.ComplianceExecutionSummary
Id : 123a45a1-c234-1234-1245-67891236db4e
ResourceId : i-1a2caf345f67d0dc2
ResourceType : ManagedInstance
Severity : UNSPECIFIED
Status : COMPLIANT
Title :
```

- Per i dettagli sull'API, vedere [ListComplianceItems](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca l'elenco degli elementi di conformità per l'ID e il tipo di risorsa specificati, filtrando il tipo di conformità utilizzando "Associazione"

```
Get-SSMComplianceItemList -ResourceId i-1a2caf345f67d0dc2 -ResourceType
ManagedInstance -Filter @{Key="ComplianceType";Values="Association"}
```

Output:

```
ComplianceType : Association
Details : {[DocumentName, AWS-GatherSoftwareInventory],
 [DocumentVersion, 1]}
ExecutionSummary :
 Amazon.SimpleSystemsManagement.Model.ComplianceExecutionSummary
Id : 123a45a1-c234-1234-1245-67891236db4e
ResourceId : i-1a2caf345f67d0dc2
ResourceType : ManagedInstance
Severity : UNSPECIFIED
Status : COMPLIANT
Title :
```

- Per i dettagli sull'API, vedere [ListComplianceItems](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **ListComplianceSummaries** con una CLI

I seguenti esempi di codice mostrano come usare `ListComplianceSummaries`.

### CLI

#### AWS CLI

Per elencare i riepiloghi di conformità per tutti i tipi di conformità

Questo esempio elenca i riepiloghi di conformità per tutti i tipi di conformità presenti nell'account.

Comando:

```
aws ssm list-compliance-summaries
```

## Output:

```
{
 "ComplianceSummaryItems": [
 {
 "ComplianceType": "Association",
 "CompliantSummary": {
 "CompliantCount": 2,
 "SeveritySummary": {
 "CriticalCount": 0,
 "HighCount": 0,
 "MediumCount": 0,
 "LowCount": 0,
 "InformationalCount": 0,
 "UnspecifiedCount": 2
 }
 },
 "NonCompliantSummary": {
 "NonCompliantCount": 0,
 "SeveritySummary": {
 "CriticalCount": 0,
 "HighCount": 0,
 "MediumCount": 0,
 "LowCount": 0,
 "InformationalCount": 0,
 "UnspecifiedCount": 0
 }
 }
 },
 {
 "ComplianceType": "Patch",
 "CompliantSummary": {
 "CompliantCount": 1,
 "SeveritySummary": {
 "CriticalCount": 0,
 "HighCount": 0,
 "MediumCount": 0,
 "LowCount": 0,
 "InformationalCount": 0,
 "UnspecifiedCount": 1
 }
 },
 "NonCompliantSummary": {
 "NonCompliantCount": 1,
```

```

 "SeveritySummary": {
 "CriticalCount": 1,
 "HighCount": 0,
 "MediumCount": 0,
 "LowCount": 0,
 "InformationalCount": 0,
 "UnspecifiedCount": 0
 },
 ...
],
 "NextToken": "eyJ0ZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAyfQ=="
}

```

Come elencare i riepiloghi di conformità per un tipo di conformità specifico

Questo esempio elenca il riepilogo della conformità per il tipo di conformità Patch.

Comando:

```
aws ssm list-compliance-summaries --
filters "Key=ComplianceType,Values=Patch,Type=EQUAL"
```

- Per i dettagli sull'API, vedi [ListComplianceSummaries](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio restituisce un conteggio riepilogativo delle risorse conformi e non conformi per tutti i tipi di conformità.

```
Get-SSMComplianceSummaryList
```

Output:

```

ComplianceType CompliantSummary
NonCompliantSummary


```



```
FleetTotal Amazon.SimpleSystemsManagement.Model.CompliantSummary
 Amazon.SimpleSystemsManagement.Model.NonCompliantSummary
Association Amazon.SimpleSystemsManagement.Model.CompliantSummary
 Amazon.SimpleSystemsManagement.Model.NonCompliantSummary
Custom:InSpec Amazon.SimpleSystemsManagement.Model.CompliantSummary
 Amazon.SimpleSystemsManagement.Model.NonCompliantSummary
Patch Amazon.SimpleSystemsManagement.Model.CompliantSummary
 Amazon.SimpleSystemsManagement.Model.NonCompliantSummary
```

- Per i dettagli sull'API, vedere [ListComplianceSummaries](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio restituisce un conteggio riepilogativo delle risorse conformi e non conformi per tutti i tipi di conformità.

```
Get-SSMComplianceSummaryList
```

### Output:

```
ComplianceType CompliantSummary
NonCompliantSummary

FleetTotal Amazon.SimpleSystemsManagement.Model.CompliantSummary
 Amazon.SimpleSystemsManagement.Model.NonCompliantSummary
Association Amazon.SimpleSystemsManagement.Model.CompliantSummary
 Amazon.SimpleSystemsManagement.Model.NonCompliantSummary
Custom:InSpec Amazon.SimpleSystemsManagement.Model.CompliantSummary
 Amazon.SimpleSystemsManagement.Model.NonCompliantSummary
Patch Amazon.SimpleSystemsManagement.Model.CompliantSummary
 Amazon.SimpleSystemsManagement.Model.NonCompliantSummary
```

- Per i dettagli sull'API, vedere [ListComplianceSummaries](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **ListDocumentVersions** con una CLI

I seguenti esempi di codice mostrano come usare `ListDocumentVersions`.

### CLI

#### AWS CLI

Per elencare le versioni del documento

L'esempio seguente `list-document-versions` elenca tutte le versioni di un documento Systems Manager.

```
aws ssm list-document-versions \
 --name "Example"
```

Output:

```
{
 "DocumentVersions": [
 {
 "Name": "Example",
 "DocumentVersion": "1",
 "CreateDate": 1583257938.266,
 "IsDefaultVersion": true,
 "DocumentFormat": "YAML",
 "Status": "Active"
 }
]
}
```

Per ulteriori informazioni, consulta [Invio di comandi che utilizzano il parametro della versione del documento](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [ListDocumentVersions](#) in AWS CLI Command Reference.

### PowerShell

#### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca tutte le versioni di un documento.

```
Get-SSMDocumentVersionList -Name "AWS-UpdateSSMAgent"
```

Output:

```
CreatedDate : 6/1/2021 5:19:10 PM
DocumentFormat : JSON
DocumentVersion : 1
IsDefaultVersion : True
Name : AWS-UpdateSSMAgent
Status : Active
```

- Per i dettagli sull'API, vedere [ListDocumentVersions](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca tutte le versioni di un documento.

```
Get-SSMDocumentVersionList -Name "AWS-UpdateSSMAgent"
```

Output:

```
CreatedDate : 6/1/2021 5:19:10 PM
DocumentFormat : JSON
DocumentVersion : 1
IsDefaultVersion : True
Name : AWS-UpdateSSMAgent
Status : Active
```

- Per i dettagli sull'API, vedere [ListDocumentVersions](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **ListDocuments** con una CLI

I seguenti esempi di codice mostrano come usare `ListDocuments`.

## CLI

### AWS CLI

Esempio 1: per elencare i documenti

L'esempio seguente `list-documents` elenca i documenti di proprietà dell'account richiedente contrassegnati con il tag personalizzato.

```
aws ssm list-documents \
 --filters Key=Owner,Values=Self Key=tag:DocUse,Values=Testing
```

Output:

```
{
 "DocumentIdentifiers": [
 {
 "Name": "Example",
 "Owner": "29884EXAMPLE",
 "PlatformTypes": [
 "Windows",
 "Linux"
],
 "DocumentVersion": "1",
 "DocumentType": "Automation",
 "SchemaVersion": "0.3",
 "DocumentFormat": "YAML",
 "Tags": [
 {
 "Key": "DocUse",
 "Value": "Testing"
 }
]
 }
]
}
```

Per ulteriori informazioni, consulta [Documenti AWS Systems Manager](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 2: come elencare i documenti condivisi

L'list-documentsesempio seguente elenca i documenti condivisi, inclusi i documenti condivisi privati non di proprietà di AWS.

```
aws ssm list-documents \
 --filters Key=Name,Values=sharedDocNamePrefix Key=Owner,Values=Private
```

Output:

```
{
 "DocumentIdentifiers": [
 {
 "Name": "Example",
 "Owner": "12345EXAMPLE",
 "PlatformTypes": [
 "Windows",
 "Linux"
],
 "DocumentVersion": "1",
 "DocumentType": "Command",
 "SchemaVersion": "0.3",
 "DocumentFormat": "YAML",
 "Tags": []
 }
]
}
```

Per ulteriori informazioni, consulta [Documenti di AWS Systems Manager](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [ListDocuments](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: elenca tutti i documenti di configurazione dell'account.

```
Get-SSMDocumentList
```

Output:

```
DocumentType : Command
```

```

DocumentVersion : 1
Name : AWS-ApplyPatchBaseline
Owner : Amazon
PlatformTypes : {Windows}
SchemaVersion : 1.2

DocumentType : Command
DocumentVersion : 1
Name : AWS-ConfigureAWSPackage
Owner : Amazon
PlatformTypes : {Windows, Linux}
SchemaVersion : 2.0

DocumentType : Command
DocumentVersion : 1
Name : AWS-ConfigureCloudWatch
Owner : Amazon
PlatformTypes : {Windows}
SchemaVersion : 1.2
...

```

Esempio 2: questo esempio recupera tutti i documenti di automazione il cui nome corrisponde a “Piattaforma”

```

Get-SSMDocumentList -DocumentFilterList @{Key="DocumentType";Value="Automation"}
| Where-Object Name -Match "Platform"

```

Output:

```

DocumentFormat : JSON
DocumentType : Automation
DocumentVersion : 7
Name : KT-Get-Platform
Owner : 987654123456
PlatformTypes : {Windows, Linux}
SchemaVersion : 0.3
Tags : {}
TargetType :
VersionName :

```

- Per i dettagli sull'API, vedere [ListDocuments](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: elenca tutti i documenti di configurazione dell'account.

```
Get-SSMDocumentList
```

Output:

```
DocumentType : Command
DocumentVersion : 1
Name : AWS-ApplyPatchBaseline
Owner : Amazon
PlatformTypes : {Windows}
SchemaVersion : 1.2

DocumentType : Command
DocumentVersion : 1
Name : AWS-ConfigureAWSPackage
Owner : Amazon
PlatformTypes : {Windows, Linux}
SchemaVersion : 2.0

DocumentType : Command
DocumentVersion : 1
Name : AWS-ConfigureCloudWatch
Owner : Amazon
PlatformTypes : {Windows}
SchemaVersion : 1.2
...
```

Esempio 2: questo esempio recupera tutti i documenti di automazione il cui nome corrisponde a "Piattaforma"

```
Get-SSMDocumentList -DocumentFilterList @{Key="DocumentType";Value="Automation"}
| Where-Object Name -Match "Platform"
```

Output:

```
DocumentFormat : JSON
DocumentType : Automation
DocumentVersion : 7
```

```
Name : KT-Get-Platform
Owner : 987654123456
PlatformTypes : {Windows, Linux}
SchemaVersion : 0.3
Tags : {}
TargetType :
VersionName :
```

- Per i dettagli sull'API, vedere [ListDocuments](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **ListInventoryEntries** con una CLI

I seguenti esempi di codice mostrano come usare `ListInventoryEntries`.

### CLI

#### AWS CLI

Esempio 1: per visualizzare le voci relative al tipo di inventario specifiche per un'istanza

L'`list-inventory-entries` seguente elenca le voci di inventario per il tipo di AWS inventario:Application su un'istanza specifica.

```
aws ssm list-inventory-entries \
 --instance-id "i-1234567890abcdef0" \
 --type-name "AWS:Application"
```

Output:

```
{
 "TypeName": "AWS:Application",
 "InstanceId": "i-1234567890abcdef0",
 "SchemaVersion": "1.1",
 "CaptureTime": "2019-02-15T12:17:55Z",
 "Entries": [
```



```
{
 "Architecture": "i386",
 "Name": "Amazon SSM Agent",
 "PackageId": "{88a60be2-89a1-4df8-812a-80863c2a2b68}",
 "Publisher": "Amazon Web Services",
 "Version": "2.3.274.0"
},
{
 "Architecture": "x86_64",
 "InstalledTime": "2018-05-03T13:42:34Z",
 "Name": "AmazonCloudWatchAgent",
 "Publisher": "",
 "Version": "1.200442.0"
}
]
```

Esempio 2: come visualizzare le voci di inventario personalizzate assegnate a un'istanza

L'esempio seguente `list-inventory-entries` elenca una voce di inventario personalizzata assegnata a un'istanza.

```
aws ssm list-inventory-entries \
 --instance-id "i-1234567890abcdef0" \
 --type-name "Custom:RackInfo"
```

Output:

```
{
 "TypeName": "Custom:RackInfo",
 "InstanceId": "i-1234567890abcdef0",
 "SchemaVersion": "1.0",
 "CaptureTime": "2021-05-22T10:01:01Z",
 "Entries": [
 {
 "RackLocation": "Bay B/Row C/Rack D/Shelf E"
 }
]
}
```

- Per i dettagli sull'API, vedi [ListInventoryEntries](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca tutte le voci di inventario personalizzate per un'istanza.

```
Get-SSMInventoryEntriesList -InstanceId "i-0cb2b964d3e14fd9f" -TypeName
"Custom:RackInfo"
```

Output:

```
CaptureTime : 2016-08-22T10:01:01Z
Entries :
 {Amazon.Runtime.Internal.Util.AlwaysSendDictionary`2[System.String,System.String]}
InstanceId : i-0cb2b964d3e14fd9f
NextToken :
SchemaVersion : 1.0
TypeName : Custom:RackInfo
```

Esempio 2: questo esempio elenca i dettagli.

```
(Get-SSMInventoryEntriesList -InstanceId "i-0cb2b964d3e14fd9f" -TypeName
"Custom:RackInfo").Entries
```

Output:

Key	Value
---	-----
RackLocation	Bay B/Row C/Rack D/Shelf E

- Per i dettagli sull'API, vedere [ListInventoryEntries](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca tutte le voci di inventario personalizzate per un'istanza.

```
Get-SSMInventoryEntriesList -InstanceId "i-0cb2b964d3e14fd9f" -TypeName
"Custom:RackInfo"
```

Output:

```

CaptureTime : 2016-08-22T10:01:01Z
Entries :
 {Amazon.Runtime.Internal.Util.AlwaysSendDictionary`2[System.String,System.String]}
InstanceId : i-0cb2b964d3e14fd9f
NextToken :
SchemaVersion : 1.0
TypeName : Custom:RackInfo

```

Esempio 2: questo esempio elenca i dettagli.

```

(Get-SSMInventoryEntriesList -InstanceId "i-0cb2b964d3e14fd9f" -TypeName
"Custom:RackInfo").Entries

```

Output:

```

Key Value
--- -
RackLocation Bay B/Row C/Rack D/Shelf E

```

- Per i dettagli sull'API, vedere [ListInventoryEntries](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **ListResourceComplianceSummaries** con una CLI

I seguenti esempi di codice mostrano come usare `ListResourceComplianceSummaries`.

### CLI

#### AWS CLI

Per elencare i conteggi riepilogativi della conformità a livello di risorsa

Questo esempio elenca i conteggi riepilogativi della conformità a livello di risorsa.

Comando:

```
aws ssm list-resource-compliance-summaries
```

## Output:

```
{
 "ResourceComplianceSummaryItems": [
 {
 "ComplianceType": "Association",
 "ResourceType": "ManagedInstance",
 "ResourceId": "i-1234567890abcdef0",
 "Status": "COMPLIANT",
 "OverallSeverity": "UNSPECIFIED",
 "ExecutionSummary": {
 "ExecutionTime": 1550509273.0
 },
 "CompliantSummary": {
 "CompliantCount": 2,
 "SeveritySummary": {
 "CriticalCount": 0,
 "HighCount": 0,
 "MediumCount": 0,
 "LowCount": 0,
 "InformationalCount": 0,
 "UnspecifiedCount": 2
 }
 },
 "NonCompliantSummary": {
 "NonCompliantCount": 0,
 "SeveritySummary": {
 "CriticalCount": 0,
 "HighCount": 0,
 "MediumCount": 0,
 "LowCount": 0,
 "InformationalCount": 0,
 "UnspecifiedCount": 0
 }
 }
 },
 {
 "ComplianceType": "Patch",
 "ResourceType": "ManagedInstance",
 "ResourceId": "i-9876543210abcdef0",
 "Status": "COMPLIANT",
 "OverallSeverity": "UNSPECIFIED",
 "ExecutionSummary": {
 "ExecutionTime": 1550248550.0,
```

```

 "ExecutionId": "7abb6378-a4a5-4f10-8312-0123456789ab",
 "ExecutionType": "Command"
 },
 "CompliantSummary": {
 "CompliantCount": 397,
 "SeveritySummary": {
 "CriticalCount": 0,
 "HighCount": 0,
 "MediumCount": 0,
 "LowCount": 0,
 "InformationalCount": 0,
 "UnspecifiedCount": 397
 }
 },
 "NonCompliantSummary": {
 "NonCompliantCount": 0,
 "SeveritySummary": {
 "CriticalCount": 0,
 "HighCount": 0,
 "MediumCount": 0,
 "LowCount": 0,
 "InformationalCount": 0,
 "UnspecifiedCount": 0
 }
 }
},
"NextToken": "--token string truncated--"
}

```

Come elencare i riepiloghi di conformità a livello di risorsa per un tipo di conformità specifico

Questo esempio elenca i riepiloghi di conformità a livello di risorsa per il tipo di conformità Patch.

Comando:

```

aws ssm list-resource-compliance-summaries --
filters "Key=ComplianceType,Values=Patch,Type=EQUAL"

```

- Per i dettagli sull'API, vedi [ListResourceComplianceSummaries](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio ottiene un conteggio riepilogativo a livello di risorsa. Il riepilogo include informazioni sullo stato conforme e non conforme e sui conteggi dettagliati di gravità degli elementi di conformità per i prodotti che corrispondono a "Windows10". Poiché il valore MaxResult predefinito è 100 se il parametro non è specificato e questo valore non è valido, viene aggiunto il MaxResult parametro e il valore è impostato su 50.

```
$FilterValues = @{"Key"="Product"
 "Type"="EQUAL "
 "Values"="Windows10"
 }

Get-SSMResourceComplianceSummaryList -Filter $FilterValues -MaxResult 50
```

- Per i dettagli sull'API, vedere [ListResourceComplianceSummaries](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio ottiene un conteggio riepilogativo a livello di risorsa. Il riepilogo include informazioni sullo stato conforme e non conforme e sui conteggi dettagliati di gravità degli elementi di conformità per i prodotti che corrispondono a "Windows10". Poiché il valore MaxResult predefinito è 100 se il parametro non è specificato e questo valore non è valido, viene aggiunto il MaxResult parametro e il valore è impostato su 50.

```
$FilterValues = @{"Key"="Product"
 "Type"="EQUAL "
 "Values"="Windows10"
 }

Get-SSMResourceComplianceSummaryList -Filter $FilterValues -MaxResult 50
```

- Per i dettagli sull'API, vedere [ListResourceComplianceSummaries](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **ListTagsForResource** con una CLI

I seguenti esempi di codice mostrano come usare `ListTagsForResource`.

### CLI

#### AWS CLI

Per elencare i tag applicati a una baseline delle patch

L'esempio seguente `list-tags-for-resource` elenca i tag per una baseline delle patch.

```
aws ssm list-tags-for-resource \
 --resource-type "PatchBaseline" \
 --resource-id "pb-0123456789abcdef0"
```

Output:

```
{
 "TagList": [
 {
 "Key": "Environment",
 "Value": "Production"
 },
 {
 "Key": "Region",
 "Value": "EMEA"
 }
]
}
```

Per ulteriori informazioni, vedere [Tagging AWS Resources](#) nella Guida AWS generale.

- Per i dettagli sull'API, vedi [ListTagsForResource](#) in AWS CLI Command Reference.

### PowerShell

#### Strumenti per PowerShell V4

Esempio 1: questo esempio elenca i tag per una finestra di manutenzione.

```
Get-SSMResourceTag -ResourceId "mw-03eb9db42890fb82d" -ResourceType
"MaintenanceWindow"
```

Output:

```
Key Value
--- -
Stack Production
```

- Per i dettagli sull'API, vedere [ListTagsForResource](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

Strumenti per V5 PowerShell

Esempio 1: questo esempio elenca i tag per una finestra di manutenzione.

```
Get-SSMResourceTag -ResourceId "mw-03eb9db42890fb82d" -ResourceType
"MaintenanceWindow"
```

Output:

```
Key Value
--- -
Stack Production
```

- Per i dettagli sull'API, vedere [ListTagsForResource](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **ModifyDocumentPermission** con una CLI

I seguenti esempi di codice mostrano come usare `ModifyDocumentPermission`.

CLI

AWS CLI

Per modificare le autorizzazioni del documento



L'esempio seguente `modify-document-permission` condivide pubblicamente un documento Systems Manager.

```
aws ssm modify-document-permission \
 --name "Example" \
 --permission-type "Share" \
 --account-ids-to-add "All"
```

Questo comando non produce alcun output.

Per ulteriori informazioni, consulta [Condividi un documento Systems Manager](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [ModifyDocumentPermission](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio aggiunge le autorizzazioni di "condivisione" a tutti gli account di un documento. Se il comando va a buon fine, non viene generato output.

```
Edit-SSMDocumentPermission -Name "RunShellScript" -PermissionType "Share" -
AccountIdsToAdd all
```

Esempio 2: questo esempio aggiunge le autorizzazioni di "condivisione" a un account specifico per un documento. Se il comando va a buon fine, non viene generato output.

```
Edit-SSMDocumentPermission -Name "RunShellScriptNew" -PermissionType "Share" -
AccountIdsToAdd "123456789012"
```

- Per i dettagli sull'API, vedere [ModifyDocumentPermission](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio aggiunge le autorizzazioni di "condivisione" a tutti gli account di un documento. Se il comando va a buon fine, non viene generato output.

```
Edit-SSMDocumentPermission -Name "RunShellScript" -PermissionType "Share" -
AccountIdsToAdd all
```

Esempio 2: questo esempio aggiunge le autorizzazioni di “condivisione” a un account specifico per un documento. Se il comando va a buon fine, non viene generato output.

```
Edit-SSMDocumentPermission -Name "RunShellScriptNew" -PermissionType "Share" -
AccountIdsToAdd "123456789012"
```

- Per i dettagli sull'API, vedere [ModifyDocumentPermission](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **PutComplianceItems** con una CLI

I seguenti esempi di codice mostrano come usare `PutComplianceItems`.

### CLI

#### AWS CLI

Per registrare un tipo di conformità e i dettagli di conformità su un'istanza designata

Questo esempio registra il tipo di conformità `Custom:AVCheck` nell'istanza gestita specificata. Se il comando va a buon fine, non viene generato output.

Comando:

```
aws ssm put-compliance-items --resource-id "i-1234567890abcdef0" --
resource-type "ManagedInstance" --compliance-type "Custom:AVCheck"
--execution-summary "ExecutionTime=2019-02-18T16:00:00Z" --
items "Id=Version2.0,Title=ScanHost,Severity=CRITICAL,Status=COMPLIANT"
```

- Per i dettagli sull'API, vedi [PutComplianceItems](#) in AWS CLI Command Reference.

### PowerShell

#### Strumenti per PowerShell V4

Esempio 1: questo esempio scrive un elemento di conformità personalizzato per l'istanza gestita specificata

```
$item = [Amazon.SimpleSystemsManagement.Model.ComplianceItemEntry]::new()
$item.Id = "07Jun2019-3"
$item.Severity="LOW"
$item.Status="COMPLIANT"
$item.Title="Fin-test-1 - custom"
Write-SSMComplianceItem -ResourceId mi-012dcb3ecea45b678 -ComplianceType
 Custom:VSSCompliant2 -ResourceType ManagedInstance -Item $item -
ExecutionSummary_ExecutionTime "07-Jun-2019"
```

- Per i dettagli sull'API, vedere [PutComplianceItems](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio scrive un elemento di conformità personalizzato per l'istanza gestita specificata

```
$item = [Amazon.SimpleSystemsManagement.Model.ComplianceItemEntry]::new()
$item.Id = "07Jun2019-3"
$item.Severity="LOW"
$item.Status="COMPLIANT"
$item.Title="Fin-test-1 - custom"
Write-SSMComplianceItem -ResourceId mi-012dcb3ecea45b678 -ComplianceType
 Custom:VSSCompliant2 -ResourceType ManagedInstance -Item $item -
ExecutionSummary_ExecutionTime "07-Jun-2019"
```

- Per i dettagli sull'API, vedere [PutComplianceItems](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **PutInventory** con una CLI

I seguenti esempi di codice mostrano come usarePutInventory.

### CLI

#### AWS CLI

Per assegnare metadati di un cliente a un'istanza

Questo esempio assegna le informazioni sulla posizione del rack a un'istanza. Se il comando va a buon fine, non viene generato output.

Comando (Linux):

```
aws ssm put-inventory --instance-id "i-016648b75dd622dab" --items
' [{"TypeName": "Custom:RackInfo", "SchemaVersion": "1.0", "CaptureTime":
"2019-01-22T10:01:01Z", "Content": [{"RackLocation": "Bay B/Row C/Rack D/Shelf
E"}]}]'
```

Comando (Windows):

```
aws ssm put-inventory --instance-id "i-016648b75dd622dab" --
items "TypeName=Custom:RackInfo,SchemaVersion=1.0,CaptureTime=2019-01-22T10:01:01Z,Content=[{"RackLocation": "Bay B/Row C/Rack D/Shelf F"}]"
```

- Per i dettagli sull'API, vedi [PutInventory](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio assegna le informazioni sulla posizione del rack a un'istanza. Se il comando va a buon fine, non viene generato output.

```
$data = New-Object
[System.Collections.Generic.Dictionary[System.String,System.String]]
$data.Add("RackLocation", "Bay B/Row C/Rack D/Shelf F")

$items = New-Object
[System.Collections.Generic.List[System.Collections.Generic.Dictionary[System.String,
System.String]]]
$items.Add($data)

$customInventoryItem = New-Object
Amazon.SimpleSystemsManagement.Model.InventoryItem
$customInventoryItem.CaptureTime = "2016-08-22T10:01:01Z"
$customInventoryItem.Content = $items
$customInventoryItem.TypeName = "Custom:TestRackInfo2"
$customInventoryItem.SchemaVersion = "1.0"
```

```
$inventoryItems = @($customInventoryItem)
```

```
Write-SSMInventory -InstanceId "i-0cb2b964d3e14fd9f" -Item $inventoryItems
```

- Per i dettagli sull'API, vedere [PutInventory](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio assegna le informazioni sulla posizione del rack a un'istanza. Se il comando va a buon fine, non viene generato output.

```
$data = New-Object
 "System.Collections.Generic.Dictionary[System.String,System.String]"
$data.Add("RackLocation", "Bay B/Row C/Rack D/Shelf F")

$items = New-Object
 "System.Collections.Generic.List[System.Collections.Generic.Dictionary[System.String,
 System.String]]"
$items.Add($data)

$customInventoryItem = New-Object
 Amazon.SimpleSystemsManagement.Model.InventoryItem
$customInventoryItem.CaptureTime = "2016-08-22T10:01:01Z"
$customInventoryItem.Content = $items
$customInventoryItem.TypeName = "Custom:TestRackInfo2"
$customInventoryItem.SchemaVersion = "1.0"

$inventoryItems = @($customInventoryItem)

Write-SSMInventory -InstanceId "i-0cb2b964d3e14fd9f" -Item $inventoryItems
```

- Per i dettagli sull'API, vedere [PutInventory](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Usare **PutParameter** con un AWS SDK o CLI

I seguenti esempi di codice mostrano come usare `PutParameter`.

## CLI

### AWS CLI

Esempio 1: per modificare il valore di un parametro

L'esempio seguente `put-parameter` modifica il valore del parametro specificato.

```
aws ssm put-parameter \
 --name "MyStringParameter" \
 --type "String" \
 --value "Vici" \
 --overwrite
```

Output:

```
{
 "Version": 2,
 "Tier": "Standard"
}
```

Per ulteriori informazioni, vedere [Creazione di un parametro di Systems Manager \(AWS CLI\)](#), [Gestione dei livelli](#) dei parametri e [Utilizzo delle politiche dei parametri](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 2: come creare un parametro avanzato

L'esempio seguente `put-parameter` crea un parametro avanzato.

```
aws ssm put-parameter \
 --name "MyAdvancedParameter" \
 --description "This is an advanced parameter" \
 --value "Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do
 eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim
 veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo
 consequat [truncated]" \
 --type "String" \
 --tier Advanced
```

Output:

```
{
 "Version": 1,
 "Tier": "Advanced"
}
```

Per ulteriori informazioni, vedere [Creazione di un parametro di Systems Manager \(AWS CLI\)](#), [Gestione dei livelli](#) dei parametri e [Utilizzo delle politiche dei parametri](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 3: come convertire un parametro standard in un parametro avanzato

L'esempio `put-parameter` seguente converte un parametro standard esistente in un parametro avanzato.

```
aws ssm put-parameter \
 --name "MyConvertedParameter" \
 --value "abc123" \
 --type "String" \
 --tier Advanced \
 --overwrite
```

Output:

```
{
 "Version": 2,
 "Tier": "Advanced"
}
```

Per ulteriori informazioni, vedere [Creazione di un parametro di Systems Manager \(AWS CLI\)](#), [Gestione dei livelli](#) dei parametri e [Utilizzo delle politiche dei parametri](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 4: come creare un parametro con una policy collegata

L'esempio seguente `put-parameter` crea un parametro avanzato con una policy dei parametri allegata.

```
aws ssm put-parameter \
 --name "/Finance/Payroll/q2accesskey" \
```

```
--value "P@sSwW)rd" \
--type "SecureString" \
--tier Advanced \
--policies "[{"Type\":"Expiration\","Version\":"1.0\","Attributes\":"Timestamp\":"2020-06-30T00:00:00.000Z\"}, {"Type\":"ExpirationNotification\","Version\":"1.0\","Attributes\":"Before\":"5\","Unit\":"Days\"}, {"Type\":"NoChangeNotification\","Version\":"1.0\","Attributes\":"After\":"60\","Unit\":"Days\"}]"]"
```

Output:

```
{
 "Version": 1,
 "Tier": "Advanced"
}
```

Per ulteriori informazioni, vedere [Creazione di un parametro di Systems Manager \(AWS CLI\)](#), [Gestione dei livelli](#) dei parametri e [Utilizzo delle politiche dei parametri](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 5: come aggiungere una policy a un parametro esistente

L'esempio seguente put-parameter collega una policy a un parametro avanzato esistente.

```
aws ssm put-parameter \
 --name "/Finance/Payroll/q2accesskey" \
 --value "N3wP@sSwW)rd" \
 --type "SecureString" \
 --tier Advanced \
 --policies "[{"Type\":"Expiration\","Version\":"1.0\","Attributes\":"Timestamp\":"2020-06-30T00:00:00.000Z\"}, {"Type\":"ExpirationNotification\","Version\":"1.0\","Attributes\":"Before\":"5\","Unit\":"Days\"}, {"Type\":"NoChangeNotification\","Version\":"1.0\","Attributes\":"After\":"60\","Unit\":"Days\"}]"]"
 --overwrite
```

Output:

```
{
 "Version": 2,
 "Tier": "Advanced"
}
```



```
}
```

Per ulteriori informazioni, vedere [Creazione di un parametro di Systems Manager \(AWS CLI\)](#), [Gestione dei livelli](#) dei parametri e [Utilizzo delle politiche dei parametri](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [PutParameter](#) in AWS CLI Command Reference.

## Java

### SDK per Java 2.x

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ssm.SsmClient;
import software.amazon.awssdk.services.ssm.model.ParameterType;
import software.amazon.awssdk.services.ssm.model.PutParameterRequest;
import software.amazon.awssdk.services.ssm.model.SsmException;

public class PutParameter {

 public static void main(String[] args) {
 final String usage = ""

 Usage:
 <paraName>

 Where:
 paraName - The name of the parameter.
 paraValue - The value of the parameter.
 """;

 if (args.length != 2) {
 System.out.println(usage);
 System.exit(1);
 }
 }
}
```

```
String paraName = args[0];
String paraValue = args[1];
Region region = Region.US_EAST_1;
SsmClient ssmClient = SsmClient.builder()
 .region(region)
 .build();

putParaValue(ssmClient, paraName, paraValue);
ssmClient.close();
}

public static void putParaValue(SsmClient ssmClient, String paraName, String
value) {
 try {
 PutParameterRequest parameterRequest = PutParameterRequest.builder()
 .name(paraName)
 .type(ParameterType.STRING)
 .value(value)
 .build();

 ssmClient.putParameter(parameterRequest);
 System.out.println("The parameter was successfully added.");

 } catch (SsmException e) {
 System.err.println(e.getMessage());
 System.exit(1);
 }
}
}
```

- Per i dettagli sulle API, consulta la [PutParameter](#) sezione AWS SDK for Java 2.x API Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio crea un parametro. Se il comando va a buon fine, non viene generato output.

```
Write-SSMParameter -Name "Welcome" -Type "String" -Value "helloWorld"
```

Esempio 2: questo esempio modifica un parametro. Se il comando va a buon fine, non viene generato output.

```
Write-SSMParameter -Name "Welcome" -Type "String" -Value "Good day, Sunshine!" -
Overwrite $true
```

- Per i dettagli sull'API, vedere [PutParameter](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio crea un parametro. Se il comando va a buon fine, non viene generato output.

```
Write-SSMParameter -Name "Welcome" -Type "String" -Value "helloWorld"
```

Esempio 2: questo esempio modifica un parametro. Se il comando va a buon fine, non viene generato output.

```
Write-SSMParameter -Name "Welcome" -Type "String" -Value "Good day, Sunshine!" -
Overwrite $true
```

- Per i dettagli sull'API, vedere [PutParameter](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

## Rust

### SDK per Rust

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
async fn make_parameter(
 client: &Client,
 name: &str,
 value: &str,
```

```

 description: &str,
) -> Result<(), Error> {
 let resp = client
 .put_parameter()
 .overwrite(true)
 .r#type(ParameterType::String)
 .name(name)
 .value(value)
 .description(description)
 .send()
 .await?;

 println!("Success! Parameter now has version: {}", resp.version());

 Ok(())
 }

```

- Per i dettagli sulle API, consulta [PutParameter](#) la sezione AWS SDK for Rust API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **RegisterDefaultPatchBaseline** con una CLI

I seguenti esempi di codice mostrano come usare `RegisterDefaultPatchBaseline`.

### CLI

#### AWS CLI

Per impostare la baseline delle patch predefinita

L'esempio seguente `register-default-patch-baseline` registra la baseline delle patch personalizzata specificata come baseline di patch predefinita per il tipo di sistema operativo che supporta.

```

aws ssm register-default-patch-baseline \
 --baseline-id "pb-abc123cf9bEXAMPLE"

```

Output:

```
{
 "BaselineId": "pb-abc123cf9bEXAMPLE"
}
```

L' `register-default-patch-baseline` seguente registra la baseline della patch predefinita fornita da AWS for CentOS come baseline della patch predefinita.

```
aws ssm register-default-patch-baseline \
 --baseline-id "arn:aws:ssm:us-east-2:733109147000:patchbaseline/
 pb-0574b43a65ea646ed"
```

Output:

```
{
 "BaselineId": "pb-abc123cf9bEXAMPLE"
}
```

Per ulteriori informazioni, consulta [Informazioni sulle baseline delle patch predefinite e personalizzate](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [RegisterDefaultPatchBaseline](#) in Command Reference. AWS CLI

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio registra una baseline delle patch come baseline delle patch predefinita.

```
Register-SSMDefaultPatchBaseline -BaselineId "pb-03da896ca3b68b639"
```

Output:

```
pb-03da896ca3b68b639
```

- Per i dettagli sull'API, vedere [RegisterDefaultPatchBaseline](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio registra una baseline delle patch come baseline delle patch predefinita.

```
Register-SSMDefaultPatchBaseline -BaselineId "pb-03da896ca3b68b639"
```

Output:

```
pb-03da896ca3b68b639
```

- Per i dettagli sull'API, vedere [RegisterDefaultPatchBaseline](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **RegisterPatchBaselineForPatchGroup** con una CLI

I seguenti esempi di codice mostrano come usare `RegisterPatchBaselineForPatchGroup`.

### CLI

#### AWS CLI

Per registrare una baseline delle patch per un gruppo di patch

L'esempio seguente `register-patch-baseline-for-patch-group` registra una baseline delle patch per un gruppo di patch.

```
aws ssm register-patch-baseline-for-patch-group \
 --baseline-id "pb-045f10b4f382baeda" \
 --patch-group "Production"
```

Output:

```
{
 "BaselineId": "pb-045f10b4f382baeda",
```

```
"PatchGroup": "Production"
}
```

Per ulteriori informazioni, vedere [Create a Patch Group](https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-group-tagging.html) < <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-group-tagging.html> >\_\_ e [Add a Patch Group to a Patch Baseline](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [RegisterPatchBaselineForPatchGroup](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio registra una baseline delle patch per un gruppo di patch.

```
Register-SSMPatchBaselineForPatchGroup -BaselineId "pb-03da896ca3b68b639" -
PatchGroup "Production"
```

Output:

BaselineId	PatchGroup
-----	-----
pb-03da896ca3b68b639	Production

- Per i dettagli sull'API, vedere [RegisterPatchBaselineForPatchGroup](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio registra una baseline delle patch per un gruppo di patch.

```
Register-SSMPatchBaselineForPatchGroup -BaselineId "pb-03da896ca3b68b639" -
PatchGroup "Production"
```

Output:

BaselineId	PatchGroup
-----	-----
pb-03da896ca3b68b639	Production

- Per i dettagli sull'API, vedere [RegisterPatchBaselineForPatchGroup](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **RegisterTargetWithMaintenanceWindow** con una CLI

I seguenti esempi di codice mostrano come usare **RegisterTargetWithMaintenanceWindow**.

### CLI

#### AWS CLI

Esempio 1: per registrare una singola destinazione con una finestra di manutenzione

L'esempio seguente `register-target-with-maintenance-window` registra un'istanza con una finestra di manutenzione.

```
aws ssm register-target-with-maintenance-window \
 --window-id "mw-ab12cd34ef56gh78" \
 --target "Key=InstanceIds,Values=i-0000293ffd8c57862" \
 --owner-information "Single instance" \
 --resource-type "INSTANCE"
```

Output:

```
{
 "WindowTargetId": "1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

Esempio 2: come registrare più destinazioni con una finestra di manutenzione utilizzando gli ID di istanza

L'esempio seguente `register-target-with-maintenance-window` registra due istanze con una finestra di manutenzione specificandone gli ID di istanza.

```
aws ssm register-target-with-maintenance-window \
 --window-id "mw-ab12cd34ef56gh78" \
```



```
--target "Key=InstanceIds,Values=i-0000293ffd8c57862,i-0cb2b964d3e14fd9f" \
--owner-information "Two instances in a list" \
--resource-type "INSTANCE"
```

Output:

```
{
 "WindowTargetId": "1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

Esempio 3: come registrare le destinazioni in una finestra di manutenzione utilizzando i tag delle risorse

L'esempio seguente `register-target-with-maintenance-window` registra le istanze con una finestra di manutenzione specificando i tag di risorsa che sono stati applicati alle istanze.

```
aws ssm register-target-with-maintenance-window \
 --window-id "mw-06cf17cbefcb4bf4f" \
 --targets "Key=tag:Environment,Values=Prod" "Key=Role,Values=Web" \
 --owner-information "Production Web Servers" \
 --resource-type "INSTANCE"
```

Output:

```
{
 "WindowTargetId": "1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

Esempio 4: come registrare le destinazioni utilizzando un gruppo di chiavi dei tag

L'esempio seguente `register-target-with-maintenance-window` registra tutte le istanze che hanno una o più chiavi dei tag assegnate, indipendentemente dai valori delle chiavi.

```
aws ssm register-target-with-maintenance-window \
 --window-id "mw-0c50858d01EXAMPLE" \
 --resource-type "INSTANCE" \
 --target "Key=tag-key,Values=Name,Instance-Type,CostCenter"
```

Output:

```
{
 "WindowTargetId": "1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

Esempio 5: come registrare le destinazioni utilizzando un nome del gruppo di risorse

L'esempio seguente `register-target-with-maintenance-window` registra un gruppo di risorse specificato, indipendentemente dal tipo di risorse che contiene.

```
aws ssm register-target-with-maintenance-window \
 --window-id "mw-0c50858d01EXAMPLE" \
 --resource-type "RESOURCE_GROUP" \
 --target "Key=resource-groups:Name,Values=MyResourceGroup"
```

Output:

```
{
 "WindowTargetId": "1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

Per ulteriori informazioni, vedere [Register a Target Instance with the Maintenance Window \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [RegisterTargetWithMaintenanceWindow](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio registra un'istanza con una finestra di manutenzione.

```
$option1 = @{"Key"="InstanceIds";Values=@"i-0000293ffd8c57862"}
Register-SSMTargetWithMaintenanceWindow -WindowId "mw-06cf17cbefcb4bf4f" -Target
$option1 -OwnerInformation "Single instance" -ResourceType "INSTANCE"
```

Output:

```
d8e47760-23ed-46a5-9f28-927337725398
```

Esempio 2: questo esempio registra più istanze con una finestra di manutenzione.

```
$option1 =
 @{Key="InstanceIds";Values=@("i-0000293ffd8c57862","i-0cb2b964d3e14fd9f")}
Register-SSMTargetWithMaintenanceWindow -WindowId "mw-06cf17cbefcb4bf4f" -Target
$option1 -OwnerInformation "Single instance" -ResourceType "INSTANCE"
```

Output:

```
6ab5c208-9fc4-4697-84b7-b02a6cc25f7d
```

Esempio 3: questo esempio registra un'istanza con una finestra di manutenzione utilizzando i tag EC2.

```
$option1 = @{Key="tag:Environment";Values=@("Production")}
Register-SSMTargetWithMaintenanceWindow -WindowId "mw-06cf17cbefcb4bf4f" -Target
$option1 -OwnerInformation "Production Web Servers" -ResourceType "INSTANCE"
```

Output:

```
2994977e-aefb-4a71-beac-df620352f184
```

- Per i dettagli sull'API, vedere [RegisterTargetWithMaintenanceWindow](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio registra un'istanza con una finestra di manutenzione.

```
$option1 = @{Key="InstanceIds";Values=@("i-0000293ffd8c57862")}
Register-SSMTargetWithMaintenanceWindow -WindowId "mw-06cf17cbefcb4bf4f" -Target
$option1 -OwnerInformation "Single instance" -ResourceType "INSTANCE"
```

Output:

```
d8e47760-23ed-46a5-9f28-927337725398
```

Esempio 2: questo esempio registra più istanze con una finestra di manutenzione.

```
$option1 =
 @{Key="InstanceIds";Values=@("i-0000293ffd8c57862","i-0cb2b964d3e14fd9f")}
Register-SSMTargetWithMaintenanceWindow -WindowId "mw-06cf17cbefcb4bf4f" -Target
 $option1 -OwnerInformation "Single instance" -ResourceType "INSTANCE"
```

Output:

```
6ab5c208-9fc4-4697-84b7-b02a6cc25f7d
```

Esempio 3: questo esempio registra un'istanza con una finestra di manutenzione utilizzando i tag EC2.

```
$option1 = @{Key="tag:Environment";Values=@("Production")}
Register-SSMTargetWithMaintenanceWindow -WindowId "mw-06cf17cbefcb4bf4f" -Target
 $option1 -OwnerInformation "Production Web Servers" -ResourceType "INSTANCE"
```

Output:

```
2994977e-aefb-4a71-beac-df620352f184
```

- Per i dettagli sull'API, vedere [RegisterTargetWithMaintenanceWindow](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **RegisterTaskWithMaintenanceWindow** con una CLI

I seguenti esempi di codice mostrano come usare `RegisterTaskWithMaintenanceWindow`.

### CLI

#### AWS CLI

Esempio 1: per registrare un'attività di automazione con una finestra di manutenzione

L'esempio seguente `register-task-with-maintenance-window` registra un'attività di automazione con una finestra di manutenzione destinata a un'istanza.

```
aws ssm register-task-with-maintenance-window \
 --window-id "mw-082dcd7649EXAMPLE" \
 --targets Key=InstanceIds,Values=i-1234520122EXAMPLE \
 --task-arn AWS-RestartEC2Instance \
 --service-role-arn arn:aws:iam::111222333444:role/SSM --task-type AUTOMATION \
 --task-invocation-parameters "{\"Automation\":{\"DocumentVersion\":{\"\"$LATEST\"},\"Parameters\":{\"\"InstanceId\":{\"\"{{RESOURCE_ID}}\"}}}}\" \
 --priority 0 \
 --max-concurrency 1 \
 --max-errors 1 \
 --name "AutomationExample" \
 --description "Restarting EC2 Instance for maintenance"
```

Output:

```
{
 "WindowTaskId": "11144444-5555-6666-7777-88888888"
}
```

Per ulteriori informazioni, vedere [Register a Task with the Maintenance Window \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 2: come registrare un'attività con una finestra di manutenzione

L'esempio seguente `register-task-with-maintenance-window` registra un'attività Lambda con una finestra di manutenzione destinata a un'istanza.

```
aws ssm register-task-with-maintenance-window \
 --window-id "mw-082dcd7649dee04e4" \
 --targets Key=InstanceIds,Values=i-12344d305eEXAMPLE \
 --task-arn arn:aws:lambda:us-east-1:111222333444:function:SSMTestLAMBDA \
 --service-role-arn arn:aws:iam::111222333444:role/SSM \
 --task-type LAMBDA \
 --task-invocation-parameters '{"Lambda":{"Payload":{"\"InstanceId\":{\"\"{{RESOURCE_ID}}\"},\"targetType\":{\"\"{{TARGET_TYPE}}\"}},\"Qualifier\":\"$LATEST\"}}' \
 --priority 0 \
 --max-concurrency 10 \
```

```
--max-errors 5 \
--name "Lambda_Example" \
--description "My Lambda Example"
```

Output:

```
{
 "WindowTaskId": "22244444-5555-6666-7777-88888888"
}
```

Per ulteriori informazioni, vedere [Register a Task with the Maintenance Window \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 3: come registrare un'attività Run Command con una finestra di manutenzione

L'esempio seguente `register-task-with-maintenance-window` registra un'attività Run Command con una finestra di manutenzione destinata a un'istanza.

```
aws ssm register-task-with-maintenance-window \
 --window-id "mw-082dcd7649dee04e4" \
 --targets "Key=InstanceIds,Values=i-12344d305eEXAMPLE" \
 --service-role-arn "arn:aws:iam::111222333444:role/SSM" \
 --task-type "RUN_COMMAND" \
 --name "SSMInstallPowerShellModule" \
 --task-arn "AWS-InstallPowerShellModule" \
 --task-invocation-parameters "{\"RunCommand\":{\"Comment\":\"\",
 \"OutputS3BucketName\":\"runcommandlogs\", \"Parameters\":{\"commands\":[\"Get-
 Module -ListAvailable\"],\"executionTimeout\":[\"3600\"],\"source\":[\"https://
 \\\gallery.technet.microsoft.com/EZOut-33ae0fb7/file/110351/1/EZOut.zip\"],
 \"workingDirectory\":[\"\\\\\\\\\\\\\"],\"TimeoutSeconds\":600}}" \
 --max-concurrency 1 \
 --max-errors 1 \
 --priority 10
```

Output:

```
{
 "WindowTaskId": "33344444-5555-6666-7777-88888888"
}
```

Per ulteriori informazioni, vedere [Register a Task with the Maintenance Window \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

## Esempio 4: come registrare un'attività Step Functions con una finestra di manutenzione

L'esempio seguente `register-task-with-maintenance-window` registra un'attività Step Functions con una finestra di manutenzione destinata a un'istanza.

```
aws ssm register-task-with-maintenance-window \
 --window-id "mw-1234d787d6EXAMPLE" \
 --targets Key=WindowTargetIds,Values=12347414-69c3-49f8-95b8-ed2dcEXAMPLE \
 --task-arn arn:aws:states:us-east-1:111222333444:stateMachine:SSMTestStateMachine \
 --service-role-arn arn:aws:iam::111222333444:role/MaintenanceWindows \
 --task-type STEP_FUNCTIONS \
 --task-invocation-parameters '{"StepFunctions":{"Input":{"InstanceId":\
 "\"{{RESOURCE_ID}}\""}}}' \
 --priority 0 \
 --max-concurrency 10 \
 --max-errors 5 \
 --name "Step_Functions_Example" \
 --description "My Step Functions Example"
```

Output:

```
{
 "WindowTaskId": "444444444-5555-6666-7777-88888888"
}
```

Per ulteriori informazioni, vedere [Register a Task with the Maintenance Window \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

## Esempio 5: come registrare un'attività utilizzando un ID di destinazione della finestra di manutenzione

L'esempio seguente `register-task-with-maintenance-window` registra un'attività utilizzando un ID di destinazione della finestra di manutenzione. L'ID di destinazione della finestra di manutenzione era nell'output del comando `aws ssm register-target-with-maintenance-window`. È inoltre possibile recuperarlo dall'output del comando `aws ssm describe-maintenance-window-targets`.

```
aws ssm register-task-with-maintenance-window \
 --targets "Key=WindowTargetIds,Values=350d44e6-28cc-44e2-951f-4b2c9EXAMPLE" \
```

```
--task-arn "AWS-RunShellScript" \
--service-role-arn "arn:aws:iam::111222333444:role/MaintenanceWindowsRole" \
--window-id "mw-ab12cd34eEXAMPLE" \
--task-type "RUN_COMMAND" \
--task-parameters "{\"commands\":{\"Values\":[\"df\"]}}" \
--max-concurrency 1 \
--max-errors 1 \
--priority 10
```

Output:

```
{
 "WindowTaskId": "33344444-5555-6666-7777-88888888"
}
```

Per ulteriori informazioni, vedere [Register a Task with the Maintenance Window \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [RegisterTaskWithMaintenanceWindow](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio registra un'attività con una finestra di manutenzione utilizzando un ID di istanza. L'output è l'ID dell'attività.

```
$parameters = @{}
$parameterValues = New-Object
Amazon.SimpleSystemsManagement.Model.MaintenanceWindowTaskParameterValueExpression
$parameterValues.Values = @("Install")
$parameters.Add("Operation", $parameterValues)

Register-SSMTaskWithMaintenanceWindow -WindowId "mw-03a342e62c96d31b0"
-ServiceRoleArn "arn:aws:iam::123456789012:role/MaintenanceWindowsRole"
-MaxConcurrency 1 -MaxError 1 -TaskArn "AWS-RunShellScript" -Target
@{ Key="InstanceIds";Values="i-0000293ffd8c57862" } -TaskType "RUN_COMMAND" -
Priority 10 -TaskParameter $parameters
```

Output:



```
f34a2c47-ddfd-4c85-a88d-72366b69af1b
```

Esempio 2: questo esempio registra un'attività con una finestra di manutenzione utilizzando un ID di destinazione. L'output è l'ID dell'attività.

```
$parameters = @{}
$parameterValues = New-Object
 Amazon.SimpleSystemsManagement.Model.MaintenanceWindowTaskParameterValueExpression
$parameterValues.Values = @("Install")
$parameters.Add("Operation", $parameterValues)

register-ssmtaskwithmaintenancwindow -WindowId "mw-03a342e62c96d31b0"
 -ServiceRoleArn "arn:aws:iam::123456789012:role/MaintenanceWindowsRole"
 -MaxConcurrency 1 -MaxError 1 -TaskArn "AWS-RunShellScript" -Target
 @{ Key="WindowTargetIds";Values="350d44e6-28cc-44e2-951f-4b2c985838f6" } -
 TaskType "RUN_COMMAND" -Priority 10 -TaskParameter $parameters
```

Output:

```
f34a2c47-ddfd-4c85-a88d-72366b69af1b
```

Esempio 3: questo esempio crea un oggetto parametro per il documento di comando run **AWS-RunPowerShellScript** e crea un'attività con una determinata finestra di manutenzione utilizzando l'ID di destinazione. L'output restituito è l'ID dell'attività.

```
$parameters =
 [Collections.Generic.Dictionary[String,Collections.Generic.List[String]]]::new()
$parameters.Add("commands",@("ipconfig","dir env:\computername"))
$parameters.Add("executionTimeout",@(3600))

$props = @{
 WindowId = "mw-0123e4cce56ff78ae"
 ServiceRoleArn = "arn:aws:iam::123456789012:role/MaintenanceWindowsRole"
 MaxConcurrency = 1
 MaxError = 1
 TaskType = "RUN_COMMAND"
 TaskArn = "AWS-RunPowerShellScript"
 Target =
 @{Key="WindowTargetIds";Values="fe1234ea-56d7-890b-12f3-456b789bee0f"}
 Priority = 1
 RunCommand_Parameter = $parameters
```

```
Name = "set-via-cmdlet"
}

Register-SSMTaskWithMaintenanceWindow @props
```

Output:

```
f1e2ef34-5678-12e3-456a-12334c5c6cbe
```

Esempio 4: questo esempio registra un'attività di AWS Systems Manager Automation utilizzando un documento denominato **Create-Snapshots**

```
$automationParameters = @{}
$automationParameters.Add("instanceId", @"({{ TARGET_ID }}"))
$automationParameters.Add("AutomationAssumeRole",
 @"({arn:aws:iam::111111111111:role/AutomationRole})")
$automationParameters.Add("SnapshotTimeout", @"(PT20M)")
Register-SSMTaskWithMaintenanceWindow -WindowId mw-123EXAMPLE456`
 -ServiceRoleArn "arn:aws:iam::123456789012:role/MW-Role"`
 -MaxConcurrency 1 -MaxError 1 -TaskArn "CreateVolumeSnapshots"`
 -Target @{ Key="WindowTargetIds";Values="4b5acdf4-946c-4355-
bd68-4329a43a5fd1" }`
 -TaskType "AUTOMATION"`
 -Priority 4`
 -Automation_DocumentVersion '$DEFAULT' -Automation_Parameter
$automationParameters -Name "Create-Snapshots"
```

- Per i dettagli sull'API, vedere [RegisterTaskWithMaintenanceWindow](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio registra un'attività con una finestra di manutenzione utilizzando un ID di istanza. L'output è l'ID dell'attività.

```
$parameters = @{}
$parameterValues = New-Object
 Amazon.SimpleSystemsManagement.Model.MaintenanceWindowTaskParameterValueExpression
$parameterValues.Values = @"(Install)"
$parameters.Add("Operation", $parameterValues)
```

```
Register-SSMTaskWithMaintenanceWindow -WindowId "mw-03a342e62c96d31b0"
-ServiceRoleArn "arn:aws:iam::123456789012:role/MaintenanceWindowsRole"
-MaxConcurrency 1 -MaxError 1 -TaskArn "AWS-RunShellScript" -Target
@{ Key="InstanceIds";Values="i-0000293ffd8c57862" } -TaskType "RUN_COMMAND" -
Priority 10 -TaskParameter $parameters
```

Output:

```
f34a2c47-ddfd-4c85-a88d-72366b69af1b
```

Esempio 2: questo esempio registra un'attività con una finestra di manutenzione utilizzando un ID di destinazione. L'output è l'ID dell'attività.

```
$parameters = @{}
$parameterValues = New-Object
Amazon.SimpleSystemsManagement.Model.MaintenanceWindowTaskParameterValueExpression
$parameterValues.Values = @("Install")
$parameters.Add("Operation", $parameterValues)

register-ssmtaskwithmaintenancewindow -WindowId "mw-03a342e62c96d31b0"
-ServiceRoleArn "arn:aws:iam::123456789012:role/MaintenanceWindowsRole"
-MaxConcurrency 1 -MaxError 1 -TaskArn "AWS-RunShellScript" -Target
@{ Key="WindowTargetIds";Values="350d44e6-28cc-44e2-951f-4b2c985838f6" } -
TaskType "RUN_COMMAND" -Priority 10 -TaskParameter $parameters
```

Output:

```
f34a2c47-ddfd-4c85-a88d-72366b69af1b
```

Esempio 3: questo esempio crea un oggetto parametro per il documento di comando run **AWS-RunPowerShellScript** e crea un'attività con una determinata finestra di manutenzione utilizzando l'ID di destinazione. L'output restituito è l'ID dell'attività.

```
$parameters =
[Collections.Generic.Dictionary[String,Collections.Generic.List[String]]]::new()
$parameters.Add("commands",@("ipconfig","dir env:\computername"))
$parameters.Add("executionTimeout",@(3600))

$props = @{
 WindowId = "mw-0123e4cce56ff78ae"
 ServiceRoleArn = "arn:aws:iam::123456789012:role/MaintenanceWindowsRole"
```

```

 MaxConcurrency = 1
 MaxError = 1
 TaskType = "RUN_COMMAND"
 TaskArn = "AWS-RunPowerShellScript"
 Target =
 @{Key="WindowTargetIds";Values="fe1234ea-56d7-890b-12f3-456b789bee0f"}
 Priority = 1
 RunCommand_Parameter = $parameters
 Name = "set-via-cmdlet"
}

Register-SSMTaskWithMaintenanceWindow @props

```

Output:

```
f1e2ef34-5678-12e3-456a-12334c5c6cbe
```

Esempio 4: questo esempio registra un'attività di AWS Systems Manager Automation utilizzando un documento denominato. **Create-Snapshots**

```

$automationParameters = @{}
$automationParameters.Add("instanceId", @("{ TARGET_ID }"))
$automationParameters.Add("AutomationAssumeRole",
 @("{arn:aws:iam::111111111111:role/AutomationRole}"))
$automationParameters.Add("SnapshotTimeout", @("PT20M"))
Register-SSMTaskWithMaintenanceWindow -WindowId mw-123EXAMPLE456`
 -ServiceRoleArn "arn:aws:iam::123456789012:role/MW-Role"`
 -MaxConcurrency 1 -MaxError 1 -TaskArn "CreateVolumeSnapshots"`
 -Target @{ Key="WindowTargetIds";Values="4b5acdf4-946c-4355-
bd68-4329a43a5fd1" }`
 -TaskType "AUTOMATION"`
 -Priority 4`
 -Automation_DocumentVersion '$DEFAULT' -Automation_Parameter
$automationParameters -Name "Create-Snapshots"

```

- Per i dettagli sull'API, vedere [RegisterTaskWithMaintenanceWindow](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **RemoveTagsFromResource** con una CLI

I seguenti esempi di codice mostrano come usare **RemoveTagsFromResource**.

### CLI

#### AWS CLI

Per rimuovere un tag da una baseline delle patch

L'esempio seguente `remove-tags-from-resource` mostra come rimuovere i tag da una baseline delle patch.

```
aws ssm remove-tags-from-resource \
 --resource-type "PatchBaseline" \
 --resource-id "pb-0123456789abcdef0" \
 --tag-keys "Region"
```

Questo comando non produce alcun output.

Per ulteriori informazioni, vedere [Tagging AWS Resources](#) nella Guida AWS generale.

- Per i dettagli sull'API, vedi [RemoveTagsFromResource](#) in AWS CLI Command Reference.

### PowerShell

#### Strumenti per PowerShell V4

Esempio 1: questo esempio rimuove un tag da una finestra di manutenzione. Se il comando va a buon fine, non viene generato output.

```
Remove-SSMResourceTag -ResourceId "mw-03eb9db42890fb82d" -ResourceType
"MaintenanceWindow" -TagKey "Production"
```

- Per i dettagli sull'API, vedere [RemoveTagsFromResource](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

#### Strumenti per V5 PowerShell

Esempio 1: questo esempio rimuove un tag da una finestra di manutenzione. Se il comando va a buon fine, non viene generato output.

```
Remove-SSMResourceTag -ResourceId "mw-03eb9db42890fb82d" -ResourceType
"MaintenanceWindow" -TagKey "Production"
```

- Per i dettagli sull'API, vedere [RemoveTagsFromResource](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Usare **SendCommand** con un AWS SDK o CLI

I seguenti esempi di codice mostrano come usare `SendCommand`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- [Informazioni di base](#)

### CLI

#### AWS CLI

Esempio 1: eseguire un comando su una o più istanze remote

L'esempio seguente `send-command` esegue un comando `echo` su un'istanza di destinazione.

```
aws ssm send-command \
 --document-name "AWS-RunShellScript" \
 --parameters 'commands=["echo HelloWorld"]' \
 --targets "Key=instanceids,Values=i-1234567890abcdef0" \
 --comment "echo HelloWorld"
```

Output:

```
{
 "Command": {
 "CommandId": "92853adf-ba41-4cd6-9a88-142d1EXAMPLE",
 "DocumentName": "AWS-RunShellScript",
 "DocumentVersion": "",
 "Comment": "echo HelloWorld",
```

```

 "ExpiresAfter": 1550181014.717,
 "Parameters": {
 "commands": [
 "echo HelloWorld"
]
 },
 "InstanceIds": [
 "i-0f00f008a2dcbe2"
],
 "Targets": [],
 "RequestedDateTime": 1550173814.717,
 "Status": "Pending",
 "StatusDetails": "Pending",
 "OutputS3BucketName": "",
 "OutputS3KeyPrefix": "",
 "MaxConcurrency": "50",
 "MaxErrors": "0",
 "TargetCount": 1,
 "CompletedCount": 0,
 "ErrorCount": 0,
 "DeliveryTimedOutCount": 0,
 "ServiceRole": "",
 "NotificationConfig": {
 "NotificationArn": "",
 "NotificationEvents": [],
 "NotificationType": ""
 },
 "CloudWatchOutputConfig": {
 "CloudWatchLogGroupName": "",
 "CloudWatchOutputEnabled": false
 }
 }
}

```

Per ulteriori informazioni, consulta [Eseguire comandi utilizzando Systems Manager Run Command](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 2: per ottenere informazioni sull'IP di un'istanza

L'esempio seguente `send-command` recupera le informazioni sull'IP di un'istanza.

```

aws ssm send-command \
 --instance-ids "i-1234567890abcdef0" \

```

```
--document-name "AWS-RunShellScript" \
--comment "IP config" \
--parameters "commands=ifconfig"
```

Vedi l'esempio 1 per un output di esempio.

Per ulteriori informazioni, consulta [Eseguire comandi utilizzando Systems Manager Run Command](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 3: eseguire un comando su istanze con tag specifici

L'esempio seguente send-command esegue un comando sulle istanze che hanno la chiave di tag "ENV" e il valore "Dev".

```
aws ssm send-command \
 --targets "Key=tag:ENV,Values=Dev" \
 --document-name "AWS-RunShellScript" \
 --parameters "commands=ifconfig"
```

Vedi l'esempio 1 per un output di esempio.

Per ulteriori informazioni, consulta [Eseguire comandi utilizzando Systems Manager Run Command](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 4: come eseguire un comando che invia notifiche SNS

L'esempio seguente send-command esegue un comando che invia notifiche SNS per tutti gli eventi di notifica e il tipo di notifica Command.

```
aws ssm send-command \
 --instance-ids "i-1234567890abcdef0" \
 --document-name "AWS-RunShellScript" \
 --comment "IP config" \
 --parameters "commands=ifconfig" \
 --service-role-arn "arn:aws:iam::123456789012:role/SNS_Role" \
 --notification-config "NotificationArn=arn:aws:sns:us-east-1:123456789012:SNSTopicName,NotificationEvents=All,NotificationType=Command"
```

Vedi l'esempio 1 per un output di esempio.

Per ulteriori informazioni, consulta [Eseguire comandi utilizzando Systems Manager Run Command](#) nella Guida per l'utente di AWS Systems Manager.



### Esempio 5: eseguire un comando che invia a S3 e CloudWatch

L'esempio seguente esegue un comando che invia i dettagli del comando a un bucket S3 e a un gruppo di log Logs. CloudWatch

```
aws ssm send-command \
 --instance-ids "i-1234567890abcdef0" \
 --document-name "AWS-RunShellScript" \
 --comment "IP config" \
 --parameters "commands=ifconfig" \
 --output-s3-bucket-name "s3-bucket-name" \
 --output-s3-key-prefix "runcommand" \
 --cloud-watch-output-
config "CloudWatchOutputEnabled=true,CloudWatchLogGroupName=CWLGroupName"
```

Vedi l'esempio 1 per un output di esempio.

Per ulteriori informazioni, consulta [Eseguire comandi utilizzando Systems Manager Run Command](#) nella Guida per l'utente di AWS Systems Manager.

### Esempio 6: come eseguire comandi su più istanze con tag diversi

L'esempio seguente send-command esegue un comando su istanze con due chiavi e valori di tag diversi.

```
aws ssm send-command \
 --document-name "AWS-RunPowerShellScript" \
 --parameters commands=["echo helloWorld"] \
 --targets Key=tag:Env,Values=Dev Key=tag:Role,Values=WebServers
```

Vedi l'esempio 1 per un output di esempio.

Per ulteriori informazioni, consulta [Eseguire comandi utilizzando Systems Manager Run Command](#) nella Guida per l'utente di AWS Systems Manager.

### Esempio 7: come indirizzare più istanze con la stessa chiave di tag

L'esempio seguente send-command esegue un comando su istanze che hanno la stessa chiave di tag ma con valori diversi.

```
aws ssm send-command \
 --document-name "AWS-RunPowerShellScript" \
 --parameters commands=["echo helloWorld"]
```

```
--targets Key=tag:Env,Values=Dev,Test
```

Vedi l'esempio 1 per un output di esempio.

Per ulteriori informazioni, consulta [Eseguire comandi utilizzando Systems Manager Run Command](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 8: come eseguire un comando che utilizza un documento condiviso

L'esempio seguente send-command esegue un documento condiviso su un'istanza di destinazione.

```
aws ssm send-command \
 --document-name "arn:aws:ssm:us-east-1:123456789012:document/ExampleDocument" \
 --targets "Key=instanceids,Values=i-1234567890abcdef0"
```

Vedi l'esempio 1 per un output di esempio.

Per ulteriori informazioni, consulta [Utilizzo di documenti condivisi SSM](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [SendCommand](#) in AWS CLI Command Reference.

## Java

### SDK per Java 2.x

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
/**
 * Sends a SSM command to a managed node asynchronously.
 *
 * @param documentName The name of the document to use.
 * @param instanceId The ID of the instance to send the command to.
 * @return The command ID.
 * <p>
```

```
 * This method initiates asynchronous requests to send a SSM command to a
 managed node.
 * It waits until the document is active, sends the command, and checks the
 command execution status.
 */
 public String sendSSMCommand(String documentName, String instanceId) throws
 InterruptedException, SsmException {
 // Before we use Document to send a command - make sure it is active.
 CompletableFuture<Void> documentActiveFuture =
 CompletableFuture.runAsync(() -> {
 boolean isDocumentActive = false;
 DescribeDocumentRequest request = DescribeDocumentRequest.builder()
 .name(documentName)
 .build();

 while (!isDocumentActive) {
 CompletableFuture<DescribeDocumentResponse> response =
 getAsyncClient().describeDocument(request);
 String documentStatus =
 response.join().document().statusAsString();
 if (documentStatus.equals("Active")) {
 System.out.println("The SSM document is active and ready to
 use.");
 isDocumentActive = true;
 } else {
 System.out.println("The SSM document is not active. Status: "
 + documentStatus);
 try {
 Thread.sleep(5000);
 } catch (InterruptedException e) {
 throw new RuntimeException(e);
 }
 }
 }
 });

 documentActiveFuture.join();

 // Create the SendCommandRequest.
 SendCommandRequest commandRequest = SendCommandRequest.builder()
 .documentName(documentName)
 .instanceIds(instanceId)
 .build();
```

```

 // Send the command.
 CompletableFuture<SendCommandResponse> commandFuture =
getAsyncClient().sendCommand(commandRequest);
 final String[] commandId = {null};

 commandFuture.whenComplete((commandResponse, ex) -> {
 if (commandResponse != null) {
 commandId[0] = commandResponse.command().commandId();
 System.out.println("Command ID: " + commandId[0]);

 // Wait for the command execution to complete.
 GetCommandInvocationRequest invocationRequest =
GetCommandInvocationRequest.builder()
 .commandId(commandId[0])
 .instanceId(instanceId)
 .build();

 try {
 System.out.println("Wait 5 secs");
 TimeUnit.SECONDS.sleep(5);

 // Retrieve the command execution details.
 CompletableFuture<GetCommandInvocationResponse>
invocationFuture = getAsyncClient().getCommandInvocation(invocationRequest);
 invocationFuture.whenComplete((commandInvocationResponse,
invocationEx) -> {
 if (commandInvocationResponse != null) {
 // Check the status of the command execution.
 CommandInvocationStatus status =
commandInvocationResponse.status();
 if (status == CommandInvocationStatus.SUCCESS) {
 System.out.println("Command execution
successful");
 } else {
 System.out.println("Command execution failed.
Status: " + status);
 }
 } else {
 Throwable invocationCause = (invocationEx instanceof
CompletionException) ? invocationEx.getCause() : invocationEx;
 throw new CompletionException(invocationCause);
 }
 }).join();
 } catch (InterruptedException e) {

```

```

 throw new RuntimeException(e);
 }
 } else {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
 if (cause instanceof SsmException) {
 throw (SsmException) cause;
 } else {
 throw new RuntimeException(cause);
 }
 }
}).join();

return commandId[0];
}

```

- Per i dettagli sulle API, consulta la [SendCommand](#) sezione AWS SDK for Java 2.x API Reference.

## JavaScript

### SDK per JavaScript (v3)

#### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```

import { SendCommandCommand, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Send an SSM command to a managed node.
 * @param {{ documentName: string }}
 */
export const main = async ({ documentName }) => {
 const client = new SSMClient({});
 try {
 await client.send(

```

```

 new SendCommandCommand({
 DocumentName: documentName,
 }),
);
 console.log("Command sent successfully.");
 return { Success: true };
} catch (caught) {
 if (caught instanceof Error && caught.name === "ValidationError") {
 console.warn(`${caught.message}. Did you provide a valid document name?`);
 } else {
 throw caught;
 }
}
};

```

- Per i dettagli sulle API, consulta la [SendCommand](#) sezione AWS SDK per JavaScript API Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio esegue un comando echo su un'istanza di destinazione.

```
Send-SSMCommand -DocumentName "AWS-RunPowerShellScript" -Parameter @{commands =
"echo helloWorld"} -Target @{Key="instanceids";Values=@"i-0cb2b964d3e14fd9f"}}
```

Output:

```

CommandId : d8d190fc-32c1-4d65-a0df-ff5ff3965524
Comment :
CompletedCount : 0
DocumentName : AWS-RunPowerShellScript
ErrorCount : 0
ExpiresAfter : 3/7/2017 10:48:37 PM
InstanceIds : {}
MaxConcurrency : 50
MaxErrors : 0
NotificationConfig : Amazon.SimpleSystemsManagement.Model.NotificationConfig
OutputS3BucketName :
OutputS3KeyPrefix :

```

```

OutputS3Region :
Parameters : {[commands,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
RequestedDateTime : 3/7/2017 9:48:37 PM
ServiceRole :
Status : Pending
StatusDetails : Pending
TargetCount : 0
Targets : {instanceids}

```

Esempio 2: questo esempio mostra come eseguire un comando che accetta parametri annidati.

```

Send-SSMCommand -DocumentName "AWS-RunRemoteScript" -Parameter
 @{ sourceType="GitHub";sourceInfo='{ "owner": "me","repository": "amazon-
 ssm","path": "Examples/Install-Win32openSSH"}'; "commandLine"=".\\Install-
 Win32openSSH.ps1"} -InstanceId i-0cb2b964d3e14fd9f

```

- Per i dettagli sull'API, vedere [SendCommand](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio esegue un comando echo su un'istanza di destinazione.

```

Send-SSMCommand -DocumentName "AWS-RunPowerShellScript" -Parameter @{commands =
 "echo helloWorld"} -Target @{Key="instanceids";Values=@("i-0cb2b964d3e14fd9f")}

```

Output:

```

CommandId : d8d190fc-32c1-4d65-a0df-ff5ff3965524
Comment :
CompletedCount : 0
DocumentName : AWS-RunPowerShellScript
ErrorCount : 0
ExpiresAfter : 3/7/2017 10:48:37 PM
InstanceIds : {}
MaxConcurrency : 50
MaxErrors : 0
NotificationConfig : Amazon.SimpleSystemsManagement.Model.NotificationConfig
OutputS3BucketName :
OutputS3KeyPrefix :
OutputS3Region :

```

```
Parameters : {[commands,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
RequestedDateTime : 3/7/2017 9:48:37 PM
ServiceRole :
Status : Pending
StatusDetails : Pending
TargetCount : 0
Targets : {instanceids}
```

Esempio 2: questo esempio mostra come eseguire un comando che accetta parametri annidati.

```
Send-SSMCommand -DocumentName "AWS-RunRemoteScript" -Parameter
@{ sourceType="GitHub";sourceInfo='{ "owner": "me","repository": "amazon-
ssm","path": "Examples/Install-Win32OpenSSH"}'; "commandLine"=".\\Install-
Win32OpenSSH.ps1"} -InstanceId i-0cb2b964d3e14fd9f
```

- Per i dettagli sull'API, vedere [SendCommand](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
class DocumentWrapper:
 """Encapsulates AWS Systems Manager Document actions."""

 def __init__(self, ssm_client):
 """
 :param ssm_client: A Boto3 Systems Manager client.
 """
 self.ssm_client = ssm_client
 self.name = None
```



```
@classmethod
def from_client(cls):
 ssm_client = boto3.client("ssm")
 return cls(ssm_client)

def send_command(self, instance_ids):
 """
 Sends a command to one or more instances.

 :param instance_ids: The IDs of the instances to send the command to.
 :return: The ID of the command.
 """
 try:
 response = self.ssm_client.send_command(
 InstanceIds=instance_ids, DocumentName=self.name,
 TimeoutSeconds=3600
)
 return response["Command"]["CommandId"]
 except ClientError as err:
 logger.error(
 "Couldn't send command to %s. Here's why: %s: %s",
 self.name,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise
```

- Per i dettagli sulle API, vedi [SendCommand](#) in AWS SDK for Python (Boto3) API Reference.

## SAP ABAP

### SDK per SAP ABAP

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```

TRY.
 DATA(lo_result) = lo_ssm->sendcommand(
 it_instanceids = it_instance_ids
 iv_documentname = iv_document_name
 iv_timeoutseconds = 3600).
 DATA(lo_command) = lo_result->get_command().
 IF lo_command IS BOUND.
 rv_command_id = lo_command->get_commandid().
 MESSAGE 'Command sent successfully.' TYPE 'I'.
 ENDIF.
CATCH /aws1/cx_ssminvaliddocument.
 MESSAGE 'Invalid document.' TYPE 'I'.
CATCH /aws1/cx_ssminvalidinstanceid.
 MESSAGE 'Invalid instance ID.' TYPE 'I'.
ENDTRY.

```

- Per i dettagli sulle API, consulta [SendCommand](#) la sezione AWS SDK for SAP ABAP API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **StartAutomationExecution** con una CLI

I seguenti esempi di codice mostrano come usare **StartAutomationExecution**.

### CLI

#### AWS CLI

Esempio 1: per eseguire un documento di automazione

L'esempio seguente **start-automation-execution** esegue un documento di automazione.

```

aws ssm start-automation-execution \
 --document-name "AWS-UpdateLinuxAmi" \
 --parameters "AutomationAssumeRole=arn:aws:iam::123456789012:role/
SSMAutomationRole,SourceAmiId=ami-EXAMPLE,IamInstanceProfileName=EC2InstanceRole"

```

Output:

```
{
 "AutomationExecutionId": "4105a4fc-f944-11e6-9d32-0a1b2EXAMPLE"
}
```

Per ulteriori informazioni, consulta [Esecuzione manuale di un flusso di lavoro di automazione](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 2: come eseguire un documento di automazione condiviso

L'esempio seguente `start-automation-execution` esegue un documento di automazione condiviso.

```
aws ssm start-automation-execution \
 --document-name "arn:aws:ssm:us-east-1:123456789012:document/ExampleDocument"
```

Output:

```
{
 "AutomationExecutionId": "4105a4fc-f944-11e6-9d32-0a1b2EXAMPLE"
}
```

Per ulteriori informazioni, consulta [Utilizzo di documenti condivisi SSM](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [StartAutomationExecution](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio esegue un documento che specifica un ruolo di automazione, un ID di origine AMI e un ruolo di istanza Amazon EC2.

```
Start-SSMAutomationExecution -DocumentName AWS-UpdateLinuxAmi -
Parameter @{'AutomationAssumeRole'='arn:aws:iam::123456789012:role/
SSMAutomationRole';'SourceAmiId'='ami-
f173cc91';'InstanceIamRole'='EC2InstanceRole'}
```

Output:

```
3a532a4f-0382-11e7-9df7-6f11185f6dd1
```

- Per i dettagli sull'API, vedere [StartAutomationExecution](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio esegue un documento che specifica un ruolo di automazione, un ID di origine AMI e un ruolo di istanza Amazon EC2.

```
Start-SSMAutomationExecution -DocumentName AWS-UpdateLinuxAmi -
Parameter @{'AutomationAssumeRole'='arn:aws:iam::123456789012:role/
SSMAutomationRole';'SourceAmiId'='ami-
f173cc91';'InstanceIamRole'='EC2InstanceRole'}
```

Output:

```
3a532a4f-0382-11e7-9df7-6f11185f6dd1
```

- Per i dettagli sull'API, vedere [StartAutomationExecution](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **StartSession** con una CLI

I seguenti esempi di codice mostrano come usare `StartSession`.

### CLI

#### AWS CLI

Esempio 1: per avviare una sessione di Session Manager

Questo esempio `start-session` stabilisce una connessione con un'istanza per una sessione di Session Manager. Si noti che questo comando interattivo richiede l'installazione del plug-in Session Manager sul computer client che effettua la chiamata.

```
aws ssm start-session \
```

```
--target "i-1234567890abcdef0"
```

Output:

```
Starting session with SessionId: Jane-Roe-07a16060613c408b5
```

Esempio 2: come avviare una sessione di Session Manager utilizzando SSH

Questo esempio `start-session` stabilisce una connessione con un'istanza per una sessione di Session Manager utilizzando SSH. Si noti che questo comando interattivo richiede l'installazione del plug-in Session Manager sul computer client che effettua la chiamata e che utilizza l'utente predefinito sull'istanza, ad esempio per le istanze `ec2-user` EC2 per Linux.

```
ssh -i /path/my-key-pair.pem ec2-user@i-02573cafcfEXAMPLE
```

Output:

```
Starting session with SessionId: ec2-user-07a16060613c408b5
```

Per ulteriori informazioni, vedere [Avvio di una sessione](#) e [installazione del plug-in Session Manager per la AWS CLI](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [StartSession](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio avvia una connessione a una destinazione per una sessione di Session Manager, abilitando il port forwarding.

```
Start-SSMSession -Target 'i-064578e5e7454488f' -DocumentName 'AWS-
StartPortForwardingSession' -Parameter @{ localPortNumber = '8080'; portNumber =
'80' }
```

Output:

SessionId	StreamUrl
-----	-----
random-id0	wss://ssmmessages.amazonaws.com/v1/data-channel/random-id

- Per i dettagli sull'API, vedere [StartSession](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio avvia una connessione a una destinazione per una sessione di Session Manager, abilitando il port forwarding. Nota: è necessario aggiungere il parametro Region se non è già stato impostato mediante AWSCredentials.

```
Start-SSMSession -Target 'i-064578e5e7454488f' -DocumentName 'AWS-
StartPortForwardingSession' -Parameter @{ localPortNumber = '8080'; portNumber =
'80' } -Region 'us-west-1'
```

Output:

```
Starting session with SessionId: testUser-xi4glew849asyeryde34u4dfsdfy
Port 8080 opened for sessionId testUser-xi4glew849asyeryde34u4dfsdfy.
Waiting for connections...
```

Esempio 2: questo esempio crea una sessione interattiva con un'istanza specificata per una sessione di Session Manager.

```
Start-SSMSession -Target 'i-1234567890abcdef0' -Region 'us-west-1'
```

Output:

```
Starting session with SessionId : testUser-xi4glew849asyeryde34u4dfsdfy
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
Install the latest PowerShell for new features and improvements!
```

```
PS C:\Windows\system32> whoami
ec2amaz-fnsdrwv\ec2-test-user
PS C:\Windows\system32>
```

Esempio 3: questo esempio crea una sessione senza connettersi ad essa e restituisce le TokenValue proprietà SessionId StreamUrl,, e richieste per connettersi alla sessione.

```
Start-SSMSession -Target 'i-1234567890abcdef0' -Region 'us-west-1' -
DisablePluginInvocation
```

Output:

```
SessionId : testUser-xi4glew849asyeryde34u4dfsdfy
StreamUrl : {StreamUrl value redacted}
TokenValue : {Token value redacted}
ContentLength : 1207
HttpStatusCode : OK
```

- Per i dettagli sull'API, vedere [StartSession](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **StopAutomationExecution** con una CLI

I seguenti esempi di codice mostrano come usare `StopAutomationExecution`.

### CLI

#### AWS CLI

Per interrompere l'esecuzione di un'automazione

L'esempio seguente `stop-automation-execution` interrompe un documento di automazione.

```
aws ssm stop-automation-execution
--automation-execution-id "4105a4fc-f944-11e6-9d32-0a1b2EXAMPLE"
```

Questo comando non produce alcun output.

Per ulteriori informazioni, consulta [Esecuzione manuale di un flusso di lavoro di automazione](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [StopAutomationExecution](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio interrompe un'esecuzione di automazione. Se il comando va a buon fine, non viene generato output.

```
Stop-SSMAutomationExecution -AutomationExecutionId "4105a4fc-f944-11e6-9d32-8fb2db27a909"
```

- Per i dettagli sull'API, vedere [StopAutomationExecution](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio interrompe un'esecuzione di automazione. Se il comando va a buon fine, non viene generato output.

```
Stop-SSMAutomationExecution -AutomationExecutionId "4105a4fc-f944-11e6-9d32-8fb2db27a909"
```

- Per i dettagli sull'API, vedere [StopAutomationExecution](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **UpdateAssociation** con una CLI

I seguenti esempi di codice mostrano come usare `UpdateAssociation`.

### CLI

#### AWS CLI

Esempio 1: per aggiornare un'associazione di documenti

L'esempio seguente `update-association` aggiorna l'associazione a una nuova versione del documento.



```
aws ssm update-association \
 --association-id "8dfe3659-4309-493a-8755-0123456789ab" \
 --document-version "$LATEST"
```

Output:

```
{
 "AssociationDescription": {
 "Name": "AWS-UpdateSSMAgent",
 "AssociationVersion": "2",
 "Date": 1550508093.293,
 "LastUpdateAssociationDate": 1550508106.596,
 "Overview": {
 "Status": "Pending",
 "DetailedStatus": "Creating"
 },
 "DocumentVersion": "$LATEST",
 "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
 "Targets": [
 {
 "Key": "tag:Name",
 "Values": [
 "Linux"
]
 }
],
 "LastExecutionDate": 1550508094.879,
 "LastSuccessfulExecutionDate": 1550508094.879
 }
}
```

Per ulteriori informazioni, consulta [Modifica e creazione di una nuova versione di un'associazione](#) nella Guida per l'utente di AWS Systems Manager.

Esempio 2: come aggiornare l'espressione di pianificazione di un'associazione

L'esempio seguente update-association aggiorna l'espressione di pianificazione per l'associazione specificata.

```
aws ssm update-association \
 --association-id "8dfe3659-4309-493a-8755-0123456789ab" \
 --schedule-expression "cron(0 0 0/4 1/1 * ? *)"
```

## Output:

```
{
 "AssociationDescription": {
 "Name": "AWS-HelloWorld",
 "AssociationVersion": "2",
 "Date": "2021-02-08T13:54:19.203000-08:00",
 "LastUpdateAssociationDate": "2021-06-29T11:51:07.933000-07:00",
 "Overview": {
 "Status": "Pending",
 "DetailedStatus": "Creating"
 },
 "DocumentVersion": "$DEFAULT",
 "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
 "Targets": [
 {
 "Key": "aws:NoOpAutomationTag",
 "Values": [
 "AWS-NoOpAutomationTarget-Value"
]
 }
],
 "ScheduleExpression": "cron(0 0 0/4 1/1 * ? *)",
 "LastExecutionDate": "2021-06-26T19:00:48.110000-07:00",
 "ApplyOnlyAtCronInterval": false
 }
}
```

Per ulteriori informazioni, consulta [Modifica e creazione di una nuova versione di un'associazione](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [UpdateAssociation](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio aggiorna un'associazione con una nuova versione del documento.

```
Update-SSMAssociation -AssociationId "93285663-92df-44cb-9f26-2292d4ecc439" -
DocumentVersion "1"
```

**Output:**

```
Name : AWS-UpdateSSMAgent
InstanceId :
Date : 3/1/2017 6:22:21 PM
Status.Name :
Status.Date :
Status.Message :
Status.AdditionalInfo :
```

- Per i dettagli sull'API, vedere [UpdateAssociation](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

**Strumenti per V5 PowerShell**

Esempio 1: questo esempio aggiorna un'associazione con una nuova versione del documento.

```
Update-SSMAssociation -AssociationId "93285663-92df-44cb-9f26-2292d4ecc439" -
DocumentVersion "1"
```

**Output:**

```
Name : AWS-UpdateSSMAgent
InstanceId :
Date : 3/1/2017 6:22:21 PM
Status.Name :
Status.Date :
Status.Message :
Status.AdditionalInfo :
```

- Per i dettagli sull'API, vedere [UpdateAssociation](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

**Utilizzo di `UpdateAssociationStatus` con una CLI**

I seguenti esempi di codice mostrano come usare `UpdateAssociationStatus`.

## CLI

### AWS CLI

Per aggiornare lo stato dell'associazione

L'esempio seguente `update-association-status` aggiorna lo stato dell'associazione tra un'istanza e un documento.

```
aws ssm update-association-status \
 --name "AWS-UpdateSSMAgent" \
 --instance-id "i-1234567890abcdef0" \
 --association-
status "Date=1424421071.939,Name=Pending,Message=temp_status_change,AdditionalInfo=Additi
Config-Needed"
```

Output:

```
{
 "AssociationDescription": {
 "Name": "AWS-UpdateSSMAgent",
 "InstanceId": "i-1234567890abcdef0",
 "AssociationVersion": "1",
 "Date": 1550507529.604,
 "LastUpdateAssociationDate": 1550507806.974,
 "Status": {
 "Date": 1424421071.0,
 "Name": "Pending",
 "Message": "temp_status_change",
 "AdditionalInfo": "Additional-Config-Needed"
 },
 "Overview": {
 "Status": "Success",
 "AssociationStatusAggregatedCount": {
 "Success": 1
 }
 },
 "DocumentVersion": "$DEFAULT",
 "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
 "Targets": [
 {
 "Key": "InstanceIds",
 "Values": [
```

```

 "i-1234567890abcdef0"
]
}
],
"LastExecutionDate": 1550507808.0,
"LastSuccessfulExecutionDate": 1550507808.0
}
}

```

Per ulteriori informazioni, consulta [Utilizzo delle associazioni in Systems Manager](#) nella AWS Guida per l'utente di Systems Manager.

- Per i dettagli sull'API, vedi [UpdateAssociationStatus](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio aggiorna lo stato dell'associazione tra un'istanza e un documento di configurazione.

```

Update-SSMAssociationStatus -Name "AWS-UpdateSSMAgent" -InstanceId
 "i-0000293ffd8c57862" -AssociationStatus_Date "2015-02-20T08:31:11Z"
 -AssociationStatus_Name "Pending" -AssociationStatus_Message
 "temporary_status_change" -AssociationStatus_AdditionalInfo "Additional-Config-
 Needed"

```

Output:

```

Name : AWS-UpdateSSMAgent
InstanceId : i-0000293ffd8c57862
Date : 2/23/2017 6:55:22 PM
Status.Name : Pending
Status.Date : 2/20/2015 8:31:11 AM
Status.Message : temporary_status_change
Status.AdditionalInfo : Additional-Config-Needed

```

- Per i dettagli sull'API, vedere [UpdateAssociationStatus](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio aggiorna lo stato dell'associazione tra un'istanza e un documento di configurazione.

```
Update-SSMAssociationStatus -Name "AWS-UpdateSSMAgent" -InstanceId
"i-0000293ffd8c57862" -AssociationStatus_Date "2015-02-20T08:31:11Z"
-AssociationStatus_Name "Pending" -AssociationStatus_Message
"temporary_status_change" -AssociationStatus_AdditionalInfo "Additional-Config-
Needed"
```

Output:

```
Name : AWS-UpdateSSMAgent
InstanceId : i-0000293ffd8c57862
Date : 2/23/2017 6:55:22 PM
Status.Name : Pending
Status.Date : 2/20/2015 8:31:11 AM
Status.Message : temporary_status_change
Status.AdditionalInfo : Additional-Config-Needed
```

- Per i dettagli sull'API, vedere [UpdateAssociationStatus](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **UpdateDocument** con una CLI

I seguenti esempi di codice mostrano come usare `UpdateDocument`.

### CLI

#### AWS CLI

Per creare una nuova versione di un documento

L'esempio seguente `update-document` crea una nuova versione di un documento quando viene eseguito su un computer Windows. Il documento specificato da `--document` deve

essere in formato JSON. Nota che `file://` deve essere referenziato seguito dal percorso del file di contenuto. A causa di `$` all'inizio del parametro `--document-version`, in Windows è necessario racchiudere il valore tra virgolette doppie. Su Linux, macOS o quando PowerShell richiesto, è necessario racchiudere il valore tra virgolette singole.

Versione Windows:

```
aws ssm update-document \
 --name "RunShellScript" \
 --content "file://RunShellScript.json" \
 --document-version "$LATEST"
```

Linux/Mac versione:

```
aws ssm update-document \
 --name "RunShellScript" \
 --content "file://RunShellScript.json" \
 --document-version '$LATEST'
```

Output:

```
{
 "DocumentDescription": {
 "Status": "Updating",
 "Hash": "f775e5df4904c6fa46686c4722fae9de1950dace25cd9608ff8d622046b68d9b",
 "Name": "RunShellScript",
 "Parameters": [
 {
 "Type": "StringList",
 "Name": "commands",
 "Description": "(Required) Specify a shell script or a command to
run."
 }
],
 "DocumentType": "Command",
 "PlatformTypes": [
 "Linux"
],
 "DocumentVersion": "2",
 "HashType": "Sha256",
 "CreateDate": 1487899655.152,
 "Owner": "809632081692",
```

```
"SchemaVersion": "2.0",
"DefaultVersion": "1",
"LatestVersion": "2",
"Description": "Run an updated script"
}
}
```

- Per i dettagli sull'API, vedi [UpdateDocument](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio crea una nuova versione di un documento con il contenuto aggiornato del file json specificato. Il documento deve essere in formato JSON. È possibile ottenere la versione del documento con il cmdlet `Get-SSMDocumentVersionList` "».

```
Update-SSMDocument -Name RunShellScript -DocumentVersion "1" -Content (Get-
Content -Raw "c:\temp\RunShellScript.json")
```

### Output:

```
CreatedDate : 3/1/2017 2:59:17 AM
DefaultVersion : 1
Description : Run an updated script
DocumentType : Command
DocumentVersion : 2
Hash :
 1d5ce820e999ff051eb4841ed887593daf77120fd76cae0d18a53cc42e4e22c1
HashType : Sha256
LatestVersion : 2
Name : RunShellScript
Owner : 809632081692
Parameters : {commands}
PlatformTypes : {Linux}
SchemaVersion : 2.0
Sha1 :
Status : Updating
```

- Per i dettagli sull'API, vedere [UpdateDocument](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).



## Strumenti per V5 PowerShell

Esempio 1: questo esempio crea una nuova versione di un documento con il contenuto aggiornato del file json specificato. Il documento deve essere in formato JSON. È possibile ottenere la versione del documento con il cmdlet `Get-SSMDocumentVersionList` "».

```
Update-SSMDocument -Name RunShellScript -DocumentVersion "1" -Content (Get-Content -Raw "c:\temp\RunShellScript.json")
```

Output:

```
CreateDate : 3/1/2017 2:59:17 AM
DefaultVersion : 1
Description : Run an updated script
DocumentType : Command
DocumentVersion : 2
Hash :
 1d5ce820e999ff051eb4841ed887593daf77120fd76cae0d18a53cc42e4e22c1
HashType : Sha256
LatestVersion : 2
Name : RunShellScript
Owner : 809632081692
Parameters : {commands}
PlatformTypes : {Linux}
SchemaVersion : 2.0
Sha1 :
Status : Updating
```

- Per i dettagli sull'API, vedere [UpdateDocument](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo di **UpdateDocumentDefaultVersion** con una CLI

I seguenti esempi di codice mostrano come usare `UpdateDocumentDefaultVersion`.

## CLI

### AWS CLI

Per aggiornare la versione predefinita di un documento

L'esempio seguente `update-document-default-version` aggiorna la versione predefinita di un documento Systems Manager.

```
aws ssm update-document-default-version \
 --name "Example" \
 --document-version "2"
```

Output:

```
{
 "Description": {
 "Name": "Example",
 "DefaultVersion": "2"
 }
}
```

Per ulteriori informazioni, consulta [Scrittura del contenuto del documento SSM](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [UpdateDocumentDefaultVersion](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio aggiorna la versione predefinita di un documento. È possibile ottenere le versioni del documento disponibili con il cmdlet `Get-SSMDocumentVersionList` ».

```
Update-SSMDocumentDefaultVersion -Name "RunShellScript" -DocumentVersion "2"
```

Output:

```
DefaultVersion Name
```

```

2 RunShellScript
```

- Per i dettagli sull'API, vedere [UpdateDocumentDefaultVersion](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio aggiorna la versione predefinita di un documento. È possibile ottenere le versioni del documento disponibili con il cmdlet `Get-SSMDocumentVersionList` "».

```
Update-SSMDocumentDefaultVersion -Name "RunShellScript" -DocumentVersion "2"
```

Output:

```
DefaultVersion Name

2 RunShellScript
```

- Per i dettagli sull'API, vedere [UpdateDocumentDefaultVersion](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Usare **UpdateMaintenanceWindow** con un AWS SDK o CLI

I seguenti esempi di codice mostrano come usare `UpdateMaintenanceWindow`.

### CLI

#### AWS CLI

Esempio 1: per aggiornare una finestra di manutenzione

L'esempio seguente `update-maintenance-window` aggiorna il nome di una finestra di manutenzione.

```
aws ssm update-maintenance-window \
```

```
--window-id "mw-1a2b3c4d5e6f7g8h9" \
--name "My-Renamed-MW"
```

Output:

```
{
 "Cutoff": 1,
 "Name": "My-Renamed-MW",
 "Schedule": "cron(0 16 ? * TUE *)",
 "Enabled": true,
 "AllowUnassociatedTargets": true,
 "WindowId": "mw-1a2b3c4d5e6f7g8h9",
 "Duration": 4
}
```

Esempio 2: come disabilitare una finestra di manutenzione

L'esempio seguente `update-maintenance-window` disattiva una finestra di manutenzione.

```
aws ssm update-maintenance-window \
 --window-id "mw-1a2b3c4d5e6f7g8h9" \
 --no-enabled
```

Esempio 3: come abilitare una finestra di manutenzione

L'esempio seguente `update-maintenance-window` attiva una finestra di manutenzione.

```
aws ssm update-maintenance-window \
 --window-id "mw-1a2b3c4d5e6f7g8h9" \
 --enabled
```

Per ulteriori informazioni, vedere [Update a Maintenance Window \(AWS CLI\)](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [UpdateMaintenanceWindow](#) in AWS CLI Command Reference.

## Java

### SDK per Java 2.x

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
/**
 * Updates an SSM maintenance window asynchronously.
 *
 * @param id The ID of the maintenance window to update.
 * @param name The new name for the maintenance window.
 * <p>
 * This method initiates an asynchronous request to update an SSM maintenance
 window.
 * If the request is successful, it prints a success message.
 * If an exception occurs, it handles the error appropriately.
 */
public void updateSSMMaintenanceWindow(String id, String name) throws
SsmException {
 UpdateMaintenanceWindowRequest updateRequest =
UpdateMaintenanceWindowRequest.builder()
 .windowId(id)
 .allowUnassociatedTargets(true)
 .duration(24)
 .enabled(true)
 .name(name)
 .schedule("cron(0 0 ? * MON *)")
 .build();

 CompletableFuture<UpdateMaintenanceWindowResponse> future =
getAsyncClient().updateMaintenanceWindow(updateRequest);
 future.whenComplete((response, ex) -> {
 if (response != null) {
 System.out.println("The SSM maintenance window was successfully
updated");
 } else {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
```

```

 if (cause instanceof SsmException) {
 throw new CompletionException(cause);
 } else {
 throw new RuntimeException(cause);
 }
 }
}).join();
}

```

- Per i dettagli sulle API, consulta la [UpdateMaintenanceWindow](#) sezione AWS SDK for Java 2.x API Reference.

## JavaScript

### SDK per JavaScript (v3)

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```

import { UpdateMaintenanceWindowCommand, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Update an SSM maintenance window.
 * @param {{ windowId: string, allowUnassociatedTargets?: boolean, duration?:
 * number, enabled?: boolean, name?: string, schedule?: string }}
 */
export const main = async ({
 windowId,
 allowUnassociatedTargets = undefined, //Allow the maintenance window to run on
 managed nodes, even if you haven't registered those nodes as targets.
 duration = undefined, //The duration of the maintenance window in hours.
 enabled = undefined,
 name = undefined,
 schedule = undefined, //The schedule of the maintenance window in the form of a
 cron or rate expression.
}) => {

```

```
const client = new SSMClient({});
try {
 const { opsItemArn, opsItemId } = await client.send(
 new UpdateMaintenanceWindowCommand({
 WindowId: windowId,
 AllowUnassociatedTargets: allowUnassociatedTargets,
 Duration: duration,
 Enabled: enabled,
 Name: name,
 Schedule: schedule,
 }),
);
 console.log("Maintenance window updated.");
 return { OpsItemArn: opsItemArn, OpsItemId: opsItemId };
} catch (caught) {
 if (caught instanceof Error && caught.name === "ValidationError") {
 console.warn(`${caught.message}. Are these values correct?`);
 } else {
 throw caught;
 }
}
};
```

- Per i dettagli sulle API, consulta la [UpdateMaintenanceWindow](#) sezione AWS SDK per JavaScript API Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio aggiorna il nome di una finestra di manutenzione.

```
Update-SSMMaintenanceWindow -WindowId "mw-03eb9db42890fb82d" -Name "My-Renamed-MW"
```

Output:

```
AllowUnassociatedTargets : False
Cutoff : 1
Duration : 2
Enabled : True
```

```
Name : My-Renamed-MW
Schedule : cron(0 */30 * * * ? *)
WindowId : mw-03eb9db42890fb82d
```

Esempio 2: questo esempio abilita una finestra di manutenzione.

```
Update-SSMMaintenanceWindow -WindowId "mw-03eb9db42890fb82d" -Enabled $true
```

Output:

```
AllowUnassociatedTargets : False
Cutoff : 1
Duration : 2
Enabled : True
Name : My-Renamed-MW
Schedule : cron(0 */30 * * * ? *)
WindowId : mw-03eb9db42890fb82d
```

Esempio 3: questo esempio disabilita una finestra di manutenzione.

```
Update-SSMMaintenanceWindow -WindowId "mw-03eb9db42890fb82d" -Enabled $false
```

Output:

```
AllowUnassociatedTargets : False
Cutoff : 1
Duration : 2
Enabled : False
Name : My-Renamed-MW
Schedule : cron(0 */30 * * * ? *)
WindowId : mw-03eb9db42890fb82d
```

- Per i dettagli sull'API, vedere [UpdateMaintenanceWindow](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

## Strumenti per V5 PowerShell

Esempio 1: questo esempio aggiorna il nome di una finestra di manutenzione.

```
Update-SSMMaintenanceWindow -WindowId "mw-03eb9db42890fb82d" -Name "My-Renamed-MW"
```



**Output:**

```
AllowUnassociatedTargets : False
Cutoff : 1
Duration : 2
Enabled : True
Name : My-Renamed-MW
Schedule : cron(0 */30 * * * ? *)
WindowId : mw-03eb9db42890fb82d
```

Esempio 2: questo esempio abilita una finestra di manutenzione.

```
Update-SSMMaintenanceWindow -WindowId "mw-03eb9db42890fb82d" -Enabled $true
```

**Output:**

```
AllowUnassociatedTargets : False
Cutoff : 1
Duration : 2
Enabled : True
Name : My-Renamed-MW
Schedule : cron(0 */30 * * * ? *)
WindowId : mw-03eb9db42890fb82d
```

Esempio 3: questo esempio disabilita una finestra di manutenzione.

```
Update-SSMMaintenanceWindow -WindowId "mw-03eb9db42890fb82d" -Enabled $false
```

**Output:**

```
AllowUnassociatedTargets : False
Cutoff : 1
Duration : 2
Enabled : False
Name : My-Renamed-MW
Schedule : cron(0 */30 * * * ? *)
WindowId : mw-03eb9db42890fb82d
```

- Per i dettagli sull'API, vedere [UpdateMaintenanceWindow](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
class MaintenanceWindowWrapper:
 """Encapsulates AWS Systems Manager maintenance window actions."""

 def __init__(self, ssm_client):
 """
 :param ssm_client: A Boto3 Systems Manager client.
 """
 self.ssm_client = ssm_client
 self.window_id = None
 self.name = None

 @classmethod
 def from_client(cls):
 ssm_client = boto3.client("ssm")
 return cls(ssm_client)

 def update(
 self, name, enabled, schedule, duration, cutoff,
 allow_unassociated_targets
):
 """
 Update an AWS Systems Manager maintenance window.

 :param name: The name of the maintenance window.
 :param enabled: Whether the maintenance window is enabled to run on
 managed nodes.
 :param schedule: The schedule of the maintenance window.
 :param duration: The duration of the maintenance window.
 :param cutoff: The cutoff time of the maintenance window.
 :param allow_unassociated_targets: Allow the maintenance window to run on
 managed nodes, even
```

```

 if you haven't registered those nodes
as targets.
 """
 try:
 self.ssm_client.update_maintenance_window(
 WindowId=self.window_id,
 Name=name,
 Enabled=enabled,
 Schedule=schedule,
 Duration=duration,
 Cutoff=cutoff,
 AllowUnassociatedTargets=allow_unassociated_targets,
)
 self.name = name
 logger.info("Updated maintenance window %s.", self.window_id)
 except ParamValidationError as error:
 logger.error(
 "Parameter validation error when trying to update maintenance
window %s. Here's why: %s",
 self.window_id,
 error,
)
 raise
 except ClientError as err:
 logger.error(
 "Couldn't update maintenance window %s. Here's why: %s: %s",
 self.name,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise

```

- Per i dettagli sulle API, vedi [UpdateMaintenanceWindow](#) in AWS SDK for Python (Boto3) API Reference.

## SAP ABAP

### SDK per SAP ABAP

#### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
TRY.
 lo_ssm->updatemaintenancewindow(
 iv_windowid = iv_window_id
 iv_name = iv_name
 iv_enabled = iv_enabled
 iv_schedule = iv_schedule
 iv_duration = iv_duration
 iv_cutoff = iv_cutoff
 iv_allowunassociatedtargets = iv_allow_unassociated_targets).
 MESSAGE 'Maintenance window updated.' TYPE 'I'.
CATCH /aws1/cx_ssmdoesnotexistex.
 MESSAGE 'Maintenance window does not exist.' TYPE 'I'.
ENDTRY.
```

- Per i dettagli sulle API, consulta [UpdateMaintenanceWindow](#) la sezione AWS SDK for SAP ABAP API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

### Utilizzo di **UpdateManagedInstanceRole** con una CLI

I seguenti esempi di codice mostrano come usare `UpdateManagedInstanceRole`.

#### CLI

##### AWS CLI

Per aggiornare il ruolo IAM di un'istanza gestita

L'esempio seguente `update-managed-instance-role` aggiorna il profilo dell'istanza IAM di un'istanza gestita.

```
aws ssm update-managed-instance-role \
 --instance-id "mi-08ab247cdfEXAMPLE" \
 --iam-role "ExampleRole"
```

Questo comando non produce alcun output.

Per ulteriori informazioni, consulta [Passaggio 4: creazione di un profilo dell'istanza IAM per Systems Manager](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedi [UpdateManagedInstanceRole](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio aggiorna il ruolo di un'istanza gestita. Se il comando va a buon fine, non viene generato output.

```
Update-SSMManagedInstanceRole -InstanceId "mi-08ab247cdf1046573" -IamRole
 "AutomationRole"
```

- Per i dettagli sull'API, vedere [UpdateManagedInstanceRole](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio aggiorna il ruolo di un'istanza gestita. Se il comando va a buon fine, non viene generato output.

```
Update-SSMManagedInstanceRole -InstanceId "mi-08ab247cdf1046573" -IamRole
 "AutomationRole"
```

- Per i dettagli sull'API, vedere [UpdateManagedInstanceRole](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Usare **UpdateOpsItem** con un AWS SDK o CLI

I seguenti esempi di codice mostrano come usare `UpdateOpsItem`.

Gli esempi di operazioni sono estratti di codice da programmi più grandi e devono essere eseguiti nel contesto. È possibile visualizzare questa operazione nel contesto nel seguente esempio di codice:

- [Informazioni di base](#)

### CLI

#### AWS CLI

Per aggiornare un OpsItem

L'update-ops-item esempio seguente aggiorna la descrizione, la priorità e la categoria di un OpsItem. Inoltre, il comando specifica un argomento SNS a cui vengono inviate le notifiche quando questo OpsItem viene modificato o cambiato.

```
aws ssm update-ops-item \
 --ops-item-id "oi-287b5EXAMPLE" \
 --description "Primary OpsItem for failover event 2020-01-01-fh398yf" \
 --priority 2 \
 --category "Security" \
 --notifications "Arn=arn:aws:sns:us-east-2:111222333444:my-us-east-2-topic"
```

Output:

This command produces no output.

Per ulteriori informazioni, vedere [Lavorare con OpsItems](#) nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [UpdateOpsItem](#) in AWS CLI Command Reference.

## Java

### SDK per Java 2.x

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
/**
 * Resolves an AWS SSM OpsItem asynchronously.
 *
 * @param opsID The ID of the OpsItem to resolve.
 * <p>
 * This method initiates an asynchronous request to resolve an SSM OpsItem.
 * If an exception occurs, it handles the error appropriately.
 */
public void resolveOpsItem(String opsID) {
 UpdateOpsItemRequest opsItemRequest = UpdateOpsItemRequest.builder()
 .opsItemId(opsID)
 .status(OpsItemStatus.RESOLVED)
 .build();

 CompletableFuture<Void> future = CompletableFuture.runAsync(() -> {
 getAsyncClient().updateOpsItem(opsItemRequest)
 .thenAccept(response -> {
 System.out.println("OpsItem resolved successfully.");
 })
 .exceptionally(ex -> {
 throw new CompletionException(ex);
 }).join();
 }).exceptionally(ex -> {
 Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
 if (cause instanceof SsmException) {
 throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
 } else {
 throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
 }
 })
}
```

```
});

try {
 future.join();
} catch (CompletionException ex) {
 throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
ex.getCause() : ex;
}
}
```

- Per i dettagli sulle API, consulta la [UpdateOpsItem](#) sezione AWS SDK for Java 2.x API Reference.

## JavaScript

### SDK per JavaScript (v3)

#### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
import { UpdateOpsItemCommand, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Update an SSM OpsItem.
 * @param {{ opsItemId: string, status?: OpsItemStatus }}
 */
export const main = async ({
 opsItemId,
 status = undefined, // The OpsItem status. Status can be Open, In Progress, or Resolved
}) => {
 const client = new SSMClient({});
 try {
 await client.send(
 new UpdateOpsItemCommand({
 OpsItemId: opsItemId,
```



```

 Status: status,
)),
);
 console.log("Ops item updated.");
 return { Success: true };
} catch (caught) {
 if (
 caught instanceof Error &&
 caught.name === "OpsItemLimitExceededException"
) {
 console.warn(
 `Couldn't create ops item because you have exceeded your open OpsItem
 limit. ${caught.message}.`,
);
 } else {
 throw caught;
 }
}
};

```

- Per i dettagli sulle API, consulta la [UpdateOpsItem](#) sezione AWS SDK per JavaScript API Reference.

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```

class OpsItemWrapper:
 """Encapsulates AWS Systems Manager OpsItem actions."""

 def __init__(self, ssm_client):
 """
 :param ssm_client: A Boto3 Systems Manager client.
 """

```

```

 self.ssm_client = ssm_client
 self.id = None

 @classmethod
 def from_client(cls):
 """
 :return: A OpsItemWrapper instance.
 """
 ssm_client = boto3.client("ssm")
 return cls(ssm_client)

 def update(self, title=None, description=None, status=None):
 """
 Update an OpsItem.

 :param title: The new OpsItem title.
 :param description: The new OpsItem description.
 :param status: The new OpsItem status.
 :return:
 """
 args = dict(OpsItemId=self.id)
 if title is not None:
 args["Title"] = title
 if description is not None:
 args["Description"] = description
 if status is not None:
 args["Status"] = status
 try:
 self.ssm_client.update_ops_item(**args)
 except ClientError as err:
 logger.error(
 "Couldn't update ops item %s. Here's why: %s: %s",
 self.id,
 err.response["Error"]["Code"],
 err.response["Error"]["Message"],
)
 raise

```

- Per i dettagli sulle API, vedi [UpdateOpsItem](#) in AWS SDK for Python (Boto3) API Reference.

## SAP ABAP

### SDK per SAP ABAP

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [repository di esempi di codice AWS](#).

```
TRY.
 lo_ssm->updateopsitem(
 iv_opsitemid = iv_ops_item_id
 iv_title = iv_title
 iv_description = iv_description
 iv_status = iv_status).
 MESSAGE 'OpsItem updated.' TYPE 'I'.
CATCH /aws1/cx_ssmopsitemnotfoundex.
 MESSAGE 'OpsItem not found.' TYPE 'I'.
CATCH /aws1/cx_ssmopsiteminvparamex.
 MESSAGE 'Invalid OpsItem parameter.' TYPE 'I'.
ENDTRY.
```

- Per i dettagli sulle API, consulta [UpdateOpsItem](#) la sezione AWS SDK for SAP ABAP API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

### Utilizzo di **UpdatePatchBaseline** con una CLI

I seguenti esempi di codice mostrano come usareUpdatePatchBaseline.

#### CLI

##### AWS CLI

Esempio 1: per aggiornare una baseline delle patch

L'esempio seguente `update-patch-baseline` aggiunge le due patch specificate come rifiutate e una patch approvata alla baseline delle patch specificata.

```
aws ssm update-patch-baseline \
 --baseline-id "pb-0123456789abcdef0" \
 --rejected-patches "KB2032276" "MS10-048" \
 --approved-patches "KB2124261"
```

Output:

```
{
 "BaselineId": "pb-0123456789abcdef0",
 "Name": "WindowsPatching",
 "OperatingSystem": "WINDOWS",
 "GlobalFilters": {
 "PatchFilters": []
 },
 "ApprovalRules": {
 "PatchRules": [
 {
 "PatchFilterGroup": {
 "PatchFilters": [
 {
 "Key": "PRODUCT",
 "Values": [
 "WindowsServer2016"
]
 }
]
 },
 "ComplianceLevel": "CRITICAL",
 "ApproveAfterDays": 0,
 "EnableNonSecurity": false
 }
]
 },
 "ApprovedPatches": [
 "KB2124261"
],
 "ApprovedPatchesComplianceLevel": "UNSPECIFIED",
 "ApprovedPatchesEnableNonSecurity": false,
 "RejectedPatches": [
 "KB2032276",
```

```

 "MS10-048"
],
 "RejectedPatchesAction": "ALLOW_AS_DEPENDENCY",
 "CreateDate": 1550244180.465,
 "ModifiedDate": 1550244180.465,
 "Description": "Patches for Windows Servers",
 "Sources": []
}

```

Esempio 2: come rinominare una baseline delle patch

L'esempio seguente `update-patch-baseline` rinomina la linea di baseline delle patch.

```

aws ssm update-patch-baseline \
 --baseline-id "pb-0713accee01234567" \
 --name "Windows-Server-2012-R2-Important-and-Critical-Security-Updates"

```

Per ulteriori informazioni, vedere `Update or Delete a Patch Baseline` < <https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-baseline-update-or-delete.html> > nella Guida per l'utente di AWS Systems Manager.

- Per i dettagli sull'API, vedere [UpdatePatchBaseline](#) in AWS CLI Command Reference.

## PowerShell

### Strumenti per PowerShell V4

Esempio 1: questo esempio aggiunge due patch come rifiutate e una patch approvata a una baseline delle patch esistente.

```

Update-SSMPatchBaseline -BaselineId "pb-03da896ca3b68b639" -RejectedPatch
 "KB2032276", "MS10-048" -ApprovedPatch "KB2124261"

```

Output:

```

ApprovalRules : Amazon.SimpleSystemsManagement.Model.PatchRuleGroup
ApprovedPatches : {KB2124261}
BaselineId : pb-03da896ca3b68b639
CreateDate : 3/3/2017 5:02:19 PM
Description : Baseline containing all updates approved for production systems
GlobalFilters : Amazon.SimpleSystemsManagement.Model.PatchFilterGroup
ModifiedDate : 3/3/2017 5:22:10 PM

```

```
Name : Production-Baseline
RejectedPatches : {KB2032276, MS10-048}
```

- Per i dettagli sull'API, vedere [UpdatePatchBaseline](#) in AWS Strumenti per PowerShell Cmdlet Reference (V4).

### Strumenti per V5 PowerShell

Esempio 1: questo esempio aggiunge due patch come rifiutate e una patch approvata a una baseline delle patch esistente.

```
Update-SSMPatchBaseline -BaselineId "pb-03da896ca3b68b639" -RejectedPatch
"KB2032276","MS10-048" -ApprovedPatch "KB2124261"
```

### Output:

```
ApprovalRules : Amazon.SimpleSystemsManagement.Model.PatchRuleGroup
ApprovedPatches : {KB2124261}
BaselineId : pb-03da896ca3b68b639
CreatedDate : 3/3/2017 5:02:19 PM
Description : Baseline containing all updates approved for production systems
GlobalFilters : Amazon.SimpleSystemsManagement.Model.PatchFilterGroup
ModifiedDate : 3/3/2017 5:22:10 PM
Name : Production-Baseline
RejectedPatches : {KB2032276, MS10-048}
```

- Per i dettagli sull'API, vedere [UpdatePatchBaseline](#) in AWS Strumenti per PowerShell Cmdlet Reference (V5).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [L'utilizzo di questo servizio con un AWS SDK](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Scenari per l'utilizzo di Systems Manager AWS SDK

I seguenti esempi di codice mostrano come implementare scenari comuni in Systems Manager con AWS SDK. Questi scenari mostrano come eseguire attività specifiche richiamando più funzioni all'interno di Systems Manager o combinandole con altre. Servizi AWS Ogni scenario include un collegamento al codice sorgente completo, dove è possibile trovare le istruzioni su come configurare ed eseguire il codice.

Gli scenari sono relativi a un livello intermedio di esperienza per aiutarti a comprendere le azioni di servizio nel contesto.

## Esempi

- [Creazione di un servizio contenitore per istanze di macchine virtuali](#)
- [Guida introduttiva alle macchine virtuali](#)
- [Configurazione della gestione dei sistemi](#)

## Creazione di un servizio contenitore per istanze di macchine virtuali

L'esempio di codice seguente mostra come:

- Crea un cluster ECS
- Crea e monitora un servizio
- Eseguire la pulizia delle risorse

## Bash

AWS CLI con lo script Bash

### Note

C'è altro su. GitHub Trova l'esempio completo e scopri come eseguire la configurazione e l'esecuzione nel [repository dei tutorial sugli esempi di codice per gli sviluppatori](#).

```
#!/bin/bash

ECS EC2 Launch Type Tutorial Script - UPDATED VERSION
This script demonstrates creating an ECS cluster, launching a container
instance,
registering a task definition, and creating a service using the EC2 launch
type.
Updated to match the tutorial draft with nginx web server and service creation.
#
- UPDATED: Changed from sleep task to nginx web server with service
```

```

set -e # Exit on any error

Configuration
SCRIPT_NAME="ecs-ec2-tutorial"
LOG_FILE="${SCRIPT_NAME}-${date +%Y%m%d-%H%M%S}.log"
CLUSTER_NAME="tutorial-cluster-$(openssl rand -hex 4)"
TASK_FAMILY="nginx-task-$(openssl rand -hex 4)"
SERVICE_NAME="nginx-service-$(openssl rand -hex 4)"
KEY_PAIR_NAME="ecs-tutorial-key-$(openssl rand -hex 4)"
SECURITY_GROUP_NAME="ecs-tutorial-sg-$(openssl rand -hex 4)"

Tags
PROJECT_TAG="doc-smith"
TUTORIAL_TAG="ecs-ec2"

Get current AWS region dynamically
AWS_REGION=$(aws configure get region || echo "us-east-1")

Resource tracking arrays
CREATED_RESOURCES=()
CLEANUP_ORDER=()

Logging function
log() {
 echo "[$(date '+%Y-%m-%d %H:%M:%S')] $1" | tee -a "$LOG_FILE"
}

Error handling function
handle_error() {
 local exit_code=$?
 log "ERROR: Script failed with exit code $exit_code"
 log "ERROR: Last command: $BASH_COMMAND"

 echo ""
 echo "=====
 echo "ERROR OCCURRED - ATTEMPTING CLEANUP"
 echo "=====
 echo "Resources created before error:"
 for resource in "${CREATED_RESOURCES[@]"; do
 echo " - $resource"
 done

 cleanup_resources
 exit $exit_code

```



```

}

Set error trap
trap handle_error ERR

FIXED: Enhanced cleanup function with proper error handling and logging
cleanup_resources() {
 log "Starting cleanup process..."
 local cleanup_errors=0

 # Delete service first (this will stop tasks automatically)
 if [[-n "${SERVICE_ARN:-}"]]; then
 log "Updating service to desired count 0: $SERVICE_NAME"
 if ! aws ecs update-service --cluster "$CLUSTER_NAME" --service
"$SERVICE_NAME" --desired-count 0 2>>"$LOG_FILE"; then
 log "WARNING: Failed to update service desired count to 0"
 ((cleanup_errors++))
 else
 log "Waiting for service tasks to stop..."
 sleep 30 # Give time for tasks to stop
 fi

 log "Deleting service: $SERVICE_NAME"
 if ! aws ecs delete-service --cluster "$CLUSTER_NAME" --service
"$SERVICE_NAME" 2>>"$LOG_FILE"; then
 log "WARNING: Failed to delete service $SERVICE_NAME"
 ((cleanup_errors++))
 fi
 fi

 # Stop and delete any remaining tasks
 if [[-n "${TASK_ARN:-}"]]; then
 log "Stopping task: $TASK_ARN"
 if ! aws ecs stop-task --cluster "$CLUSTER_NAME" --task "$TASK_ARN" --
reason "Tutorial cleanup" 2>>"$LOG_FILE"; then
 log "WARNING: Failed to stop task $TASK_ARN"
 ((cleanup_errors++))
 else
 log "Waiting for task to stop..."
 if ! aws ecs wait tasks-stopped --cluster "$CLUSTER_NAME" --tasks
"$TASK_ARN" 2>>"$LOG_FILE"; then
 log "WARNING: Task stop wait failed for $TASK_ARN"
 ((cleanup_errors++))
 fi
 fi
 fi
}

```

```

 fi
 fi

 # Deregister task definition
 if [[-n "${TASK_DEFINITION_ARN:-}"]]; then
 log "Deregistering task definition: $TASK_DEFINITION_ARN"
 if ! aws ecs deregister-task-definition --task-definition
"$TASK_DEFINITION_ARN" 2>>"$LOG_FILE"; then
 log "WARNING: Failed to deregister task definition
$TASK_DEFINITION_ARN"
 ((cleanup_errors++))
 fi
 fi

 # Terminate EC2 instance
 if [[-n "${INSTANCE_ID:-}"]]; then
 log "Terminating EC2 instance: $INSTANCE_ID"
 if ! aws ec2 terminate-instances --instance-ids "$INSTANCE_ID"
2>>"$LOG_FILE"; then
 log "WARNING: Failed to terminate instance $INSTANCE_ID"
 ((cleanup_errors++))
 else
 log "Waiting for instance to terminate..."
 if ! aws ec2 wait instance-terminated --instance-ids "$INSTANCE_ID"
2>>"$LOG_FILE"; then
 log "WARNING: Instance termination wait failed for $INSTANCE_ID"
 ((cleanup_errors++))
 fi
 fi
 fi

 # Delete security group with retry logic
 if [[-n "${SECURITY_GROUP_ID:-}"]]; then
 log "Deleting security group: $SECURITY_GROUP_ID"
 local retry_count=0
 local max_retries=3

 while [[$retry_count -lt $max_retries]]; do
 if aws ec2 delete-security-group --group-id "$SECURITY_GROUP_ID"
2>>"$LOG_FILE"; then
 log "Successfully deleted security group"
 break
 else
 ((retry_count++))
 fi
 done
 fi

```

```

 if [[$retry_count -lt $max_retries]]; then
 log "Retry $retry_count/$max_retries: Waiting 10 seconds
before retrying security group deletion..."
 sleep 10
 else
 log "ERROR: Failed to delete security group after
$max_retries attempts"
 ((cleanup_errors++))
 fi
 fi
done
fi

Delete key pair
if [[-n "${KEY_PAIR_NAME:-}"]]; then
 log "Deleting key pair: $KEY_PAIR_NAME"
 if ! aws ec2 delete-key-pair --key-name "$KEY_PAIR_NAME" 2>>"$LOG_FILE";
then
 log "WARNING: Failed to delete key pair $KEY_PAIR_NAME"
 ((cleanup_errors++))
 fi
 rm -f "${KEY_PAIR_NAME}.pem" 2>>"$LOG_FILE" || log "WARNING: Failed to
remove local key file"
fi

Delete ECS cluster
if [[-n "${CLUSTER_NAME:-}"]]; then
 log "Deleting ECS cluster: $CLUSTER_NAME"
 if ! aws ecs delete-cluster --cluster "$CLUSTER_NAME" 2>>"$LOG_FILE";
then
 log "WARNING: Failed to delete cluster $CLUSTER_NAME"
 ((cleanup_errors++))
 fi
fi

if [[$cleanup_errors -eq 0]]; then
 log "Cleanup completed successfully"
else
 log "Cleanup completed with $cleanup_errors warnings/errors. Check log
file for details."
fi
}

Function to check prerequisites

```

```
check_prerequisites() {
 log "Checking prerequisites..."

 # Check AWS CLI
 if ! command -v aws &> /dev/null; then
 log "ERROR: AWS CLI is not installed"
 exit 1
 fi

 # Check AWS credentials
 if ! aws sts get-caller-identity &> /dev/null; then
 log "ERROR: AWS credentials not configured"
 exit 1
 fi

 # Get caller identity
 CALLER_IDENTITY=$(aws sts get-caller-identity --output text --query
'Account')
 log "AWS Account: $CALLER_IDENTITY"
 log "AWS Region: $AWS_REGION"

 # Check for default VPC
 DEFAULT_VPC=$(aws ec2 describe-vpcs --filters "Name=is-default,Values=true"
--query 'Vpcs[0].VpcId' --output text)
 if [["$DEFAULT_VPC" == "None"]]; then
 log "ERROR: No default VPC found. Please create a VPC first."
 exit 1
 fi
 log "Using default VPC: $DEFAULT_VPC"

 # Get default subnet
 DEFAULT_SUBNET=$(aws ec2 describe-subnets --filters "Name=vpc-id,Values=
$DEFAULT_VPC" "Name=default-for-az,Values=true" --query 'Subnets[0].SubnetId' --
output text)
 if [["$DEFAULT_SUBNET" == "None"]]; then
 log "ERROR: No default subnet found"
 exit 1
 fi
 log "Using default subnet: $DEFAULT_SUBNET"

 log "Prerequisites check completed successfully"
}

Function to create ECS cluster
```

```

create_cluster() {
 log "Creating ECS cluster: $CLUSTER_NAME"

 CLUSTER_ARN=$(aws ecs create-cluster --cluster-name "$CLUSTER_NAME" --
tags key=project,value=$PROJECT_TAG key=tutorial,value=$TUTORIAL_TAG --query
'cluster.clusterArn' --output text)

 if [[-z "$CLUSTER_ARN"]]; then
 log "ERROR: Failed to create cluster"
 exit 1
 fi

 log "Created cluster: $CLUSTER_ARN"
 CREATED_RESOURCES+=("ECS Cluster: $CLUSTER_NAME")
}

Function to create key pair
create_key_pair() {
 log "Creating EC2 key pair: $KEY_PAIR_NAME"

 # FIXED: Set secure umask before key creation
 umask 077
 aws ec2 create-key-pair --key-name "$KEY_PAIR_NAME" --query 'KeyMaterial' --
output text > "${KEY_PAIR_NAME}.pem"
 chmod 400 "${KEY_PAIR_NAME}.pem"
 umask 022 # Reset umask

 log "Created key pair: $KEY_PAIR_NAME"
 CREATED_RESOURCES+=("EC2 Key Pair: $KEY_PAIR_NAME")

 aws ec2 create-tags --resources "$KEY_PAIR_NAME" --tags Key=project,Value=
$PROJECT_TAG Key=tutorial,Value=$TUTORIAL_TAG 2>>"$LOG_FILE" || log "WARNING:
Failed to tag key pair"
}

Function to create security group
create_security_group() {
 log "Creating security group: $SECURITY_GROUP_NAME"

 SECURITY_GROUP_ID=$(aws ec2 create-security-group \
 --group-name "$SECURITY_GROUP_NAME" \
 --description "ECS tutorial security group" \
 --vpc-id "$DEFAULT_VPC" \

```

```

 --tag-specifications "ResourceType=security-
group,Tags=[{Key=project,Value=$PROJECT_TAG},{Key=tutorial,Value=$TUTORIAL_TAG}]"
 \
 --query 'GroupId' --output text)

 if [[-z "$SECURITY_GROUP_ID"]]; then
 log "ERROR: Failed to create security group"
 exit 1
 fi

 # Add HTTP access rule for nginx web server with restricted CIDR
 # SECURITY FIX: Restrict access to specific CIDR if available, otherwise
 document the risk
 log "WARNING: Security group allows HTTP (port 80) from 0.0.0.0/0 - restrict
 this in production"
 aws ec2 authorize-security-group-ingress \
 --group-id "$SECURITY_GROUP_ID" \
 --protocol tcp \
 --port 80 \
 --cidr "0.0.0.0/0"

 log "Created security group: $SECURITY_GROUP_ID"
 log "Added HTTP access on port 80"
 CREATED_RESOURCES+=("Security Group: $SECURITY_GROUP_ID")
}

Function to get ECS optimized AMI
get_ecs_ami() {
 log "Getting ECS-optimized AMI ID..."

 ECS_AMI_ID=$(aws ssm get-parameters \
 --names /aws/service/ecs/optimized-ami/amazon-linux-2/recommended \
 --query 'Parameters[0].Value' --output text | jq -r '.image_id')

 if [[-z "$ECS_AMI_ID"]]; then
 log "ERROR: Failed to get ECS-optimized AMI ID"
 exit 1
 fi

 log "ECS-optimized AMI ID: $ECS_AMI_ID"
}

Function to create IAM role for ECS instance (if it doesn't exist)
ensure_ecs_instance_role() {

```

```
log "Checking for ecsInstanceRole..."

if ! aws iam get-role --role-name ecsInstanceRole &> /dev/null; then
 log "Creating ecsInstanceRole..."

 # Create trust policy
 cat > ecs-instance-trust-policy.json << 'EOF'
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "ec2.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
]
}
EOF

 # SECURITY FIX: Validate JSON before using
 if ! jq empty ecs-instance-trust-policy.json 2>/dev/null; then
 log "ERROR: Invalid JSON in trust policy"
 rm -f ecs-instance-trust-policy.json
 exit 1
 fi

 # Create role
 aws iam create-role \
 --role-name ecsInstanceRole \
 --assume-role-policy-document file://ecs-instance-trust-policy.json

 aws iam tag-role --role-name ecsInstanceRole --tags Key=project,Value=
$PROJECT_TAG Key=tutorial,Value=$TUTORIAL_TAG

 # Attach managed policy
 aws iam attach-role-policy \
 --role-name ecsInstanceRole \
 --policy-arn arn:aws:iam::aws:policy/service-role/
AmazonEC2ContainerServiceforEC2Role

 # Create instance profile
 aws iam create-instance-profile --instance-profile-name ecsInstanceRole
```

```

Add role to instance profile
aws iam add-role-to-instance-profile \
 --instance-profile-name ecsInstanceRole \
 --role-name ecsInstanceRole

FIXED: Enhanced wait for role to be ready
log "Waiting for IAM role to be ready..."
aws iam wait role-exists --role-name ecsInstanceRole
sleep 30 # Additional buffer for eventual consistency

rm -f ecs-instance-trust-policy.json
log "Created ecsInstanceRole"
CREATED_RESOURCES+=("IAM Role: ecsInstanceRole")
else
 log "ecsInstanceRole already exists"
fi
}

Function to launch container instance
launch_container_instance() {
 log "Launching ECS container instance..."

 # Create user data script
 cat > ecs-user-data.sh << EOF
#!/bin/bash
echo ECS_CLUSTER=$CLUSTER_NAME >> /etc/ecs/ecs.config
EOF

 # SECURITY FIX: Validate user data script before use
 if ! bash -n ecs-user-data.sh 2>/dev/null; then
 log "ERROR: Invalid user data script"
 rm -f ecs-user-data.sh
 exit 1
 fi

 INSTANCE_ID=$(aws ec2 run-instances \
 --image-id "$ECS_AMI_ID" \
 --instance-type t3.micro \
 --key-name "$KEY_PAIR_NAME" \
 --security-group-ids "$SECURITY_GROUP_ID" \
 --subnet-id "$DEFAULT_SUBNET" \
 --iam-instance-profile Name=ecsInstanceRole \
 --user-data file://ecs-user-data.sh \

```



```

--tag-specifications "ResourceType=instance,Tags=[{Key=Name,Value=ecs-
tutorial-instance},{Key=project,Value=$PROJECT_TAG},{Key=tutorial,Value=
$TUTORIAL_TAG}]" \
--monitoring Enabled=false \
--metadata-options HttpTokens=required,HttpPutResponseHopLimit=1 \
--query 'Instances[0].InstanceId' --output text)

if [[-z "$INSTANCE_ID"]]; then
 log "ERROR: Failed to launch EC2 instance"
 rm -f ecs-user-data.sh
 exit 1
fi

log "Launched EC2 instance: $INSTANCE_ID"
log "Instance metadata options: IMDSv2 enforced with hop limit 1"
CREATED_RESOURCES+=("EC2 Instance: $INSTANCE_ID")

Wait for instance to be running
log "Waiting for instance to be running..."
aws ec2 wait instance-running --instance-ids "$INSTANCE_ID"

Wait for ECS agent to register
log "Waiting for ECS agent to register with cluster..."
local max_attempts=30
local attempt=0

while [[$attempt -lt $max_attempts]]; do
 CONTAINER_INSTANCES=$(aws ecs list-container-instances --cluster
"$CLUSTER_NAME" --query 'containerInstanceArns' --output text)
 if [[-n "$CONTAINER_INSTANCES" && "$CONTAINER_INSTANCES" != "None"]];
then
 log "Container instance registered successfully"
 break
 fi

 attempt=$((attempt + 1))
 log "Waiting for container instance registration... (attempt $attempt/
$max_attempts)"
 sleep 10
done

if [[$attempt -eq $max_attempts]]; then
 log "ERROR: Container instance failed to register within expected time"
 rm -f ecs-user-data.sh

```

```
 exit 1
 fi

 rm -f ecs-user-data.sh
}

Function to register task definition
register_task_definition() {
 log "Creating task definition..."

 # Create nginx task definition JSON matching the tutorial
 cat > task-definition.json << 'EOF'
{
 "family": "TASK_FAMILY_PLACEHOLDER",
 "containerDefinitions": [
 {
 "name": "nginx",
 "image": "public.ecr.aws/docker/library/nginx:latest",
 "cpu": 256,
 "memory": 512,
 "essential": true,
 "portMappings": [
 {
 "containerPort": 80,
 "hostPort": 80,
 "protocol": "tcp"
 }
],
 "logConfiguration": {
 "logDriver": "awslogs",
 "options": {
 "awslogs-group": "/ecs/nginx-task",
 "awslogs-region": "REGION_PLACEHOLDER",
 "awslogs-stream-prefix": "ecs"
 }
 }
 }
],
 "requiresCompatibilities": ["EC2"],
 "networkMode": "bridge",
 "tags": [
 {
 "key": "project",
 "value": "PROJECT_TAG_PLACEHOLDER"
 }
]
}
```

```

 },
 {
 "key": "tutorial",
 "value": "TUTORIAL_TAG_PLACEHOLDER"
 }
]
}
EOF

Replace placeholders securely
sed -i "s|TASK_FAMILY_PLACEHOLDER|$TASK_FAMILY|g" task-definition.json
sed -i "s|REGION_PLACEHOLDER|$AWS_REGION|g" task-definition.json
sed -i "s|PROJECT_TAG_PLACEHOLDER|$PROJECT_TAG|g" task-definition.json
sed -i "s|TUTORIAL_TAG_PLACEHOLDER|$TUTORIAL_TAG|g" task-definition.json

FIXED: Validate JSON before registration
if ! jq empty task-definition.json 2>/dev/null; then
 log "ERROR: Invalid JSON in task definition"
 rm -f task-definition.json
 exit 1
fi

TASK_DEFINITION_ARN=$(aws ecs register-task-definition \
 --cli-input-json file://task-definition.json \
 --query 'taskDefinition.taskDefinitionArn' --output text)

if [[-z "$TASK_DEFINITION_ARN"]]; then
 log "ERROR: Failed to register task definition"
 rm -f task-definition.json
 exit 1
fi

log "Registered task definition: $TASK_DEFINITION_ARN"
log "Task definition includes CloudWatch Logs configuration for monitoring"
CREATED_RESOURCES+=("Task Definition: $TASK_DEFINITION_ARN")

rm -f task-definition.json
}

Function to create service
create_service() {
 log "Creating ECS service..."

 SERVICE_ARN=$(aws ecs create-service \

```

```

--cluster "$CLUSTER_NAME" \
--service-name "$SERVICE_NAME" \
--task-definition "$TASK_FAMILY" \
--desired-count 1 \
--tags key=project,value=$PROJECT_TAG key=tutorial,value=$TUTORIAL_TAG \
--query 'service.serviceArn' --output text)

if [[-z "$SERVICE_ARN"]]; then
 log "ERROR: Failed to create service"
 exit 1
fi

log "Created service: $SERVICE_ARN"
CREATED_RESOURCES+=("ECS Service: $SERVICE_NAME")

Wait for service to be stable
log "Waiting for service to be stable..."
aws ecs wait services-stable --cluster "$CLUSTER_NAME" --services
"$SERVICE_NAME"

log "Service is now stable and running"

Get the task ARN for monitoring
TASK_ARN=$(aws ecs list-tasks --cluster "$CLUSTER_NAME" --service-name
"$SERVICE_NAME" --query 'taskArns[0]' --output text)
if [[-n "$TASK_ARN" && "$TASK_ARN" != "None"]]; then
 log "Service task: $TASK_ARN"
 CREATED_RESOURCES+=("ECS Task: $TASK_ARN")
fi
}

Function to demonstrate monitoring and testing
demonstrate_monitoring() {
 log "Demonstrating monitoring capabilities..."

 # List services
 log "Listing services in cluster:"
 aws ecs list-services --cluster "$CLUSTER_NAME" --output table

 # Describe service
 log "Service details:"
 aws ecs describe-services --cluster "$CLUSTER_NAME" --
services "$SERVICE_NAME" --output table --query 'services[0].
{ServiceName:serviceName,Status:status,RunningCount:runningCount,DesiredCount:desiredCount}'

```

```

List tasks
log "Listing tasks in service:"
aws ecs list-tasks --cluster "$CLUSTER_NAME" --service-name "$SERVICE_NAME"
--output table

Describe task
if [[-n "$TASK_ARN" && "$TASK_ARN" != "None"]]; then
 log "Task details:"
 aws ecs describe-tasks --cluster "$CLUSTER_NAME"
--tasks "$TASK_ARN" --output table --query 'tasks[0].
{TaskArn:taskArn,LastStatus:lastStatus,DesiredStatus:desiredStatus,CreatedAt:createdAt}'
 fi

List container instances
log "Container instances in cluster:"
aws ecs list-container-instances --cluster "$CLUSTER_NAME" --output table

Describe container instance
CONTAINER_INSTANCE_ARN=$(aws ecs list-container-instances --cluster
"$CLUSTER_NAME" --query 'containerInstanceArns[0]' --output text)
if [[-n "$CONTAINER_INSTANCE_ARN" && "$CONTAINER_INSTANCE_ARN" != "None"]];
then
 log "Container instance details:"
 aws ecs describe-container-instances --cluster "$CLUSTER_NAME"
--container-instances "$CONTAINER_INSTANCE_ARN" --output table --query
'containerInstances[0].
{Arn:containerInstanceArn,Status:status,RunningTasks:runningTasksCount,PendingTasks:pendi
 fi

Test the nginx web server
log "Testing nginx web server..."
PUBLIC_IP=$(aws ec2 describe-instances --instance-ids "$INSTANCE_ID" --query
'Reservations[0].Instances[0].PublicIpAddress' --output text)

if [[-n "$PUBLIC_IP" && "$PUBLIC_IP" != "None"]]; then
 log "Container instance public IP: $PUBLIC_IP"
 log "Testing HTTP connection to nginx..."

Wait a moment for nginx to be fully ready
sleep 10

 if curl -s --connect-timeout 10 "http://$PUBLIC_IP" | grep -q "Welcome to
nginx"; then

```

```

 log "SUCCESS: Nginx web server is responding correctly"
 echo ""
 echo "=====
 echo "WEB SERVER TEST SUCCESSFUL"
 echo "=====
 echo "You can access your nginx web server at: http://$PUBLIC_IP"
 echo "The nginx welcome page should be visible in your browser."
 else
 log "WARNING: Nginx web server may not be fully ready yet. Try
accessing http://$PUBLIC_IP in a few minutes."
 fi
 else
 log "WARNING: Could not retrieve public IP address"
 fi
}

Main execution
main() {
 log "Starting ECS EC2 Launch Type Tutorial (UPDATED VERSION)"
 log "Log file: $LOG_FILE"
 log "Security improvements: IMDSv2 enforced, JSON validation, input
sanitization, CloudWatch Logs configured"

 check_prerequisites
 create_cluster
 create_key_pair
 create_security_group
 get_ecs_ami
 ensure_ecs_instance_role
 launch_container_instance
 register_task_definition
 create_service
 demonstrate_monitoring

 log "Tutorial completed successfully!"

 echo ""
 echo "=====
 echo "TUTORIAL COMPLETED SUCCESSFULLY"
 echo "=====
 echo "Resources created:"
 for resource in "${CREATED_RESOURCES[@]}"; do
 echo " - $resource"
 done

```

```

 echo ""
 echo "The nginx service will continue running and maintain the desired task
count."
 echo "You can monitor the service status using:"
 echo " aws ecs describe-services --cluster $CLUSTER_NAME --services
$SERVICE_NAME"
 echo ""
 if [[-n "${PUBLIC_IP:-}"]]; then
 echo "Access your web server at: http://$PUBLIC_IP"
 echo ""
 fi
 echo "=====
echo "CLEANUP CONFIRMATION"
echo "=====
log "Auto-confirming cleanup - proceeding with resource cleanup"
cleanup_resources
log "All resources have been cleaned up"
}

Run main function
main "$@"

```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella documentazione di riferimento dei comandi della AWS CLI .
  - [AddRoleToInstanceProfile](#)
  - [AttachRolePolicy](#)
  - [AuthorizeSecurityGroupIngress](#)
  - [CreateCluster](#)
  - [CreateInstanceProfile](#)
  - [CreateKeyPair](#)
  - [CreateRole](#)
  - [CreateSecurityGroup](#)
  - [CreateService](#)
  - [DeleteCluster](#)
  - [DeleteKeyPair](#)
  - [DeleteSecurityGroup](#)
  - [DeleteService](#)

- [DeregisterTaskDefinition](#)
- [DescribeContainerInstances](#)
- [DescribeInstances](#)
- [DescribeServices](#)
- [DescribeSubnets](#)
- [DescribeTasks](#)
- [DescribeVpcs](#)
- [GetCallerIdentity](#)
- [GetParameters](#)
- [GetRole](#)
- [ListContainerInstances](#)
- [ListServices](#)
- [ListTasks](#)
- [RegisterTaskDefinition](#)
- [RunInstances](#)
- [StopTask](#)
- [TerminateInstances](#)
- [UpdateService](#)
- [Aspetta \(Amazon EC2\)](#)
- [Attendi \(Amazon ECS\)](#)
- [Aspetta \(IAM\)](#)

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Guida introduttiva alle macchine virtuali

L'esempio di codice seguente mostra come:

- Creazione di una coppia di chiavi



- Arrestare e avviare un'istanza
- Verifica la persistenza di Elastic IP
- Eseguire la pulizia delle risorse

## Bash

### AWS CLI con lo script Bash

#### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri come eseguire la configurazione e l'esecuzione nel [repository dei tutorial sugli esempi di codice per gli sviluppatori](#).

```
#!/bin/bash

EC2 Basics Tutorial Script - Revised
This script demonstrates the basics of working with EC2 instances using AWS CLI
Updated to use Amazon Linux 2023 and enhanced security settings

Set up logging
LOG_FILE="ec2_tutorial_$(date +%Y%m%d_%H%M%S).log"
exec > >(tee -a "$LOG_FILE") 2>&1

Function to log messages
log() {
 echo "$(date '+%Y-%m-%d %H:%M:%S') - $1"
}

Function to handle errors
handle_error() {
 log "ERROR: $1"
 log "Cleaning up resources..."
 cleanup
 exit 1
}

Function to clean up resources
cleanup() {
 log "Resources created:"
```

```
if [-n "$ASSOCIATION_ID"]; then
 log "- Elastic IP Association: $ASSOCIATION_ID"
fi

if [-n "$ALLOCATION_ID"]; then
 log "- Elastic IP Allocation: $ALLOCATION_ID (IP: $ELASTIC_IP)"
fi

if [-n "$INSTANCE_ID"]; then
 log "- EC2 Instance: $INSTANCE_ID"
fi

if [-n "$SECURITY_GROUP_ID"]; then
 log "- Security Group: $SECURITY_GROUP_ID"
fi

if [-n "$KEY_NAME"]; then
 log "- Key Pair: $KEY_NAME (File: $KEY_FILE)"
fi

REPLY=y

if [[$REPLY =~ ^[Yy]$]]; then
 log "Starting cleanup..."

 # Track cleanup failures
 CLEANUP_FAILURES=0

 # Disassociate Elastic IP if it exists
 if [-n "$ASSOCIATION_ID"]; then
 log "Disassociating Elastic IP..."
 if ! aws ec2 disassociate-address --association-id "$ASSOCIATION_ID"; then
 log "Failed to disassociate Elastic IP"
 ((CLEANUP_FAILURES++))
 fi
 fi

 # Release Elastic IP if it exists
 if [-n "$ALLOCATION_ID"]; then
 log "Releasing Elastic IP..."
 if ! aws ec2 release-address --allocation-id "$ALLOCATION_ID"; then
 log "Failed to release Elastic IP"
 ((CLEANUP_FAILURES++))
 fi
 fi
fi
```

```
 fi
 fi

 # Terminate instance if it exists
 if [-n "$INSTANCE_ID"]; then
 log "Terminating instance $INSTANCE_ID..."
 if ! aws ec2 terminate-instances --instance-ids "$INSTANCE_ID" > /dev/null;
 then
 log "Failed to terminate instance"
 ((CLEANUP_FAILURES++))
 else
 log "Waiting for instance to terminate..."
 if ! aws ec2 wait instance-terminated --instance-ids "$INSTANCE_ID"; then
 log "Failed while waiting for instance to terminate"
 ((CLEANUP_FAILURES++))
 fi
 fi
fi

Delete security group if it exists
if [-n "$SECURITY_GROUP_ID"]; then
 log "Deleting security group..."
 if ! aws ec2 delete-security-group --group-id "$SECURITY_GROUP_ID"; then
 log "Failed to delete security group"
 ((CLEANUP_FAILURES++))
 fi
fi

Delete key pair if it exists
if [-n "$KEY_NAME"]; then
 log "Deleting key pair..."
 if ! aws ec2 delete-key-pair --key-name "$KEY_NAME"; then
 log "Failed to delete key pair"
 ((CLEANUP_FAILURES++))
 fi
fi

Remove key file
if [-f "$KEY_FILE"]; then
 log "Removing key file..."
 if ! rm -f "$KEY_FILE"; then
 log "Failed to remove key file"
 ((CLEANUP_FAILURES++))
 fi
fi
fi
```

```
fi

Report cleanup status
if [$CLEANUP_FAILURES -eq 0]; then
 log "Cleanup completed successfully."
else
 log "WARNING: Cleanup completed with $CLEANUP_FAILURES failures. Some
resources may not have been deleted properly."
fi
else
 log "Resources were not deleted."
fi
}

Generate random identifier for resource names
RANDOM_ID=$(openssl rand -hex 4)
KEY_NAME="ec2-tutorial-key-$RANDOM_ID"
SG_NAME="ec2-tutorial-sg-$RANDOM_ID"

Create a directory for the key file
KEY_DIR=$(mktemp -d)
KEY_FILE="$KEY_DIR/$KEY_NAME.pem"

log "Starting EC2 basics tutorial script"
log "Random identifier: $RANDOM_ID"
log "Key name: $KEY_NAME"
log "Security group name: $SG_NAME"

Step 1: Create a key pair
log "Creating key pair..."
KEY_RESULT=$(aws ec2 create-key-pair --key-name "$KEY_NAME" --query 'KeyMaterial'
--output text)

if [$? -ne 0] || [-z "$KEY_RESULT"]; then
 handle_error "Failed to create key pair"
fi

echo "$KEY_RESULT" > "$KEY_FILE"
chmod 400 "$KEY_FILE"
log "Created key pair and saved to $KEY_FILE"

Step 2: Create a security group
log "Creating security group..."
SECURITY_GROUP_ID=$(aws ec2 create-security-group \
```

```
--group-name "$SG_NAME" \
--description "Security group for EC2 tutorial" \
--tag-specifications 'ResourceType=security-group,Tags=[{Key=project,Value=doc-smith},{Key=tutorial,Value=ec2-basics}]' \
--query "GroupId" \
--output text)

if [$? -ne 0] || [-z "$SECURITY_GROUP_ID"]; then
 handle_error "Failed to create security group"
fi

log "Created security group: $SECURITY_GROUP_ID"

Get current public IP address for SSH access
MY_IP=$(curl -s http://checkip.amazonaws.com)
if [$? -ne 0] || [-z "$MY_IP"]; then
 handle_error "Failed to get current IP address"
fi

log "Adding SSH ingress rule for IP $MY_IP..."
aws ec2 authorize-security-group-ingress \
 --group-id "$SECURITY_GROUP_ID" \
 --protocol tcp \
 --port 22 \
 --cidr "$MY_IP/32" > /dev/null

if [$? -ne 0]; then
 handle_error "Failed to add security group ingress rule"
fi

log "Added SSH ingress rule for IP $MY_IP"

Step 3: Find an Amazon Linux 2023 AMI (updated from AL2)
log "Finding latest Amazon Linux 2023 AMI..."
AMI_ID=$(aws ssm get-parameters-by-path \
 --path "/aws/service/ami-amazon-linux-latest" \
 --query "Parameters[?contains(Name, 'al2023-ami-kernel-default-x86_64')].Value"
 \
 --output text | head -1)

if [$? -ne 0] || [-z "$AMI_ID"]; then
 handle_error "Failed to find Amazon Linux 2023 AMI"
fi
```

```
log "Selected AMI: $AMI_ID"

Get the architecture of the AMI
log "Getting AMI architecture..."
AMI_ARCH=$(aws ec2 describe-images \
 --image-ids "$AMI_ID" \
 --query "Images[0].Architecture" \
 --output text)

if [$? -ne 0] || [-z "$AMI_ARCH"]; then
 handle_error "Failed to get AMI architecture"
fi

log "AMI architecture: $AMI_ARCH"

Find a compatible instance type
log "Finding compatible instance type..."
Directly use t2.micro for simplicity
INSTANCE_TYPE="t2.micro"
log "Using instance type: $INSTANCE_TYPE"

Step 4: Launch an EC2 instance with enhanced security
log "Launching EC2 instance with IMDSv2 and encryption enabled..."
INSTANCE_ID=$(aws ec2 run-instances \
 --image-id "$AMI_ID" \
 --instance-type "$INSTANCE_TYPE" \
 --key-name "$KEY_NAME" \
 --security-group-ids "$SECURITY_GROUP_ID" \
 --metadata-options "HttpTokens=required,HttpEndpoint=enabled" \
 --block-device-mappings "DeviceName=/dev/xvda,Ebs={Encrypted=true}" \
 --tag-specifications 'ResourceType=instance,Tags=[{Key=project,Value=doc-smith},{Key=tutorial,Value=ec2-basics}]'
 'ResourceType=volume,Tags=[{Key=project,Value=doc-smith},
{Key=tutorial,Value=ec2-basics}]' \
 --count 1 \
 --query 'Instances[0].InstanceId' \
 --output text)

if [$? -ne 0] || [-z "$INSTANCE_ID"]; then
 handle_error "Failed to launch EC2 instance"
fi

log "Launched instance $INSTANCE_ID. Waiting for it to start..."
```

```
Wait for the instance to be running
aws ec2 wait instance-running --instance-ids "$INSTANCE_ID"
if [$? -ne 0]; then
 handle_error "Failed while waiting for instance to start"
fi

Get instance details
INSTANCE_DETAILS=$(aws ec2 describe-instances \
 --instance-ids "$INSTANCE_ID" \
 --query 'Reservations[0].Instances[0].\
{ID:InstanceId,Type:InstanceType,State:State.Name,PublicIP:PublicIpAddress}' \
 --output json)

if [$? -ne 0]; then
 handle_error "Failed to get instance details"
fi

log "Instance details: $INSTANCE_DETAILS"

Get the public IP address
PUBLIC_IP=$(echo "$INSTANCE_DETAILS" | grep -oP '"PublicIP": "\K[^"]+')
if [-z "$PUBLIC_IP"]; then
 handle_error "Failed to get instance public IP"
fi

log "Instance public IP: $PUBLIC_IP"
log "To connect to your instance, run: ssh -i $KEY_FILE ec2-user@$PUBLIC_IP"

Pause to allow user to connect if desired
sleep 2

Step 6: Stop and Start the Instance
log "Stopping instance $INSTANCE_ID..."
aws ec2 stop-instances --instance-ids "$INSTANCE_ID" > /dev/null
if [$? -ne 0]; then
 handle_error "Failed to stop instance"
fi

log "Waiting for instance to stop..."
aws ec2 wait instance-stopped --instance-ids "$INSTANCE_ID"
if [$? -ne 0]; then
 handle_error "Failed while waiting for instance to stop"
fi
```

```
log "Instance stopped. Starting instance again..."
aws ec2 start-instances --instance-ids "$INSTANCE_ID" > /dev/null
if [$? -ne 0]; then
 handle_error "Failed to start instance"
fi

log "Waiting for instance to start..."
aws ec2 wait instance-running --instance-ids "$INSTANCE_ID"
if [$? -ne 0]; then
 handle_error "Failed while waiting for instance to start"
fi

Get the new public IP address
NEW_PUBLIC_IP=$(aws ec2 describe-instances \
 --instance-ids "$INSTANCE_ID" \
 --query 'Reservations[0].Instances[0].PublicIpAddress' \
 --output text)

if [$? -ne 0] || [-z "$NEW_PUBLIC_IP"]; then
 handle_error "Failed to get new public IP"
fi

log "Instance restarted with new public IP: $NEW_PUBLIC_IP"
log "To connect to your instance, run: ssh -i $KEY_FILE ec2-user@$NEW_PUBLIC_IP"

Step 7: Allocate and Associate an Elastic IP Address
log "Allocating Elastic IP address..."
ALLOCATION_RESULT=$(aws ec2 allocate-address \
 --domain vpc \
 --tag-specifications 'ResourceType=elastic-ip,Tags=[{Key=project,Value=doc-smith},{Key=tutorial,Value=ec2-basics}]' \
 --query '[PublicIp,AllocationId]' \
 --output text)

if [$? -ne 0] || [-z "$ALLOCATION_RESULT"]; then
 handle_error "Failed to allocate Elastic IP"
fi

ELASTIC_IP=$(echo "$ALLOCATION_RESULT" | awk '{print $1}')
ALLOCATION_ID=$(echo "$ALLOCATION_RESULT" | awk '{print $2}')

log "Allocated Elastic IP: $ELASTIC_IP with ID: $ALLOCATION_ID"

log "Associating Elastic IP with instance..."
```



```
ASSOCIATION_ID=$(aws ec2 associate-address \
 --instance-id "$INSTANCE_ID" \
 --allocation-id "$ALLOCATION_ID" \
 --query "AssociationId" \
 --output text)

if [$? -ne 0] || [-z "$ASSOCIATION_ID"]; then
 handle_error "Failed to associate Elastic IP"
fi

log "Associated Elastic IP with instance. Association ID: $ASSOCIATION_ID"
log "To connect to your instance using the Elastic IP, run: ssh -i $KEY_FILE ec2-
user@$ELASTIC_IP"

Pause to allow user to connect if desired
sleep 2

Step 8: Test the Elastic IP by Stopping and Starting the Instance
log "Stopping instance $INSTANCE_ID to test Elastic IP persistence..."
aws ec2 stop-instances --instance-ids "$INSTANCE_ID" > /dev/null
if [$? -ne 0]; then
 handle_error "Failed to stop instance"
fi

log "Waiting for instance to stop..."
aws ec2 wait instance-stopped --instance-ids "$INSTANCE_ID"
if [$? -ne 0]; then
 handle_error "Failed while waiting for instance to stop"
fi

log "Instance stopped. Starting instance again..."
aws ec2 start-instances --instance-ids "$INSTANCE_ID" > /dev/null
if [$? -ne 0]; then
 handle_error "Failed to start instance"
fi

log "Waiting for instance to start..."
aws ec2 wait instance-running --instance-ids "$INSTANCE_ID"
if [$? -ne 0]; then
 handle_error "Failed while waiting for instance to start"
fi

Verify the Elastic IP is still associated
CURRENT_IP=$(aws ec2 describe-instances \
```

```
--instance-ids "$INSTANCE_ID" \
--query 'Reservations[0].Instances[0].PublicIpAddress' \
--output text)

if [$? -ne 0] || [-z "$CURRENT_IP"]; then
 handle_error "Failed to get current public IP"
fi

log "Current public IP address: $CURRENT_IP"
log "Elastic IP address: $ELASTIC_IP"

if ["$CURRENT_IP" = "$ELASTIC_IP"]; then
 log "Success! The Elastic IP is still associated with your instance."
else
 log "Something went wrong. The Elastic IP is not associated with your
 instance."
fi

log "To connect to your instance, run: ssh -i $KEY_FILE ec2-user@$ELASTIC_IP"

Step 9: Clean up resources
log "Tutorial completed successfully!"
cleanup

exit 0
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella documentazione di riferimento dei comandi della AWS CLI .
  - [AllocateAddress](#)
  - [AssociateAddress](#)
  - [AuthorizeSecurityGroupIngress](#)
  - [CreateKeyPair](#)
  - [CreateSecurityGroup](#)
  - [DeleteKeyPair](#)
  - [DeleteSecurityGroup](#)
  - [DescribeImages](#)
  - [DescribeInstances](#)
  - [DisassociateAddress](#)
  - [GetParametersByPath](#)

- [ReleaseAddress](#)
- [RunInstances](#)
- [StartInstances](#)
- [StopInstances](#)
- [TerminateInstances](#)
- [Attendi](#)

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Configurazione della gestione dei sistemi

L'esempio di codice seguente mostra come:

- Crea autorizzazioni IAM per Systems Manager
- Creare un ruolo IAM per Systems Manager
- Configurare Systems Manager
- Verifica la configurazione
- Eseguire la pulizia delle risorse

### Bash

AWS CLI con lo script Bash

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri come eseguire la configurazione e l'esecuzione nel [repository dei tutorial sugli esempi di codice per gli sviluppatori](#).

```
#!/bin/bash
```

```
AWS Systems Manager Setup Script
```

```
This script sets up AWS Systems Manager for a single account and region
```

```
#
Version 17 fixes:
1. Added cloudformation.amazonaws.com to the IAM role trust policy
2. Systems Manager Quick Setup uses CloudFormation for deployments, so the role
 must trust CloudFormation service

Initialize log file
LOG_FILE="ssm_setup_$(date +%Y%m%d_%H%M%S).log"
UNIQUE_ID=$(openssl rand -hex 4)
echo "Starting AWS Systems Manager setup at $(date)" > "$LOG_FILE"

Function to log commands and their outputs with immediate terminal display
log_cmd() {
 echo "$(date): Running command: $1" | tee -a "$LOG_FILE"
 local output
 output=$(eval "$1" 2>&1)
 local status=$?
 echo "$output" | tee -a "$LOG_FILE"
 return $status
}

Function to check for errors in command output
check_error() {
 local cmd_output="$1"
 local cmd_status="$2"
 local error_msg="$3"

 if [[$cmd_status -ne 0 || "$cmd_output" =~ [Ee][Rr][Rr][Oo][Rr]]]; then
 echo "ERROR: $error_msg" | tee -a "$LOG_FILE"
 echo "Command output: $cmd_output" | tee -a "$LOG_FILE"
 cleanup_on_error
 exit 1
 fi
}

Array to track created resources for cleanup
declare -a CREATED_RESOURCES

Function to add a resource to the tracking array
track_resource() {
 local resource_type="$1"
 local resource_id="$2"
 CREATED_RESOURCES+=("$resource_type:$resource_id")
 echo "Tracked resource: $resource_type:$resource_id" | tee -a "$LOG_FILE"
```

```

}

Function to clean up resources on error
cleanup_on_error() {
 echo "" | tee -a "$LOG_FILE"
 echo "===== " | tee -a "$LOG_FILE"
 echo "ERROR OCCURRED - CLEANING UP RESOURCES" | tee -a "$LOG_FILE"
 echo "===== " | tee -a "$LOG_FILE"
 echo "The following resources were created:" | tee -a "$LOG_FILE"

 # Display resources in reverse order
 for ((i=${#CREATED_RESOURCES[@]}-1; i>=0; i--)); do
 echo "${CREATED_RESOURCES[$i]}" | tee -a "$LOG_FILE"
 done

 echo "" | tee -a "$LOG_FILE"
 echo "Attempting to clean up resources..." | tee -a "$LOG_FILE"

 # Clean up resources in reverse order
 cleanup_resources
}

Function to clean up all created resources
cleanup_resources() {
 # Process resources in reverse order (last created, first deleted)
 for ((i=${#CREATED_RESOURCES[@]}-1; i>=0; i--)); do
 IFS=':' read -r resource_type resource_id <<< "${CREATED_RESOURCES[$i]}"

 echo "Deleting $resource_type: $resource_id" | tee -a "$LOG_FILE"

 case "$resource_type" in
 "IAM_POLICY")
 # Delete the policy (detachment should have been handled when the
 role was deleted)
 log_cmd "aws iam delete-policy --policy-arn $resource_id" || true
 ;;
 "IAM_ROLE")
 # Detach all policies from the role first
 if [[-n "$POLICY_ARN"]]; then
 log_cmd "aws iam detach-role-policy --role-name $resource_id
--policy-arn $POLICY_ARN" || true
 fi

 # Delete the role

```

```

 log_cmd "aws iam delete-role --role-name $resource_id" || true
 ;;
 "SSM_CONFIG_MANAGER")
 log_cmd "aws ssm-quicksetup delete-configuration-manager --
manager-arn $resource_id" || true
 ;;
 *)
 echo "Unknown resource type: $resource_type, cannot delete
automatically" | tee -a "$LOG_FILE"
 ;;
 esac
done

echo "Cleanup completed" | tee -a "$LOG_FILE"

Clean up temporary files
rm -f ssm-onboarding-policy.json trust-policy.json ssm-config.json 2>/dev/
null || true
}

Main script execution
echo "AWS Systems Manager Setup Script"
echo "=====
echo "This script will set up AWS Systems Manager for a single account and
region."
echo "It will create IAM policies and roles, then enable Systems Manager
features."
echo ""

Get the current AWS region
CURRENT_REGION=$(aws configure get region)
if [[-z "$CURRENT_REGION"]]; then
 echo "No AWS region configured. Please specify a region:"
 CURRENT_REGION="{AWS_DEFAULT_REGION:-us-west-2}"
 if [[-z "$CURRENT_REGION"]]; then
 echo "ERROR: A region must be specified" | tee -a "$LOG_FILE"
 exit 1
 fi
fi

echo "Using AWS region: $CURRENT_REGION" | tee -a "$LOG_FILE"

Step 1: Create IAM policy for Systems Manager onboarding
echo "Step 1: Creating IAM policy for Systems Manager onboarding..."

```

```
Create policy document
cat > ssm-onboarding-policy.json << 'EOF'
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "QuickSetupActions",
 "Effect": "Allow",
 "Action": [
 "ssm-quicksetup:*"
],
 "Resource": "*"
 },
 {
 "Sid": "SsmReadOnly",
 "Effect": "Allow",
 "Action": [
 "ssm:DescribeAutomationExecutions",
 "ssm:GetAutomationExecution",
 "ssm:ListAssociations",
 "ssm:DescribeAssociation",
 "ssm:ListDocuments",
 "ssm:ListResourceDataSync",
 "ssm:DescribePatchBaselines",
 "ssm:GetPatchBaseline",
 "ssm:DescribeMaintenanceWindows",
 "ssm:DescribeMaintenanceWindowTasks"
],
 "Resource": "*"
 },
 {
 "Sid": "SsmDocument",
 "Effect": "Allow",
 "Action": [
 "ssm:GetDocument",
 "ssm:DescribeDocument"
],
 "Resource": [
 "arn:aws:ssm:*:*:document/AWSQuickSetupType-*",
 "arn:aws:ssm:*:*:document/AWS-EnableExplorer"
]
 }
]
}
```

```

 "Sid": "SsmEnableExplorer",
 "Effect": "Allow",
 "Action": "ssm:StartAutomationExecution",
 "Resource": "arn:aws:ssm:*:*:automation-definition/AWS-EnableExplorer:*"
 },
 {
 "Sid": "SsmExplorerRds",
 "Effect": "Allow",
 "Action": [
 "ssm:GetOpsSummary",
 "ssm:CreateResourceDataSync",
 "ssm:UpdateResourceDataSync"
],
 "Resource": "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*"
 },
 {
 "Sid": "OrgsReadOnly",
 "Effect": "Allow",
 "Action": [
 "organizations:DescribeAccount",
 "organizations:DescribeOrganization",
 "organizations:ListDelegatedAdministrators",
 "organizations:ListRoots",
 "organizations:ListParents",
 "organizations:ListOrganizationalUnitsForParent",
 "organizations:DescribeOrganizationalUnit",
 "organizations:ListAWSServiceAccessForOrganization"
],
 "Resource": "*"
 },
 {
 "Sid": "OrgsAdministration",
 "Effect": "Allow",
 "Action": [
 "organizations:EnableAWSServiceAccess",
 "organizations:RegisterDelegatedAdministrator",
 "organizations:DeregisterDelegatedAdministrator"
],
 "Resource": "*",
 "Condition": {
 "StringEquals": {
 "organizations:ServicePrincipal": [
 "ssm.amazonaws.com",
 "ssm-quicksetup.amazonaws.com",

```



```

 "member.org.stacksets.cloudformation.amazonaws.com",
 "resource-explorer-2.amazonaws.com"
]
}
},
{
 "Sid": "CfnReadOnly",
 "Effect": "Allow",
 "Action": [
 "cloudformation:ListStacks",
 "cloudformation:DescribeStacks",
 "cloudformation:ListStackSets",
 "cloudformation:DescribeOrganizationsAccess"
],
 "Resource": "*"
},
{
 "Sid": "OrgCfnAccess",
 "Effect": "Allow",
 "Action": [
 "cloudformation:ActivateOrganizationsAccess"
],
 "Resource": "*"
},
{
 "Sid": "CfnStackActions",
 "Effect": "Allow",
 "Action": [
 "cloudformation:CreateStack",
 "cloudformation>DeleteStack",
 "cloudformation:DescribeStackResources",
 "cloudformation:DescribeStackEvents",
 "cloudformation:GetTemplate",
 "cloudformation:RollbackStack",
 "cloudformation:TagResource",
 "cloudformation:UntagResource",
 "cloudformation:UpdateStack"
],
 "Resource": [
 "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*",
 "arn:aws:cloudformation:*:*:stack/AWS-QuickSetup-*",
 "arn:aws:cloudformation:*:*:type/resource/*"
]
}

```

```

},
{
 "Sid": "CfnStackSetActions",
 "Effect": "Allow",
 "Action": [
 "cloudformation:CreateStackInstances",
 "cloudformation:CreateStackSet",
 "cloudformation>DeleteStackInstances",
 "cloudformation>DeleteStackSet",
 "cloudformation:DescribeStackInstance",
 "cloudformation:DetectStackSetDrift",
 "cloudformation:ListStackInstanceResourceDrifts",
 "cloudformation:DescribeStackSet",
 "cloudformation:DescribeStackSetOperation",
 "cloudformation:ListStackInstances",
 "cloudformation:ListStackSetOperations",
 "cloudformation:ListStackSetOperationResults",
 "cloudformation:TagResource",
 "cloudformation:UntagResource",
 "cloudformation:UpdateStackSet"
],
 "Resource": [
 "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
 "arn:aws:cloudformation:*:*:type/resource/*",
 "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-*:*"
]
},
{
 "Sid": "ValidationReadonlyActions",
 "Effect": "Allow",
 "Action": [
 "iam:ListRoles",
 "iam:GetRole"
],
 "Resource": "*"
},
{
 "Sid": "IamRolesMgmt",
 "Effect": "Allow",
 "Action": [
 "iam:CreateRole",
 "iam>DeleteRole",
 "iam:GetRole",
 "iam:AttachRolePolicy",

```

```

 "iam:DetachRolePolicy",
 "iam:GetRolePolicy",
 "iam:ListRolePolicies"
],
 "Resource": [
 "arn:aws:iam::*:role/AWS-QuickSetup-*",
 "arn:aws:iam::*:role/service-role/AWS-QuickSetup-*"
]
},
{
 "Sid": "IamPassRole",
 "Effect": "Allow",
 "Action": [
 "iam:PassRole"
],
 "Resource": [
 "arn:aws:iam::*:role/AWS-QuickSetup-*",
 "arn:aws:iam::*:role/service-role/AWS-QuickSetup-*"
],
 "Condition": {
 "StringEquals": {
 "iam:PassedToService": [
 "ssm.amazonaws.com",
 "ssm-quicksetup.amazonaws.com",
 "cloudformation.amazonaws.com"
]
 }
 }
},
{
 "Sid": "IamRolesPoliciesMgmt",
 "Effect": "Allow",
 "Action": [
 "iam:AttachRolePolicy",
 "iam:DetachRolePolicy"
],
 "Resource": [
 "arn:aws:iam::*:role/AWS-QuickSetup-*",
 "arn:aws:iam::*:role/service-role/AWS-QuickSetup-*"
],
 "Condition": {
 "ArnEquals": {
 "iam:PolicyARN": [

```

```

 "arn:aws:iam::aws:policy/
AWSSystemsManagerEnableExplorerExecutionPolicy",
 "arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentRolePolicy"
]
}
},
{
 "Sid": "CfnStackSetsSLR",
 "Effect": "Allow",
 "Action": [
 "iam:CreateServiceLinkedRole"
],
 "Resource": [
 "arn:aws:iam::*:role/aws-service-role/
stacksets.cloudformation.amazonaws.com/
AWSServiceRoleForCloudFormationStackSetsOrgAdmin",
 "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM",
 "arn:aws:iam::*:role/aws-service-role/
accountdiscovery.ssm.amazonaws.com/AWSServiceRoleForAmazonSSM_AccountDiscovery",
 "arn:aws:iam::*:role/aws-service-role/ssm-quicksetup.amazonaws.com/
AWSServiceRoleForSSMQuickSetup",
 "arn:aws:iam::*:role/aws-service-role/resource-explorer-2.amazonaws.com/
AWSServiceRoleForResourceExplorer"
]
}
]
}
EOF

Create the IAM policy
POLICY_OUTPUT=$(log_cmd "aws iam create-policy --policy-name SSMOnboardingPolicy-
$UNIQUE_ID --policy-document file://ssm-onboarding-policy.json --output json")
POLICY_STATUS=$?
check_error "$POLICY_OUTPUT" $POLICY_STATUS "Failed to create IAM policy"

Extract the policy ARN
POLICY_ARN=$(echo "$POLICY_OUTPUT" | grep -o 'arn:aws:iam::[0-9]*:policy/
SSMOnboardingPolicy-[a-f0-9]*')
if [[-z "$POLICY_ARN"]]; then
 echo "ERROR: Failed to extract policy ARN" | tee -a "$LOG_FILE"
 exit 1
fi

```

```
Track the created policy
track_resource "IAM_POLICY" "$POLICY_ARN"
aws iam tag-policy --policy-arn "$POLICY_ARN" \
 --tags Key=project,Value=doc-smith Key=tutorial,Value=aws-systems-manager-gs

echo "Created policy: $POLICY_ARN" | tee -a "$LOG_FILE"

Step 2: Create and configure IAM role for Systems Manager
echo ""
echo "Step 2: Creating IAM role for Systems Manager..."

Get current user name
USER_OUTPUT=$(log_cmd "aws sts get-caller-identity --output json")
USER_STATUS=$?
check_error "$USER_OUTPUT" $USER_STATUS "Failed to get caller identity"

Extract account ID
ACCOUNT_ID=$(echo "$USER_OUTPUT" | grep -o '"Account": "[0-9]*"' | cut -d'"' -f4)
if [[-z "$ACCOUNT_ID"]]; then
 echo "ERROR: Failed to extract account ID" | tee -a "$LOG_FILE"
 exit 1
fi

Generate a unique role name
ROLE_NAME="SSMTutorialRole-$(openssl rand -hex 4)"

Create trust policy for the role - FIXED: Added cloudformation.amazonaws.com
cat > trust-policy.json << 'EOF'
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": [
 "ssm.amazonaws.com",
 "ssm-quicksetup.amazonaws.com",
 "cloudformation.amazonaws.com"
]
 },
 "Action": "sts:AssumeRole"
 }
],
}
```

```

 "Effect": "Allow",
 "Principal": {
 "AWS": "arn:aws:iam::ACCOUNT_ID:root"
 },
 "Action": "sts:AssumeRole"
 }
]
}
EOF

Replace ACCOUNT_ID placeholder in trust policy
sed -i "s/ACCOUNT_ID/$ACCOUNT_ID/g" trust-policy.json

Create the IAM role
ROLE_OUTPUT=$(log_cmd "aws iam create-role --role-name $ROLE_NAME --assume-role-policy-document file:///trust-policy.json --description 'Role for Systems Manager tutorial' --output json")
ROLE_STATUS=$?
check_error "$ROLE_OUTPUT" $ROLE_STATUS "Failed to create IAM role"

Extract the role ARN
ROLE_ARN=$(echo "$ROLE_OUTPUT" | grep -o 'arn:aws:iam::[0-9]*:role/[^"]*')
if [[-z "$ROLE_ARN"]]; then
 echo "ERROR: Failed to extract role ARN" | tee -a "$LOG_FILE"
 cleanup_on_error
 exit 1
fi

Track the created role
track_resource "IAM_ROLE" "$ROLE_NAME"
aws iam tag-role --role-name "$ROLE_NAME" \
 --tags Key=project,Value=doc-smith Key=tutorial,Value=aws-systems-manager-gs

echo "Created IAM role: $ROLE_NAME" | tee -a "$LOG_FILE"
echo "Role ARN: $ROLE_ARN" | tee -a "$LOG_FILE"

Set identity variables for cleanup
IDENTITY_TYPE="role"
IDENTITY_NAME="$ROLE_NAME"

Attach the policy to the role
ATTACH_OUTPUT=$(log_cmd "aws iam attach-role-policy --role-name $ROLE_NAME --policy-arn $POLICY_ARN")
ATTACH_STATUS=$?

```

```
check_error "$ATTACH_OUTPUT" $ATTACH_STATUS "Failed to attach policy to role
$ROLE_NAME"

echo "Policy attached to role: $ROLE_NAME" | tee -a "$LOG_FILE"

Step 3: Create Systems Manager configuration using Host Management
echo ""
echo "Step 3: Creating Systems Manager configuration..."

Generate a random identifier for the configuration name
CONFIG_NAME="SSMSetup-$(openssl rand -hex 4)"

Create configuration file for Systems Manager setup using Host Management
Added both required parameters for single account deployment based on
CloudFormation documentation
cat > ssm-config.json << EOF
[
 {
 "Type": "AWSQuickSetupType-SSMHostMgmt",
 "LocalDeploymentAdministrationRoleArn": "$ROLE_ARN",
 "LocalDeploymentExecutionRoleName": "$ROLE_NAME",
 "Parameters": {
 "TargetAccounts": "$ACCOUNT_ID",
 "TargetRegions": "$CURRENT_REGION"
 }
 }
]
EOF

echo "Configuration file created:" | tee -a "$LOG_FILE"
cat ssm-config.json | tee -a "$LOG_FILE"

Create the configuration manager
CONFIG_OUTPUT=$(log_cmd "aws ssm-quicksetup create-configuration-manager --name
\"$CONFIG_NAME\" --configuration-definitions file://ssm-config.json --region
$CURRENT_REGION")
CONFIG_STATUS=$?
check_error "$CONFIG_OUTPUT" $CONFIG_STATUS "Failed to create Systems Manager
configuration"

Extract the manager ARN
MANAGER_ARN=$(echo "$CONFIG_OUTPUT" | grep -o 'arn:aws:ssm-quicksetup:[^"]*')
if [[-z "$MANAGER_ARN"]]; then
 echo "ERROR: Failed to extract manager ARN" | tee -a "$LOG_FILE"
```

```

 exit 1
 fi

 # Track the created configuration manager
 track_resource "SSM_CONFIG_MANAGER" "$MANAGER_ARN"

 echo "Created Systems Manager configuration: $MANAGER_ARN" | tee -a "$LOG_FILE"

 # Step 4: Verify the setup
 echo ""
 echo "Step 4: Verifying the setup..."

 # Wait for the configuration to be fully deployed
 echo "Waiting for the configuration to be deployed (this may take a few
 minutes)..."
 sleep 30

 # Check the configuration manager status
 VERIFY_OUTPUT=$(log_cmd "aws ssm-quicksetup get-configuration-manager --manager-
 arn $MANAGER_ARN --region $CURRENT_REGION")
 VERIFY_STATUS=$?
 check_error "$VERIFY_OUTPUT" $VERIFY_STATUS "Failed to verify configuration
 manager"

 echo "Systems Manager setup completed successfully!" | tee -a "$LOG_FILE"

 # List the created resources
 echo ""
 echo "====="
 echo "CREATED RESOURCES"
 echo "====="
 for resource in "${CREATED_RESOURCES[@]+"${CREATED_RESOURCES[@]}"}"; do
 echo "$resource"
 done

 # Prompt for cleanup
 echo ""
 echo "====="
 echo "CLEANUP CONFIRMATION"
 echo "====="
 echo "Do you want to clean up all created resources? (y/n): "
 CLEANUP_CHOICE="y"

 if [["$CLEANUP_CHOICE" =~ ^[Yy]$]]; then

```



```
 echo "Cleaning up resources..." | tee -a "$LOG_FILE"
 cleanup_resources
 echo "Cleanup completed." | tee -a "$LOG_FILE"
else
 echo "Resources will not be cleaned up. You can manually clean them up
 later." | tee -a "$LOG_FILE"
fi

echo ""
echo "Script execution completed. See $LOG_FILE for details."

Clean up temporary files
rm -f ssm-onboarding-policy.json trust-policy.json ssm-config.json 2>/dev/null ||
 true
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella documentazione di riferimento dei comandi della AWS CLI .
  - [AttachRolePolicy](#)
  - [CreateConfigurationManager](#)
  - [CreatePolicy](#)
  - [CreateRole](#)
  - [DeleteConfigurationManager](#)
  - [DeletePolicy](#)
  - [DeleteRole](#)
  - [DetachRolePolicy](#)
  - [GetCallerIdentity](#)
  - [GetConfigurationManager](#)

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [L'utilizzo di questo servizio con un AWS SDK](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

# Registrazione e monitoraggio AWS Systems Manager

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle AWS Systems Manager AWS soluzioni esistenti. È necessario raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire il debug di un errore multipunto, se si verifica. Tuttavia, prima di iniziare il monitoraggio di Systems Manager, è opportuno creare un piano di monitoraggio che includa le risposte alle seguenti domande:

- Quali sono gli obiettivi del monitoraggio?
- Di quali risorse si intende eseguire il monitoraggio?
- Con quale frequenza sarà eseguito il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio verranno utilizzati?
- Chi esegue le attività di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

Dopo avere definito gli obiettivi del monitoraggio e aver creato il piano di monitoraggio, la fase successiva consiste nello stabilire una baseline per le normali prestazioni di Systems Manager nel proprio ambiente. È necessario misurare le prestazioni di Systems Manager in diversi orari e in diverse condizioni di carico. Durante il monitoraggio di Systems Manager è necessario archiviare una cronologia dei dati di monitoraggio raccolti. Puoi confrontare le prestazioni correnti di Systems Manager con questi dati storici per aiutarti a identificare i modelli di prestazioni normali e le anomalie prestazionali, oltre a creare metodi per affrontarle.

Ad esempio, è possibile monitorare l'esito positivo o l'errore di operazioni quali i flussi di lavoro di automazione, l'applicazione delle baseline delle patch, gli eventi della finestra di manutenzione e la conformità alla configurazione. L'automazione è uno strumento di AWS Systems Manager.

È inoltre possibile monitorare l'utilizzo della CPU I/O, del disco e della rete dei nodi gestiti. Quando le prestazioni non rientrano nella linea di base stabilita, potrebbe essere necessario riconfigurare o ottimizzare il nodo per ridurre l'utilizzo della CPU, migliorare il disco I/O o ridurre il traffico di rete. Per ulteriori informazioni sul monitoraggio di istanze EC2, consulta [Monitoraggio di Amazon EC2](#) nella Guida per l'utente di Amazon EC2.

## Argomenti

- [Strumenti di monitoraggio](#)

- [Invio dei log dei nodi a CloudWatch registri unificati \(CloudWatch agente\)](#)
- [Invio Agente SSM da log a CloudWatch Logs](#)
- [Monitoraggio degli eventi della richiesta di modifica](#)
- [Monitoraggio delle automazioni](#)
- [Monitoraggio delle Run Command metriche tramite Amazon CloudWatch](#)
- [Registrazione dei log AWS Systems Manager Chiamate API con AWS CloudTrail](#)
- [Uscita dell'azione Logging Automation con Logs CloudWatch](#)
- [Configurazione di Amazon CloudWatch Logs per Run Command](#)
- [Monitoraggio degli eventi di Systems Manager con Amazon EventBridge](#)
- [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#)

## Strumenti di monitoraggio

Il contenuto di questo capitolo fornisce informazioni sull'utilizzo degli strumenti disponibili per il monitoraggio del Systems Manager e di altre AWS risorse. Per un elenco più completo degli strumenti, consulta [Registrazione e monitoraggio AWS Systems Manager](#).

### Invio dei log dei nodi a CloudWatch registri unificati (CloudWatch agente)

Puoi configurare e utilizzare l' CloudWatch agente Amazon per raccogliere metriche e log dai tuoi nodi invece di usare AWS Systems Manager Agent (SSM Agent) per queste attività. L' CloudWatch agente consente di raccogliere più metriche sulle istanze EC2 di quelle disponibili utilizzando SSM Agent. Inoltre, è possibile raccogliere metriche dai server locali utilizzando l'agente CloudWatch.

È inoltre possibile memorizzare le impostazioni di configurazione dell'agente in Systems Manager Parameter Store per utilizzarle con l' CloudWatch agente. Parameter Store è uno strumento in AWS Systems Manager.

#### Note

AWS Systems Manager supporta la migrazione da SSM Agent all' CloudWatch agente unificato per la raccolta di log e metriche solo sulle versioni a 64 bit di Windows. Per informazioni sulla configurazione dell' CloudWatch agente unificato su altri sistemi operativi e

per informazioni complete sull'utilizzo CloudWatch dell'agente, consulta [Raccolta di metriche e registri da istanze Amazon EC2 e server locali con l'agente nella Amazon User Guide.](#)

[CloudWatch](#) [CloudWatch](#)

È possibile utilizzare l' CloudWatch agente su altri sistemi operativi supportati, ma non sarà possibile utilizzare Systems Manager per eseguire una migrazione degli strumenti.

SSM Agent scrive informazioni su esecuzioni, operazioni pianificate, errori e stati di integrità in file di log per ogni nodo. La connessione manuale a un nodo per visualizzare i file di log e risolvere un problema con SSM Agent è dispendiosa in termini di tempo. Per un monitoraggio più efficiente dei nodi, puoi configurare SSM Agent se stesso o l' CloudWatch agente per inviare questi dati di log ad Amazon CloudWatch Logs.

 Important

L' CloudWatch agente unificato è stato sostituito SSM Agent come strumento per l'invio dei dati di log ad Amazon CloudWatch Logs. Il plugin aws:cloudWatch SSM Agent non è supportato. Ti consigliamo di utilizzare solo l' CloudWatch agente unificato per i processi di raccolta dei log. Per ulteriori informazioni, consulta i seguenti argomenti:

- [Invio dei log dei nodi a CloudWatch registri unificati \(CloudWatch agente\)](#)
- [Esegui la migrazione della raccolta di log dei nodi di Windows Server all'agente CloudWatch](#)
- [Raccolta di metriche, log e tracce con l' CloudWatch agente](#) nella Amazon CloudWatch User Guide.

Utilizzando CloudWatch Logs, puoi monitorare i dati di log in tempo reale, cercare e filtrare i dati di log creando uno o più filtri metrici e archiviare e recuperare i dati storici quando ne hai bisogno. Per ulteriori informazioni sui CloudWatch log, consulta la [Amazon CloudWatch Logs User Guide.](#)

La configurazione di un agente per inviare dati di log ad Amazon CloudWatch Logs offre i seguenti vantaggi:

- Archiviazione centralizzata di tutti i file di log di SSM Agent.
- Accesso più rapido ai file per esaminare gli errori
- Conservazione indefinita (configurabile) dei file di log

- Log gestibili e accessibili indipendentemente dallo stato del nodo.
- Accesso ad altre CloudWatch funzionalità come metriche e allarmi.

Per informazioni sul monitoraggio delle attività di Session Manager, consulta [Attività di registrazione delle sessioni](#) e [Abilitazione e disabilitazione della registrazione di sessione](#).

## Esegui la migrazione della raccolta di log dei nodi di Windows Server all'agente CloudWatch

Se utilizzi SSM Agent Windows Server nodi supportati per inviare file di SSM Agent log ad Amazon CloudWatch Logs, puoi utilizzare Systems Manager per migrare dall' CloudWatch agente SSM Agent all'agente come strumento di raccolta dei log e migrare le impostazioni di configurazione.

L' CloudWatch agente non è supportato nelle versioni a 32 bit di Windows Server

Per le istanze EC2 a 64 bit di Windows Server, è possibile eseguire la migrazione all' CloudWatch agente automaticamente o manualmente. Per server on-premises e macchine virtuali (VM), il processo deve essere eseguito manualmente.

### Note

Durante il processo di migrazione, i dati inviati CloudWatch potrebbero essere interrotti o duplicati. I parametri e i dati di log verranno registrati di nuovo accuratamente in CloudWatch al termine della migrazione.

Consigliamo di testare la migrazione su un numero limitato di nodi prima di migrare un'intera flotta verso l'agente. CloudWatch Se dopo la migrazione si preferisce la raccolta di log con SSM Agent, è possibile tornare a utilizzarla.

### Important

Nei seguenti casi, non sarà possibile migrare all' CloudWatch agente utilizzando i passaggi descritti in questo argomento:

- La configurazione esistente per SSM Agent specifica più Regioni.
- La configurazione esistente per SSM Agent specifica più set di credenziali access/secret chiave.

In questi casi, sarà necessario disattivare la raccolta dei log SSM Agent e installare l' CloudWatch agente senza un processo di migrazione. Per ulteriori informazioni, consulta i seguenti argomenti nella Amazon CloudWatch User Guide:

- [Installazione dell' CloudWatch agente](#)
- [Installazione dell' CloudWatch agente su server locali](#)

## Prima di iniziare

Prima di iniziare una migrazione all' CloudWatch agente per la raccolta dei log, assicurati che i nodi su cui esegui la migrazione soddisfino questi requisiti:

- Il sistema operativo è una versione a 64 bit di Windows Server.
- Nel nodo è installato SSM Agent 2.2.93.0 o una versione successiva.
- SSM Agent è configurato per il monitoraggio sul nodo.

## Argomenti

- [Migrazione automatica all'agente CloudWatch](#)
- [Migrazione manuale all'agente CloudWatch](#)

## Migrazione automatica all'agente CloudWatch

Windows ServerSolo per le istanze EC2, puoi utilizzare la AWS Systems Manager console o AWS Command Line Interface (AWS CLI) per migrare automaticamente all' CloudWatch agente come strumento di raccolta dei log.

### Note

AWS Systems Manager supporta la migrazione da SSM Agent all' CloudWatch agente unificato per la raccolta di log e metriche solo sulle versioni a 64 bit di Windows. Per informazioni sulla configurazione dell' CloudWatch agente unificato su altri sistemi operativi e per informazioni complete sull'utilizzo CloudWatch dell'agente, consulta [Raccolta di metriche e registri da istanze Amazon EC2 e server locali con l'agente nella Amazon User Guide.](#)  
[CloudWatch](#) [CloudWatch](#)

È possibile utilizzare l' CloudWatch agente su altri sistemi operativi supportati, ma non sarà possibile utilizzare Systems Manager per eseguire una migrazione degli strumenti.

Una volta completata la migrazione, controlla i risultati CloudWatch per assicurarti di ricevere le metriche, i registri o i registri degli eventi di Windows previsti. Se ottieni i risultati desiderati, puoi facoltativamente [Memorizza le impostazioni di configurazione CloudWatch dell'agente in Parameter Store](#). Se la migrazione ha esito negativo o i risultati non sono quelli previsti, puoi tentare [Tornando alla raccolta dei log con Agente SSM](#).

#### Note

Se desideri eseguire la migrazione di un file di configurazione di origine contenente una voce {hostname}, tieni presente che la voce {hostname} può modificare il valore del campo al termine della migrazione. Ad esempio, supponiamo che la seguente "LogStream": "{hostname}" voce sia associata a un server denominato. MyLogServer001

```
{
 "Id": "CloudWatchIISLogs",
 "FullName":
 "AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch",
 "Parameters": {
 "AccessKey": "",
 "SecretKey": "",
 "Region": "us-east-1",
 "LogGroup": "Production-Windows-IIS",
 "LogStream": "{hostname}"
 }
}
```

Dopo la migrazione, questa voce viene mappata a un dominio, ad esempio ip-11-1-1-11.production.ExampleCompany.com. Per mantenere il nome host locale come valore, specifica {local\_hostname} anziché {hostname}.

Per migrare automaticamente all' CloudWatch agente (console)

1. Aprire la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>

2. Nel riquadro di navigazione scegliere Run Command e quindi Esegui comando.
3. Nell'elenco Documento comando, scegli AmazonCloudWatch-MigrateCloudWatchAgent.
4. In Status (Stato), scegliere Enabled (Abilitato).
5. Nella sezione Destinazioni, identifica i nodi in cui si desidera eseguire questa operazione specificando i tag, selezionando manualmente le istanze, i dispositivi edge o indicando un gruppo di risorse.

 Tip

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

6. In Controllo velocità:
  - In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti presi di mira, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.
7. (Facoltativo) Nella sezione Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Scrivi l'output del comando in un bucket S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

 Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine



attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

8. Se vuoi che vengano inviate notifiche sullo stato dell'esecuzione del comando, nella sezione Notifiche SNS selezionare la casella di controllo Abilita notifiche SNS.

Per ulteriori informazioni sulla configurazione delle notifiche Amazon SNS per Run Command, consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

9. Scegli Esegui.

Per migrare automaticamente all'agente ( CloudWatch AWS CLI)

- Eseguire il seguente comando seguente.

```
aws ssm send-command --document-name AmazonCloudWatch-MigrateCloudWatchAgent --
targets Key=instanceids,Values=ID1,ID2,ID3
```

*ID1* e *ID3* rappresentano gli ID dei nodi da aggiornare *ID2*, ad esempio I-02573CAFCFExample.

## Migrazione manuale all'agente CloudWatch

Per Windows Server i nodi locali o le istanze EC2 per Windows Server, segui questi passaggi per migrare manualmente la raccolta di log all'agente Amazon. CloudWatch

### Note

Se desideri eseguire la migrazione di un file di configurazione di origine contenente una voce {hostname}, tieni presente che la voce {hostname} può modificare il valore del campo al termine della migrazione. Ad esempio, supponiamo che la seguente "LogStream": "{hostname}" voce sia associata a un server denominato. MyLogServer001

```
{
 "Id": "CloudWatchIISLogs",
 "FullName":
 "AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch",
 "Parameters": {
 "AccessKey": "",
 "SecretKey": "",
 "Region": "us-east-1",
 "LogGroup": "Production-Windows-IIS",
 "LogStream": "{hostname}"
 }
}
```

Dopo la migrazione, questa voce viene mappata a un dominio, ad esempio ip-11-1-1-11.production.ExampleCompany.com. Per mantenere il nome host locale come valore, specifica {local\_hostname} anziché {hostname}.

Uno: installare l' CloudWatch agente (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel riquadro di navigazione scegliere Run Command e quindi Esegui comando.
3. Nell'elenco Documento comando, scegli AWS-ConfigureAWSPackage.
4. Per Action (Operazione), scegliere Install.
5. In Nome, inserisci **AmazonCloudWatchAgent**.
6. In Version (Versione), inserire **latest**, se non è già specificata per impostazione predefinita.
7. Nella sezione Destinazioni, identifica i nodi in cui si desidera eseguire questa operazione specificando i tag, selezionando manualmente le istanze, i dispositivi edge o indicando un gruppo di risorse.

 Tip

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

## 8. In Controllo velocità:

- In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

### Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti presi di mira, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.
9. (Facoltativo) Nella sezione Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Scrivi l'output del comando in un bucket S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

### Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

10. Se vuoi che vengano inviate notifiche sullo stato dell'esecuzione del comando, nella sezione Notifiche SNS selezionare la casella di controllo Abilita notifiche SNS.

Per ulteriori informazioni sulla configurazione delle notifiche Amazon SNS per Run Command, consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

## 11. Scegli Esegui.

Due: per aggiornare il formato JSON dei dati di configurazione

- Per aggiornare la formattazione JSON delle impostazioni di configurazione esistenti per l' CloudWatch agente Run Command, utilizza o accedi al nodo direttamente con una connessione RDP per eseguire i seguenti PowerShell comandi Windows sul nodo, uno alla volta.

```
cd ${Env:ProgramFiles}\\Amazon\\AmazonCloudWatchAgent
```

```
.\amazon-cloudwatch-agent-config-wizard.exe --isNonInteractiveWindowsMigration
```

*{Env:ProgramFiles}* rappresenta la posizione in cui è possibile trovare, in genere, la directory Amazon contenente l' CloudWatch agente. C:\Program Files

Tre: configurare e avviare l' CloudWatch agente (console)

- Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
- Nel riquadro di navigazione scegliere Run Command e quindi Esegui comando.
- Nell'elenco Documento comando, scegli AWS-RunPowerShellScript.
- In Commands (Comandi) inserire i due comandi seguenti.

```
cd ${Env:ProgramFiles}\\Amazon\\AmazonCloudWatchAgent
```

```
.\amazon-cloudwatch-agent-ctl.ps1 -a fetch-config -m ec2 -c file:config.json -s
```

*{Env:ProgramFiles}* rappresenta la posizione in cui è possibile trovare, in genere, la directory Amazon contenente l' CloudWatch agente C:\Program Files.

- Nella sezione Destinazioni, identifica i nodi in cui si desidera eseguire questa operazione specificando i tag, selezionando manualmente le istanze, i dispositivi edge o indicando un gruppo di risorse.

 Tip

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

## 6. In Controllo velocità:

- In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti presi di mira, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.

7. (Facoltativo) Nella sezione Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Scrivi l'output del comando in un bucket S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

 Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM

associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

8. Se vuoi che vengano inviate notifiche sullo stato dell'esecuzione del comando, nella sezione Notifiche SNS selezionare la casella di controllo Abilita notifiche SNS.

Per ulteriori informazioni sulla configurazione delle notifiche Amazon SNS per Run Command, consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

9. Scegli Esegui.

Quattro: per disattivare la raccolta dei log in Agente SSM (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel riquadro di navigazione scegliere Run Command e quindi Esegui comando.
3. Nell'elenco Documento comando, scegli AWS-ConfigureCloudWatch.
4. In Status (Stato), scegliere Enabled (Abilitato).
5. Nella sezione Destinazioni, identifica i nodi in cui si desidera eseguire questa operazione specificando i tag, selezionando manualmente le istanze, i dispositivi edge o indicando un gruppo di risorse.

 Tip

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

6. Per Status (Stato), scegli Disabled.
7. In Controllo velocità:
  - In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti presi di mira, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.
8. (Facoltativo) Nella sezione Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Scrivi l'output del comando in un bucket S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

 Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

9. Se vuoi che vengano inviate notifiche sullo stato dell'esecuzione del comando, nella sezione Notifiche SNS selezionare la casella di controllo Abilita notifiche SNS.

Per ulteriori informazioni sulla configurazione delle notifiche Amazon SNS per Run Command, consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

10. Scegli Esegui.

Dopo aver completato questi passaggi, controlla i tuoi accessi CloudWatch per verificare di ricevere le metriche, i registri o i registri degli eventi di Windows previsti. Se ottieni i risultati

desiderati, puoi facoltativamente [Memorizza le impostazioni di configurazione CloudWatch dell'agente in Parameter Store](#). Se la migrazione ha esito negativo o i risultati non sono quelli previsti, puoi [Tornando alla raccolta dei log con Agente SSM](#).

## Memorizza le impostazioni di configurazione CloudWatch dell'agente in Parameter Store

È possibile archiviare il contenuto di un file di configurazione CloudWatch dell'agente in Parameter Store. Gestendo questi dati di configurazione in un parametro, più nodi potranno ottenere le rispettive impostazioni di configurazione dal parametro e non sarà necessario creare o aggiornare manualmente i file di configurazione sui tuoi nodi. Ad esempio, è possibile Run Command utilizzarlo per scrivere il contenuto del parametro nei file di configurazione su più nodi o utilizzare State Manager uno strumento in AWS Systems Manager, per evitare la deriva della configurazione nelle impostazioni di configurazione dell' CloudWatch agente su una flotta di nodi.

Quando si esegue la procedura guidata di configurazione CloudWatch dell'agente, è possibile scegliere di lasciare che la procedura guidata salvi le impostazioni di configurazione come nuovo parametro in. Parameter Store Per informazioni sull'esecuzione della procedura guidata di configurazione CloudWatch dell'agente, consulta [Create the CloudWatch agent configuration file with the wizard](#) nella Amazon User Guide. CloudWatch

Se hai eseguito la procedura guidata ma non hai scelto l'opzione per salvare le impostazioni come parametro o hai creato il file di configurazione CloudWatch dell'agente manualmente, puoi recuperare i dati da salvare come parametro sul tuo nodo nel file seguente.

```
${Env:ProgramFiles}\Amazon\AmazonCloudWatchAgent\config.json
```

`{Env:ProgramFiles}` rappresenta la posizione in cui è possibile trovare, in genere, la directory Amazon contenente l' CloudWatch agente. C:\Program Files

È consigliabile mantenere un backup del testo JSON di questo file in una posizione diversa dal nodo stesso.

Per informazioni sulla creazione di un parametro, consulta [Creazione in corso Parameter Store parametri in Systems Manager](#).

Per ulteriori informazioni sull' CloudWatch agente, consulta [Raccolta di metriche e log da istanze Amazon EC2 e server locali con l' CloudWatch agente](#) nella Amazon User Guide. CloudWatch



## Tornando alla raccolta dei log con Agente SSM

Se desideri tornare a utilizzare SSM Agent per la raccolta di log, segui questa procedura.

Uno: per recuperare i dati di configurazione da Agente SSM

1. Nel nodo in cui si desidera tornare a raccogliere i log con SSM Agent, individuare il contenuto del file di configurazione di SSM Agent. Tale file JSON si trova in genere nel percorso seguente:

```
${Env:ProgramFiles}\\Amazon\\SSM\\Plugins\\awsCloudWatch\\
\\AWS.EC2.Windows.CloudWatch.json
```

`{Env:ProgramFiles}` rappresenta la posizione in cui è possibile trovare la Amazon directory, in genere. C:\Program Files

2. Copiare i dati in un file di testo per utilizzarli in un secondo momento.

È consigliabile archiviare un backup del testo JSON in una posizione diversa dal nodo stesso.

Due: per disinstallare l' CloudWatch agente (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel riquadro di navigazione scegliere Run Command e quindi Esegui comando.
3. Nell'elenco Documento comando, scegli AWS-ConfigureAWSPackage.
4. In Action (Operazione), scegliere Uninstall (Disinstalla).
5. In Nome, inserisci **AmazonCloudWatchAgent**.
6. Nella sezione Destinazioni, identifica i nodi in cui si desidera eseguire questa operazione specificando i tag, selezionando manualmente le istanze, i dispositivi edge o indicando un gruppo di risorse.

### Tip

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

7. In Controllo velocità:

- In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti presi di mira, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.
8. (Facoltativo) Nella sezione Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Scrivi l'output del comando in un bucket S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

 Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

9. Se vuoi che vengano inviate notifiche sullo stato dell'esecuzione del comando, nella sezione Notifiche SNS selezionare la casella di controllo Abilita notifiche SNS.

Per ulteriori informazioni sulla configurazione delle notifiche Amazon SNS per Run Command, consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

10. Scegli Esegui.

Tre: per riattivare la raccolta dei log in Agente SSM (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel riquadro di navigazione scegliere Run Command e quindi Esegui comando.
3. Nell'elenco Documento comando, scegli AWS-ConfigureCloudWatch.
4. Per Status (Stato), scegli Enabled.
5. In Properties (Proprietà), incollare il contenuto dei vecchi dati di configurazione salvati nel file di testo.
6. Nella sezione Destinazioni, identifica i nodi in cui si desidera eseguire questa operazione specificando i tag, selezionando manualmente le istanze, i dispositivi edge o indicando un gruppo di risorse.

 Tip

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

7. In Controllo velocità:

- In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti presi di mira, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.

8. (Facoltativo) Nella sezione Opzioni di output, per salvare l'output del comando in un file, seleziona la casella **Scrivi l'output del comando in un bucket S3**. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

#### Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

9. Se vuoi che vengano inviate notifiche sullo stato dell'esecuzione del comando, nella sezione **Notifiche SNS** selezionare la casella di controllo **Abilita notifiche SNS**.

Per ulteriori informazioni sulla configurazione delle notifiche Amazon SNS per Run Command, consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

10. Scegli **Esegui**.

## Invio Agente SSM da log a CloudWatch Logs

AWS Systems Manager Agent (SSM Agent) è un software Amazon che viene eseguito su istanze EC2, dispositivi edge, server locali e macchine virtuali (VM) configurati per Systems Manager. SSM Agent elabora le richieste dal servizio Systems Manager nel cloud e configura la macchina come specificato nella richiesta. Per ulteriori informazioni su SSM Agent, consultare [Lavorare con Agente SSM](#).

Inoltre, utilizzando i seguenti passaggi, puoi configurare l'invio SSM Agent di dati di log ad Amazon CloudWatch Logs.

Prima di iniziare

Crea un gruppo di log in CloudWatch Logs. Per ulteriori informazioni, consulta [Getting started with CloudWatch Logs](#) nella Amazon CloudWatch Logs User Guide.

Per configurare Agente SSM a cui inviare registri a CloudWatch

1. Accedi a un nodo e individua il seguente file:

Linux

Sulla maggior parte dei tipi di nodi Linux: `/etc/amazon/ssm/seelog.xml.template`.

Il Ubuntu Server 20.04 e il 18.04 LTS: `/snap/amazon-ssm-agent/current/seelog.xml.template`

macOS

`/opt/aws/ssm/seelog.xml.template`

Windows

`%ProgramFiles%\Amazon\SSM\seelog.xml.template`

2. Modificare il nome del file da `seelog.xml.template` a `seelog.xml`.

 Note

Il Ubuntu Server 20.04 e il 18.04 LTS, il file `seelog.xml` deve essere creato nella directory. `/etc/amazon/ssm/` È possibile creare questa directory e il file eseguendo i seguenti comandi.

```
sudo mkdir -p /etc/amazon/ssm
```

```
sudo cp -pr /snap/amazon-ssm-agent/current/* /etc/amazon/ssm
```

```
sudo cp -p /etc/amazon/ssm/seelog.xml.template /etc/amazon/ssm/seelog.xml
```

3. Aprire il file `seelog.xml` in un editor di testo e individuare la sezione seguente.

## Linux and macOS

```
<outputs formatid="fmtinfo">
 <console formatid="fmtinfo"/>
 <rollingfile type="size" filename="/var/log/amazon/ssm/amazon-ssm-agent.log"
maxsize="300000000" maxrolls="5"/>
 <filter levels="error,critical" formatid="fmterror">
 <rollingfile type="size" filename="/var/log/amazon/ssm/errors.log"
maxsize="100000000" maxrolls="5"/>
 </filter>
</outputs>
```

## Windows

```
<outputs formatid="fmtinfo">
 <console formatid="fmtinfo"/>
 <rollingfile type="size" maxrolls="5" maxsize="300000000"
filename="{{LOCALAPPDATA}}\Amazon\SSM\Logs\amazon-ssm-agent.log"/>
 <filter formatid="fmterror" levels="error,critical">
 <rollingfile type="size" maxrolls="5" maxsize="100000000"
filename="{{LOCALAPPDATA}}\Amazon\SSM\Logs\errors.log"/>
 </filter>
</outputs>
```

4. Modificare il file e aggiungere un elemento nome personalizzato dopo il tag `</filter>` di chiusura. Nell'esempio seguente, il nome personalizzato è stato specificato come `cloudwatch_receiver`.

## Linux and macOS

```
<outputs formatid="fmtinfo">
 <console formatid="fmtinfo"/>
 <rollingfile type="size" filename="/var/log/amazon/ssm/amazon-ssm-agent.log"
maxsize="300000000" maxrolls="5"/>
 <filter levels="error,critical" formatid="fmterror">
 <rollingfile type="size" filename="/var/log/amazon/ssm/errors.log"
maxsize="100000000" maxrolls="5"/>
 </filter>
 <custom name="cloudwatch_receiver" formatid="fmtdebug" data-log-group="your-
CloudWatch-log-group-name"/>
</outputs>
```

## Windows

```
<outputs formatid="fmtinfo">
 <console formatid="fmtinfo"/>
 <rollingfile type="size" maxrolls="5" maxsize="30000000"
filename="{{LOCALAPPDATA}}\Amazon\SSM\Logs\amazon-ssm-agent.log"/>
 <filter formatid="fmterror" levels="error,critical">
 <rollingfile type="size" maxrolls="5" maxsize="10000000"
filename="{{LOCALAPPDATA}}\Amazon\SSM\Logs\errors.log"/>
 </filter>
 <custom name="cloudwatch_receiver" formatid="fmtdebug" data-log-group="your-CloudWatch-log-group-name"/>
</outputs>
```

5. Salvare le modifiche, quindi riavviare SSM Agent o il nodo.
6. Apri la console all' CloudWatch indirizzo. <https://console.aws.amazon.com/cloudwatch/>
7. Nel riquadro di navigazione, scegliere Log groups (Gruppi di log), quindi selezionare il nome del gruppo di log.

### Tip

Il flusso di log per i dati dei file di log di SSM Agent è organizzato per ID nodo.

## Monitoraggio degli eventi della richiesta di modifica

### Change Manager modifica della disponibilità

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

Dopo aver attivato l'integrazione con AWS CloudTrail Lake e aver creato un archivio dati per eventi, puoi visualizzare dettagli verificabili sulle richieste di modifica eseguite nel tuo account o nella tua organizzazione. I dettagli includono le informazioni seguenti:

- L'identità dell'utente che ha avviato la richiesta di modifica
- Il Regione AWS luogo in cui sono state apportate le modifiche
- L'indirizzo IP di origine della richiesta
- La chiave di AWS accesso utilizzata per la richiesta
- Le operazioni API eseguite per la richiesta di modifica
- I parametri di richiesta inclusi per tali operazioni
- Le risorse aggiornate durante il processo

Di seguito sono riportati alcuni esempi dei dettagli degli eventi che è possibile visualizzare per una richiesta di modifica dopo aver creato il data store degli eventi in AWS CloudTrail Lake.

## Details

L'immagine seguente mostra le informazioni generali relative a una richiesta di modifica disponibili nella scheda Dettagli. Tali dettagli includono varie informazioni, come l'ora di inizio dell'operazione di richiesta di modifica, l'ID dell'utente che ha avviato la richiesta di modifica, la Regione AWS interessata, nonché i relativi ID dell'evento e ID della richiesta.

Details			Event record
Event time	AWS access key	AWS region	
2022-08-29 19:33:05.000	ASIASU4TTD4A[REDACTED]	us-east-1	
User name	Source IP address	Error code	
ChangeRequest-oi-30bc3[REDACTED]	ssm.amazonaws.com	-	
Event name	Event ID	Read-only	
AssumeRole	7339c165-e1bc-4b96-bca7-[REDACTED]	false	
Event source	Request ID	CloudTrail Source	
sts.amazonaws.com	dd6a8c70-fad0-450c-bce0-[REDACTED]	AssumeRole <a href="#">[link]</a>	

## Event record

L'immagine seguente mostra la struttura del contenuto JSON fornito da CloudTrail Lake per un evento di richiesta di modifica. Questi dati vengono forniti nella scheda Record di eventi di una richiesta di modifica.



Details | Event record

```

2 "eventVersion": "1.08",
3 "userIdentity": {"type": "AssumedRole", "principalId": "AROAS[REDACTED]ChangeRequest-01-30b[REDACTED]", "arn": "arn:aws:sts::18230877363:assumed-role/[REDACTED]ChangeRequest-01-30b[REDACTED]"},
4 "eventTime": "2022-08-29 19:33:05.000",
5 "eventSource": "sts.amazonaws.com",
6 "eventName": "AssumeRole",
7 "awsRegion": "us-east-1",
8 "sourceIPAddress": "ssm.amazonaws.com",
9 "userAgent": "ssm.amazonaws.com",
10 "errorCode": "",
11 "errorMessage": "",
12 "requestParameters": {"roleArn": "arn:aws:iam::[REDACTED]:role/AWS-SystemsManager-AutomationExecutionRole", "roleSessionName": "bdec45"},
13 "responseElements": {"assumedRoleId": "[REDACTED]:bdec45c-6772-497e-a052-[REDACTED]"},
14 "additionalEventData": {},
15 "requestID": "dd69ac70-fad0-459c-bc0e-[REDACTED]",
16 "eventID": "7339c165-e1bc-4b96-bca7-[REDACTED]",
17 "readOnly": "false",
18 "resources": [{"accountId": "[REDACTED]", "type": "AWS::IAM::Role", "arn": "arn:aws:iam::[REDACTED]:role/AWS-SystemsManager-AutomationExecutionRole"}],
19 "eventType": "AwsApiCall",
20 "apiVersion": "",
21 "managementEvent": "true",
22 "recipientAccountId": "[REDACTED]",
23 "shareEventID": "9adcfa93-bdef-417e-b322-[REDACTED]",
24 "annotation": "",
25 "vpceEndpointId": "",
26 "serviceEventDetails": "",
27 "addendum": "",
28 "edgeDeviceDetails": "",
29 "insightDetails": "",
30 "eventCategory": "Management",
31 "tlsDetails": "",
32 "sessionCredentialFromConsole": ""
33

```

### ⚠ Important

Se l'organizzazione utilizza Change Manager, puoi completare la seguente procedura dopo aver effettuato l'accesso all'account di gestione o all'account amministratore delegato di Change Manager.

Tuttavia, per utilizzare l'account amministratore delegato per completare questi passaggi, è necessario specificare lo stesso account amministratore delegato per entrambi e. CloudTrail Change Manager

Quando si accede all'account di gestione per Change Manager, è possibile aggiungere o modificare l'account amministratore delegato per nella CloudTrail CloudTrail [pagina Impostazioni](#). Questa operazione deve essere eseguita prima che l'account amministratore delegato possa creare un archivio dati degli eventi per l'intera organizzazione.

Per attivare il monitoraggio degli eventi di CloudTrail Lake da Change Manager

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Change Manager.
3. Seleziona la scheda Richieste.
4. Scegli una richiesta di modifica esistente, quindi scegli la scheda Eventi associati.
5. Scegli Abilita CloudTrail Lake.

6. Segui i passaggi descritti in [Creare un archivio dati per CloudTrail gli eventi](#) nella Guida per l'AWS CloudTrail utente.

Per assicurarti che i dati degli eventi per le tue richieste di modifica siano archiviati, effettua le seguenti selezioni mentre completi la procedura:

- Per Tipo di evento, lascia selezionati gli AWS eventi e CloudTrail gli eventi predefiniti.
- Se utilizzi Change Manager con un'organizzazione, seleziona Abilita per tutti gli account nella mia organizzazione.
- Per Eventi di gestione non deselezionare la casella di controllo Scrittura.

Le altre opzioni scelte durante la creazione dell'archivio dati degli eventi non influiscono sull'archiviazione dei dati per le richieste di modifica.

## Monitoraggio delle automazioni

Le metriche sono il concetto fondamentale in Amazon CloudWatch. Una metrica rappresenta un insieme di punti dati ordinati nel tempo su cui vengono pubblicati. CloudWatch pensa a un parametro come a una variabile da monitorare e ai punti di dati come i valori di questa variabile nel tempo.

L'automazione è uno strumento di AWS Systems Manager. Systems Manager pubblica le metriche sull'utilizzo dell'automazione in CloudWatch. Ciò consente di impostare allarmi in base a tali metriche.

Per visualizzare le metriche di automazione nella console CloudWatch

1. Apri la CloudWatch console all'indirizzo. <https://console.aws.amazon.com/cloudwatch/>
2. Nel riquadro di navigazione, seleziona Parametri.
3. Scegliere SSM.
4. Nella scheda Metriche, scegli Utilizzo, quindi scegli Per AWS risorsa.
5. Nella casella di ricerca vicino all'elenco dei parametri, inserisci SSM.

Per visualizzare le metriche di automazione utilizzando AWS CLI

Aprire un prompt dei comandi e usare il comando seguente.

```
aws cloudwatch list-metrics \
```

```
--namespace "AWS/Usage"
```

## Parametri di Automazione

Systems Manager invia le seguenti metriche di automazione a CloudWatch

Metrica	Description
ConcurrentAutomationUsage	Il numero di automazioni in esecuzione contemporaneamente nell'attuale Account AWS e. Regione AWS
QueuedAutomationUsage	Il numero di automazioni attualmente in coda che non sono state avviate e hanno lo stato Pending.

Per ulteriori informazioni sull'utilizzo delle CloudWatch metriche, consulta i seguenti argomenti nella Amazon CloudWatch User Guide:

- [Parametri](#)
- [Utilizzo delle metriche di Amazon CloudWatch](#)
- [Utilizzo degli allarmi Amazon CloudWatch](#)

## Monitoraggio delle Run Command metriche tramite Amazon CloudWatch

Le metriche sono il concetto fondamentale in Amazon CloudWatch. Una metrica rappresenta un insieme di punti dati ordinati nel tempo su cui vengono pubblicati. CloudWatch pensa a un parametro come a una variabile da monitorare e ai punti di dati come i valori di questa variabile nel tempo.

AWS Systems Manager pubblica metriche sullo stato dei Run Command comandi di CloudWatch, consentendoti di impostare allarmi in base a tali metriche. Run Command è uno strumento in AWS Systems Manager. Queste statistiche vengono registrate per un periodo prolungato in modo da poter accedere alle informazioni storiche e ottenere una migliore prospettiva sulla percentuale di successo dei comandi eseguiti nel proprio Account AWS.

I valori di stato terminale relativi ai comandi per i quali è possibile monitorare i parametri includono Success, Failed e Delivery Timed Out. Per esempio, affinché un set di documenti di comando SSM venga eseguito ogni ora, è possibile configurare un allarme per avvisare l'utente quando uno stato Success non viene segnalato per una di queste ore. Per ulteriori informazioni sui valori di stato dei comandi, consulta [Informazioni sugli stati dei comandi](#).

Per visualizzare le metriche nella console CloudWatch

1. Apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Nel riquadro di navigazione, seleziona Parametri.
3. Nell'area Allarmi per AWS servizio, per Servizi, scegli SSM-. Run Command

Per visualizzare le metriche utilizzando il AWS CLI

Aprire un prompt dei comandi e usare il comando seguente.

```
aws cloudwatch list-metrics --namespace "AWS/SSM-RunCommand"
```

Per visualizzare un elenco di tutti i parametri disponibili, usare il comando seguente.

```
aws cloudwatch list-metrics
```

## Parametri e dimensioni di Systems Manager Run Command

Systems Manager invia le metriche dei Run Command comandi CloudWatch una volta al minuto.

Systems Manager invia le seguenti metriche di comando a CloudWatch.

### Note

Questi parametri utilizzano Count come unità, quindi Sum e SampleCount sono le statistiche più utili.

Metrica	Description
CommandsDeliveryTimedOut	Il numero di comandi con lo stato terminale di Delivery Timed Out.

Metrica	Description
CommandsFailed	Il numero di comandi con lo stato terminale di Failed.
CommandsSucceeded	Il numero di comandi con lo stato terminale di Success.

Per ulteriori informazioni sull'utilizzo CloudWatch delle metriche, consulta i seguenti argomenti nella Amazon CloudWatch User Guide:

- [Parametri](#)
- [Utilizzo dei CloudWatch parametri di Amazon](#)
- [Utilizzo degli CloudWatch allarmi Amazon](#)

## Registrazione dei log AWS Systems Manager Chiamate API con AWS CloudTrail

AWS Systems Manager è integrato con [AWS CloudTrail](#) un servizio che fornisce una registrazione delle azioni intraprese da un utente, da un ruolo o da un Servizio AWS. CloudTrail acquisisce tutte le chiamate API Systems Manager come eventi. Le chiamate acquisite includono le chiamate dalla console di Systems Manager e le chiamate di codice alle operazioni delle API Systems Manager. È possibile utilizzare CloudTrail le informazioni per determinare la richiesta effettuata Systems Manager, l'indirizzo IP di origine 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 CloudTrail degli 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 relativi ai dati di Systems Manager in CloudTrail

Gli [eventi di dati](#) forniscono informazioni sulle operazioni delle risorse eseguite su o in una risorsa (ad esempio, creazione o apertura di un canale di controllo). Queste operazioni sono definite anche operazioni del piano dei dati. Gli eventi di dati sono spesso attività che interessano volumi elevati di dati. Per impostazione predefinita, CloudTrail non registra gli eventi relativi ai dati. La cronologia CloudTrail degli eventi non registra gli eventi relativi ai dati.

Per gli eventi di dati sono previsti costi aggiuntivi. Per ulteriori informazioni sui CloudTrail prezzi, consulta [AWS CloudTrail Prezzi](#).

È possibile registrare gli eventi relativi ai dati per i tipi di risorse di Systems Manager utilizzando la CloudTrail AWS CLI console o le operazioni CloudTrail API. Per ulteriori informazioni su come registrare gli eventi relativi ai dati, consulta [Registrazione di eventi relativi ai dati con Console di gestione AWS](#) e [Registrazione di eventi di dati con AWS Command Line Interface](#) nella Guida per l'utente AWS CloudTrail .

La tabella seguente elenca i tipi di risorse Systems Manager per i quali è possibile registrare gli eventi di dati. La colonna Tipo di evento di dati (console) mostra il valore da scegliere dall'elenco dei tipi di eventi di dati sulla CloudTrail console. La colonna del valore `resources.type` mostra il `resources.type` valore da specificare durante la configurazione dei selettori di eventi avanzati utilizzando le API or. AWS CLI CloudTrail La CloudTrail colonna Data API loggate mostra le chiamate API registrate per il tipo di risorsa. CloudTrail

Tipo di evento di dati (console)	valore <code>resources.type</code>	API di dati a cui è stato effettuato l'accesso CloudTrail
Systems Manager	<code>AWS::SSMMessages::ControlChannel</code>	<ul style="list-style-type: none"> <li><code>CreateControlChannel</code></li> <li><code>OpenControlChannel</code></li> </ul> <p>Per ulteriori informazioni su queste operazioni, consulta la sezione <a href="#">Operazioni</a></p>

Tipo di evento di dati (console)	valore resources.type	API di dati a cui è stato effettuato l'accesso CloudTrail
		<a href="#">definite da Amazon Message Gateway Service</a> nella Service Authorization Reference.
Nodo gestito da Systems Manager	AWS::SSM::ManagedNode	<ul style="list-style-type: none"> <li>RequestManagedInstanceRoleToken — Questo evento viene generato quando l' AWS Systems Manager Agent (SSM Agent) in esecuzione su un nodo gestito da Systems Manager richiede le credenziali dal servizio di credenziali di Systems Manager.</li> </ul> <p>Per ulteriori informazioni sull'operazione RequestManagedInstanceRoleToken , consulta <a href="#">Convalida di macchine attivate da sistemi tramite un'impronta digitale hardware</a></p>

È possibile configurare selettori di eventi avanzati per filtrare i campi eventName, readOnly e resources .ARN per registrare solo gli eventi importanti per l'utente. Per ulteriori informazioni su questi campi, consulta [AdvancedFieldSelector](#) in Riferimento API AWS CloudTrail .

## Eventi di gestione di Systems Manager 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.



Systems Manager registra tutte le operazioni del piano di controllo CloudTrail come eventi di gestione. Le operazioni API di Systems Manager sono documentate nella [Documentazione di riferimento API AWS Systems Manager](#). Ad esempio, le chiamate a `CreateMaintenanceWindows`, `PutInventorySendCommand`, e `StartSession` le azioni generano voci nei file di CloudTrail registro. Per un esempio di configurazione per CloudTrail monitorare una chiamata all'API di Systems Manager, vedere [Monitoraggio dell'attività della sessione tramite Amazon EventBridge \(console\)](#).

## Esempi di eventi Systems Manager

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.

Esempi:

- [Esempi di eventi di gestione](#)
- [Esempi di eventi di dati](#)

### Esempi di eventi di gestione

#### Esempio 1: **DeleteDocument**

L'esempio seguente mostra un CloudTrail evento che dimostra l'`DeleteDocument` operazione su un documento denominato `example-Document` nella regione Stati Uniti orientali (Ohio) (`us-east-2`).

```
{
 "eventVersion": "1.04",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "AKIAI44QH8DHBEXAMPLE:203.0.113.11",
 "arn": "arn:aws:sts::123456789012:assumed-role/example-role/203.0.113.11",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
 "attributes": {
 "mfaAuthenticated": "false",
 "creationDate": "2018-03-06T20:19:16Z"
 },
 "sessionIssuer": {
 "type": "Role",
```

```

 "principalId": "AKIAI44QH8DHBEXAMPLE",
 "arn": "arn:aws:iam::123456789012:role/example-role",
 "accountId": "123456789012",
 "userName": "example-role"
 }
},
"eventTime": "2018-03-06T20:30:12Z",
"eventSource": "ssm.amazonaws.com",
"eventName": "DeleteDocument",
"awsRegion": "us-east-2",
"sourceIPAddress": "203.0.113.11",
"userAgent": "example-user-agent-string",
"requestParameters": {
 "name": "example-Document"
},
"responseElements": null,
"requestID": "86168559-75e9-11e4-8cf8-75d18EXAMPLE",
"eventID": "832b82d5-d474-44e8-a51d-093ccEXAMPLE",
"resources": [
 {
 "ARN": "arn:aws:ssm:us-east-2:123456789012:document/example-Document",
 "accountId": "123456789012"
 }
],
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012",
"eventCategory": "Management"
}

```

## Esempio 2: **StartConnection**

L'esempio seguente mostra un CloudTrail evento per un utente che avvia una connessione RDP utilizzando Fleet Manager nella regione Stati Uniti orientali (Ohio) (us-east-2). L'azione API sottostante è **StartConnection**.

```

{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "AKIAI44QH8DHBEXAMPLE",
 "arn": "arn:aws:sts::123456789012:assumed-role/exampleRole",
 "accountId": "123456789012",

```

```

 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
 "sessionIssuer": {
 "type": "Role",
 "principalId": "AKIAI44QH8DHBEXAMPLE",
 "arn": "arn:aws:sts::123456789012:assumed-role/exampleRole",
 "accountId": "123456789012",
 "userName": "exampleRole"
 },
 "webIdFederationData": {},
 "attributes": {
 "creationDate": "2021-12-13T14:57:05Z",
 "mfaAuthenticated": "false"
 }
 },
 "eventTime": "2021-12-13T16:50:41Z",
 "eventSource": "ssm-guiconnect.amazonaws.com",
 "eventName": "StartConnection",
 "awsRegion": "us-east-2",
 "sourceIPAddress": "34.230.45.60",
 "userAgent": "example-user-agent-string",
 "requestParameters": {
 "AuthType": "Credentials",
 "Protocol": "RDP",
 "ConnectionType": "SessionManager",
 "InstanceId": "i-02573cafcfEXAMPLE"
 },
 "responseElements": {
 "ConnectionArn": "arn:aws:ssm-guiconnect:us-east-2:123456789012:connection/fcb810cd-241f-4aae-9ee4-02d59EXAMPLE",
 "ConnectionKey": "71f9629f-0f9a-4b35-92f2-2d253EXAMPLE",
 "ClientToken": "49af0f92-d637-4d47-9c54-ea51aEXAMPLE",
 "requestId": "d466710f-2adf-4e87-9464-055b2EXAMPLE"
 },
 "requestID": "d466710f-2adf-4e87-9464-055b2EXAMPLE",
 "eventID": "fc514f57-ba19-4e8b-9079-c2913EXAMPLE",
 "readOnly": false,
 "eventType": "AwsApiCall",
 "managementEvent": true,
 "recipientAccountId": "123456789012",
 "eventCategory": "Management"
 }
}

```

## Esempi di eventi di dati

### Esempio 1: **CreateControlChannel**

L'esempio seguente mostra un CloudTrail evento che dimostra l'operazione.

#### CreateControlChannel

```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "AKIAI44QH8DHBEXAMPLE",
 "arn": "arn:aws:sts::123456789012:assumed-role/exampleRole",
 "accountId": "123456789012",
 "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
 "sessionContext": {
 "sessionIssuer": {
 "type": "Role",
 "principalId": "AKIAI44QH8DHBEXAMPLE",
 "arn": "arn:aws:iam::123456789012:role/exampleRole",
 "accountId": "123456789012",
 "userName": "exampleRole"
 },
 "attributes": {
 "creationDate": "2023-05-04T23:14:50Z",
 "mfaAuthenticated": "false"
 }
 },
 "attributes": {
 "creationDate": "2023-05-04T23:14:50Z",
 "mfaAuthenticated": "false"
 }
 },
 "eventTime": "2023-05-04T23:53:55Z",
 "eventSource": "ssm.amazonaws.com",
 "eventName": "CreateControlChannel",
 "awsRegion": "us-east-1",
 "sourceIPAddress": "192.0.2.0",
 "userAgent": "example-agent",
 "requestParameters": {
 "channelId": "44295c1f-49d2-48b6-b218-96823EXAMPLE",
 "messageSchemaVersion": "1.0",
 "requestId": "54993150-0e8f-4142-aa54-3438EXAMPLE",
 "userAgent": "example-agent"
 },
 "responseElements": {
 "messageSchemaVersion": "1.0",
```

```

 "tokenValue": "Value hidden due to security reasons.",
 "url": "example-url"
 },
 "requestID": "54993150-0e8f-4142-aa54-3438EXAMPLE",
 "eventID": "a48a28de-7996-4ca1-a3a0-a51fEXAMPLE",
 "readOnly": false,
 "resources": [
 {
 "accountId": "123456789012",
 "type": "AWS::SSMMessages::ControlChannel",
 "ARN": "arn:aws:ssmmessages:us-east-1:123456789012:control-
channel/44295c1f-49d2-48b6-b218-96823EXAMPLE"
 }
],
 "eventType": "AwsApiCall",
 "managementEvent": false,
 "recipientAccountId": "123456789012",
 "eventCategory": "Data"
}

```

## Esempio 2: RequestManagedInstanceRoleToken

L'esempio seguente mostra un CloudTrail evento che dimostra l'RequestManagedInstanceRoleToken operazione.

```

{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012:aws:ec2-instance:i-02854e4bEXAMPLE",
 "arn": "arn:aws:sts::123456789012:assumed-role/aws:ec2-instance/
i-02854e4bEXAMPLE",
 "accountId": "123456789012",
 "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
 "sessionContext": {
 "sessionIssuer": {
 "type": "Role",
 "principalId": "123456789012:aws:ec2-instance",
 "arn": "arn:aws:iam::123456789012:role/aws:ec2-instance",
 "accountId": "123456789012",
 "userName": "aws:ec2-instance"
 }
 },
 "attributes": {

```

```

 "creationDate": "2023-08-27T03:34:46Z",
 "mfaAuthenticated": "false"
 },
 "ec2RoleDelivery": "2.0"
}
},
"eventTime": "2023-08-27T03:37:15Z",
"eventSource": "ssm.amazonaws.com",
"eventName": "RequestManagedInstanceRoleToken",
"awsRegion": "us-east-1",
"sourceIPAddress": "192.0.2.0",
"userAgent": "Apache-HttpClient/UNAVAILABLE (Java/1.8.0_362)",
"requestParameters": {
 "fingerprint": "i-02854e4bf85EXAMPLE"
},
"responseElements": null,
"requestID": "2582cced-455b-4189-9b82-7b48EXAMPLE",
"eventID": "7f200508-e547-4c27-982d-4da0EXAMLE",
"readOnly": true,
"resources": [
 {
 "accountId": "123456789012",
 "type": "AWS::SSM::ManagedNode",
 "ARN": "arn:aws:ec2:us-east-1:123456789012:instance/i-02854e4bEXAMPLE"
 }
],
"eventType": "AwsApiCall",
"managementEvent": false,
"recipientAccountId": "123456789012",
"eventCategory": "Data"
}

```

Per informazioni sui contenuti dei CloudTrail record, vedere i contenuti dei [CloudTrail record](#) nella Guida per l'AWS CloudTrail utente.

## Uscita dell'azione Logging Automation con Logs CloudWatch

L'automazione si integra con Amazon CloudWatch Logs. È possibile inviare l'output dalle operazioni `aws:executeScript` nei propri runbook al gruppo di log specificato. Systems Manager non crea un gruppo di log o flussi di log per i documenti che non utilizzano le operazioni di `aws:executeScript`. Se il documento utilizza `aws:executeScript`, l'output inviato a CloudWatch Logs riguarda solo tali azioni. È possibile utilizzare l'output dell'`aws:executeScript` azione memorizzato nel gruppo

di CloudWatch log Logs per scopi di debug e risoluzione dei problemi. Se scegli un gruppo di log crittografato, anche l'output dell'azione `aws:executeScript` è crittografato. Il log dell'output delle azioni di `aws:executeScript` è un'impostazione a livello di account.

Per inviare l'output delle azioni a CloudWatch Logs for Amazon owned runbook, l'utente o il ruolo che esegue l'automazione deve disporre delle autorizzazioni per le seguenti operazioni:

- `logs:CreateLogGroup`
- `logs:CreateLogStream`
- `logs:DescribeLogGroups`
- `logs:DescribeLogStreams`
- `logs:PutLogEvents`

Per i runbook di tua proprietà, devi aggiungere le stesse autorizzazioni al ruolo (o AssumeRole) del servizio IAM che usi per eseguire il runbook.

Per inviare l'output dell'azione a CloudWatch Logs (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Automazione.
3. Scegli la scheda Preferenze, quindi seleziona Modifica.
4. Seleziona la casella di controllo accanto a `Invia output a CloudWatch Logs`.
5. (Consigliato) Seleziona la casella di controllo accanto a `Crittografare i dati di log`. Se questa opzione è attivata, i dati di log vengono crittografati utilizzando la chiave di crittografia lato server specificata per il gruppo di log. Se non desideri crittografare i dati di registro inviati a CloudWatch Logs, deseleziona la casella di controllo. Deselezionare la casella di controllo se la crittografia non è consentita nel gruppo di log.
6. Per il gruppo di CloudWatch log Logs, per specificare il gruppo di CloudWatch log Logs esistente nel tuo gruppo a Account AWS cui desideri inviare l'output dell'azione, seleziona una delle seguenti opzioni:
  - Invia l'output al gruppo di log predefinito: se il gruppo di log predefinito non esiste (`/aws/ssm/automation/executeScript`), l'automazione lo crea automaticamente.

- Choose from the list of log groups (Scegli un gruppo dall'elenco dei gruppi di log): selezionare un gruppo di log che è già stato creato nel proprio account per archiviare i risultati delle operazioni.
  - Enter a bucket name in the text box (Immetti un nome di bucket nella casella di testo): immettere il nome di un gruppo di log che è già stato creato nell'account per archiviare i risultati delle operazioni.
7. Scegli Save (Salva).

Per inviare l'output dell'azione a CloudWatch Logs (riga di comando)

1. Aprire lo strumento di riga di comando preferito ed eseguire il comando seguente per aggiornare la destinazione del risultato dell'azione.

#### Linux & macOS

```
aws ssm update-service-setting \
 --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-destination \
 --setting-value CloudWatch
```

#### Windows

```
aws ssm update-service-setting ^
 --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-destination ^
 --setting-value CloudWatch
```

#### PowerShell

```
Update-SSMServiceSetting `
 -SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-destination" `
 -SettingValue "CloudWatch"
```

Se il comando va a buon fine, non viene generato output.

2. Eseguire il comando seguente per specificare il gruppo di log a cui inviare il risultato dell'azione.



## Linux & macOS

```
aws ssm update-service-setting \
 --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-group-name \
 --setting-value my-log-group
```

## Windows

```
aws ssm update-service-setting ^
 --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-group-name ^
 --setting-value my-log-group
```

## PowerShell

```
Update-SSMServiceSetting `
 -SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-group-name" `
 -SettingValue "my-log-group"
```

Se il comando va a buon fine, non viene generato output.

3. Esegui il comando seguente per visualizzare le impostazioni correnti del servizio per le preferenze di registrazione delle azioni di Automation nell'attuale Account AWS e Regione AWS.

## Linux & macOS

```
aws ssm get-service-setting \
 --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-destination
```

## Windows

```
aws ssm get-service-setting ^
 --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-destination
```

## PowerShell

```
Get-SSMServiceSetting `
 -SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-destination"
```

Il comando restituisce informazioni simili alle seguenti.

```
{
 "ServiceSetting": {
 "Status": "Customized",
 "LastModifiedDate": 1613758617.036,
 "SettingId": "/ssm/automation/customer-script-log-destination",
 "LastModifiedUser": "arn:aws:sts::123456789012:assumed-role/Administrator/
User_1",
 "SettingValue": "CloudWatch",
 "ARN": "arn:aws:ssm:us-east-2:123456789012:servicesetting/ssm/automation/
customer-script-log-destination"
 }
}
```

## Configurazione di Amazon CloudWatch Logs per Run Command

Quando invii un comando usando Run Command, puoi specificare la destinazione a cui inviare l'output del comando. Per impostazione predefinita, Systems Manager restituisce solo i primi 24.000 caratteri dell'output del comando. Se si desidera visualizzare i dettagli completi del risultato del comando, è possibile specificare un bucket Amazon Simple Storage Service (Amazon S3). Oppure puoi specificare Amazon CloudWatch Logs. Se specifichi CloudWatch Logs, invia Run Command periodicamente tutti gli output dei comandi e i log degli errori a CloudWatch Logs. È possibile monitorare i log di output in tempo quasi reale, cercare locuzioni, valori o modelli specifici e creare allarmi in base alla ricerca.

Se hai configurato il nodo gestito per utilizzare le policy gestite AWS Identity and Access Management (IAM) AmazonSSMManagedInstanceCore eCloudWatchAgentServerPolicy, allora il nodo non richiede alcuna configurazione aggiuntiva per inviare l'output a CloudWatch Logs. Scegli questa opzione se invii comandi dalla console o aggiungi la `cloud-watch-output-config` sezione e il `CloudWatchOutputEnabled` parametro se usi la AWS Command Line Interface (AWS

CLI) o un'operazione API. AWS Tools for Windows PowerShell La sezione `cloud-watch-output-config` e il parametro `CloudWatchOutputEnabled` sono descritti in dettaglio più avanti in questo argomento.

Per informazioni sull'aggiunta di policy a un profilo dell'istanza per le istanze EC2, consulta la pagina [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#). Per informazioni sull'aggiunta di policy a un ruolo di servizio per server on-premises e macchine virtuali che si prevede di utilizzare come nodi gestiti, si veda [Creazione di un ruolo di servizio IAM richiesto per System Manager in ambiente ibrido e multicloud](#).

Se utilizzi una policy personalizzata sui tuoi nodi, aggiorna la policy su ogni nodo per consentire a Systems Manager di inviare output e CloudWatch log a Logs. Aggiungere i seguenti oggetti di policy alla policy personalizzata. Per informazioni sull'aggiornamento di una policy IAM, si veda [Editing IAM policies \(Modifica di policy IAM\)](#) nella Guida per l'utente di IAM.

```
{
 "Effect": "Allow",
 "Action": "logs:DescribeLogGroups",
 "Resource": "*"
},
{
 "Effect": "Allow",
 "Action": [
 "logs:CreateLogGroup",
 "logs:CreateLogStream",
 "logs:DescribeLogStreams",
 "logs:PutLogEvents"
],
 "Resource": "arn:aws:logs:*:*:log-group:/aws/ssm/*"
},
```

## Specificare i CloudWatch log quando si inviano comandi

Per specificare CloudWatch Logs come output quando inviate un comando da Console di gestione AWS, scegliete `CloudWatch Output` nella sezione `Opzioni di output`. Facoltativamente, è possibile specificare il nome del gruppo CloudWatch Logs a cui inviare l'output del comando. Se non si specifica il nome di un gruppo, Systems Manager crea automaticamente un gruppo di log. Il gruppo di log utilizza il seguente formato di nomi: `/aws/ssm/SystemsManagerDocumentName`

Se si eseguono comandi utilizzando il AWS CLI, specificare la `cloud-watch-output-config` sezione del comando. Questa sezione consente di specificare il `CloudWatchOutputEnabled` parametro e, facoltativamente, il `CloudWatchLogGroupName` parametro. Ecco un esempio.

## Linux & macOS

```
aws ssm send-command \
 --instance-ids "instance ID" \
 --document-name "AWS-RunShellScript" \
 --parameters "commands=echo helloWorld" \
 --cloud-watch-output-config
 "CloudWatchOutputEnabled=true,CloudWatchLogGroupName=log group name"
```

## Windows

```
aws ssm send-command ^
 --document-name "AWS-RunPowerShellScript" ^
 --parameters commands=["echo helloWorld"] ^
 --targets "Key=instanceids,Values=an instance ID" ^
 --cloud-watch-output-config '{"CloudWatchLogGroupName": "log group name",
 "CloudWatchOutputEnabled":true}'
```

## Visualizzazione dell'output dei comandi nei log CloudWatch

Non appena il comando inizia a essere eseguito, Systems Manager invia l'output a CloudWatch Logs in tempo quasi reale. L'output in CloudWatch Logs utilizza il seguente formato:

*CommandID/InstanceID/PluginID/stdout*

*CommandID/InstanceID/PluginID/stderr*

Il risultato dell'esecuzione viene caricato ogni 30 secondi o quando il buffer supera i 200 KB, a seconda di quale condizione si verifica prima.

### Note

I flussi di log vengono creati solo quando sono disponibili dati di output. Per esempio, se per un'esecuzione non sono presenti dati con errori, il flusso `stderr` non viene creato.

Ecco un esempio dell'output del comando così come viene visualizzato in CloudWatch Logs.

```
Group - /aws/ssm/AWS-RunShellScript
Streams -
1234-567-8910/i-abcd-efg-hijk/AWS-RunPowerShellScript/stdout
24/1234-567-8910/i-abcd-efg-hijk/AWS-RunPowerShellScript/stderr
```

## Monitoraggio degli eventi di Systems Manager con Amazon EventBridge

Amazon EventBridge è un servizio di bus di eventi senza server che ti consente di connettere le tue applicazioni con dati provenienti da una varietà di fonti. EventBridge fornisce un flusso di dati in tempo reale dalle tue applicazioni, dalle applicazioni Software-as-a-Service (SaaS) Servizi AWS e indirizza tali dati verso obiettivi come AWS Lambda. È possibile impostare regole di routing per determinare dove inviare i dati per creare architetture applicative che reagiscono in tempo reale a tutte le fonti di dati. EventBridge consente di creare architetture basate sugli eventi, che sono liberamente accoppiate e distribuite.

EventBridge in precedenza si chiamava Amazon Events. CloudWatch EventBridge include nuove funzionalità che ti consentono di ricevere eventi dai partner SaaS e dalle tue applicazioni. Gli utenti esistenti di CloudWatch Events possono accedere al bus, alle regole e agli eventi predefiniti esistenti nella nuova EventBridge console e nella console CloudWatch Events. EventBridge utilizza la stessa API CloudWatch Events, quindi tutto l'utilizzo dell'API CloudWatch Events esistente rimane lo stesso.

EventBridge puoi aggiungere decine di eventi Servizi AWS alle tue regole e obiettivi da oltre 20 Servizi AWS.

EventBridge fornisce supporto sia per AWS Systems Manager gli eventi che per gli obiettivi di Systems Manager.

### Tipi di eventi supportati da Systems Manager

Tra i molti tipi di eventi di Systems Manager che è EventBridge possibile rilevare ci sono:

- gli aggiornamenti dello stato della richiesta di accesso ai nodi just-in-time per le approvazioni manuali.
- Le mancate richieste di accesso ai nodi just-in-time.
- La disattivazione della finestra di manutenzione.

- Un flusso di lavoro di Automation completato in modo corretto. L'automazione è uno strumento di AWS Systems Manager.
- Un nodo gestito non rientra nella conformità delle patch.
- Valore del parametro in fase di aggiornamento.

EventBridge supporta gli eventi provenienti dai seguenti AWS Systems Manager strumenti:

- Just-in-time accesso al nodo (gli eventi vengono emessi nel migliore dei modi)
- Automation (gli eventi vengono emessi sulla base del miglior tentativo).
- Change Calendar (Gli eventi vengono emessi nel miglior modo possibile.)
- Conformità
- Inventario (Gli eventi vengono emessi nel miglior modo possibile).
- Maintenance Windows (Gli eventi vengono emessi nel miglior modo possibile.)
- Parameter Store (Gli eventi vengono emessi nel miglior modo possibile.)
- Run Command (Gli eventi vengono emessi nel miglior modo possibile.)
- State Manager (Gli eventi vengono emessi nel miglior modo possibile.)

Per informazioni dettagliate sui tipi di evento di Systems Manager supportati, vedere [Riferimento: modelli e tipi di EventBridge eventi Amazon per Systems Manager](#) e [Esempi di EventBridge eventi Amazon per Systems Manager](#).

### Tipi di target supportati da Systems Manager

EventBridge supporta i seguenti tre strumenti di Systems Manager come obiettivi di una regola di evento:

- Esecuzione di un flusso di lavoro di Automation
- Esecuzione di un documento di comando Run Command (Gli eventi vengono emessi nel miglior modo possibile).
- Creazione di un OpsCenter OpsItem

Per le modalità suggerite in cui è possibile utilizzare queste destinazioni, vedere [Scenari di esempio: obiettivi di Systems Manager nelle EventBridge regole di Amazon](#).

Per ulteriori informazioni su come iniziare EventBridge e impostare le regole, consulta [Getting started with Amazon EventBridge](#) nella Amazon EventBridge User Guide. Per informazioni complete su come lavorare con EventBridge, consulta la [Amazon EventBridge User Guide](#).

## Argomenti

- [Configurazione EventBridge per gli eventi di Systems Manager](#)
- [Esempi di EventBridge eventi Amazon per Systems Manager](#)
- [Scenari di esempio: obiettivi di Systems Manager nelle EventBridge regole di Amazon](#)

## Configurazione EventBridge per gli eventi di Systems Manager

Puoi usare Amazon EventBridge per eseguire un evento target quando si verificano cambiamenti di AWS Systems Manager stato supportati, cambiamenti di stato o altre condizioni. Puoi scegliere di creare una regola che venga eseguita ogni volta che si verifica una transizione di stato o status, o quando si verifica una transizione verso uno o più stati di interesse.

La procedura seguente fornisce i passaggi generali per la creazione di una EventBridge regola che si attiva quando un evento specificato viene emesso da Systems Manager. Per un elenco delle procedure in questa guida per l'utente relative a scenari specifici, vedere Ulteriori informazioni alla fine di questo argomento.

### Note

Quando un servizio all'interno dell'utente Account AWS emette un evento, viene sempre indirizzato al bus eventi predefinito dell'account. Per scrivere una regola che risponde agli eventi provenienti dagli Servizi AWS nel tuo account, associala al router di eventi predefinito. Puoi creare una regola su un bus di eventi personalizzato da cui cercare gli eventi Servizi AWS, ma questa regola si applica solo quando ricevi un evento di questo tipo da un altro account tramite la distribuzione di eventi su più account. Per ulteriori informazioni, consulta [Invio e ricezione di EventBridge eventi Amazon tra Account AWS](#) nella Amazon EventBridge User Guide.

## EventBridge Per configurare gli eventi di Systems Manager

1. Apri la EventBridge console Amazon all'indirizzo <https://console.aws.amazon.com/events/>.
2. Nel pannello di navigazione, scegli Regole.

3. Scegli Crea regola.
4. Inserisci un nome e una descrizione per la regola.

Una regola non può avere lo stesso nome di un'altra regola nello stesso bus di eventi Regione AWS e sullo stesso bus.

5. Per Router di eventi, scegli quello che desideri associare a questa regola. Se desideri che questa regola risponda agli eventi corrispondenti che provengono dai tuoi Account AWS, seleziona predefinito. Quando un Servizio AWS utente del tuo account emette un evento, viene sempre indirizzato al bus eventi predefinito del tuo account.
6. Per Tipo di regola, scegli Regola con un modello di eventi.
7. Scegli Avanti.
8. Per Origine degli eventi, scegli AWS eventi o eventi EventBridge partner.
9. Nella sezione Modello di eventi, scegli Modulo di modello di eventi.
10. Per Origine evento, scegli Servizi AWS .
11. Per AWS , scegli Systems Manager.
12. Per Tipo di evento, procedere in uno dei seguenti modi:

- Scegli Tutti gli eventi.

Se scegli Tutti gli eventi, quelli emessi da Systems Manager corrisponderanno alla regola. Tieni presente che questa opzione può comportare molte operazioni di destinazione evento.

- Scegli il tipo di evento di Systems Manager da utilizzare per questa regola. EventBridge supporta gli eventi dei seguenti AWS Systems Manager strumenti:
  - Automazione
  - Change Calendar
  - Conformità
  - Inventory
  - Maintenance Windows
  - Parameter Store
  - Run Command
  - State Manager



 Note

Per le azioni di Systems Manager che non sono supportate da EventBridge, puoi scegliere una chiamata AWS API CloudTrail per creare una regola di evento basata su una chiamata API, che viene registrata da CloudTrail. Per un esempio, consulta [Monitoraggio dell'attività della sessione tramite Amazon EventBridge \(console\)](#).

13. (Facoltativo) Per rendere la regola più specifica, aggiungi i valori del filtro. Ad esempio, se hai scelto State Manager e vuoi limitare la regola allo stato di una singola istanza gestita a cui è destinata un'associazione, per Tipi specifici, scegli Modifica dello stato dell'associazione dell'istanza del gestore di stato EC2.

Per informazioni complete sui tipi di dettagli supportati, consulta [Riferimento: modelli e tipi di EventBridge eventi Amazon per Systems Manager](#).

Alcuni tipi di dettaglio hanno altre opzioni supportate, come lo stato. Le opzioni disponibili dipendono dallo strumento selezionato.

14. Scegli Avanti.
15. Per Tipi di destinazione, scegli servizio AWS .
16. Per Seleziona un obiettivo, scegli un obiettivo, ad esempio un argomento o una AWS Lambda funzione di Amazon SNS. La destinazione viene attivata quando viene ricevuto un evento che corrisponde al modello di evento definito nella regola.
17. Per molti tipi di target, EventBridge sono necessarie le autorizzazioni per inviare eventi al target. In questi casi, EventBridge può creare il ruolo AWS Identity and Access Management (IAM) necessario per l'esecuzione della regola:
- Per creare un ruolo IAM automaticamente, seleziona Crea un nuovo ruolo per questa risorsa specifica.
  - Per utilizzare un ruolo IAM creato in precedenza, seleziona Utilizza un ruolo esistente.
18. (Facoltativo) Scegli Aggiungi destinazione per aggiungere un'altra destinazione per questa regola.
19. Scegli Avanti.
20. (Facoltativo) Inserire uno o più tag per la regola. Per ulteriori informazioni, consulta i EventBridge tag [Amazon](#) nella Amazon EventBridge User Guide.
21. Scegli Avanti.

22. Rivedi i dettagli della regola e scegli **Crea regola**.

#### Ulteriori informazioni

- [Creazione di un EventBridge evento che utilizza un runbook \(console\)](#)
- [Trasmissione dei dati ad Automazione tramite trasformatori di input](#)
- [Risolvere i problemi di conformità utilizzando EventBridge](#)
- [Visualizzazione delle azioni di eliminazione dell'inventario in EventBridge](#)
- [Configura EventBridge le regole per creare OpsItems](#)
- [Configurazione delle EventBridge regole per i parametri e delle politiche relative ai parametri](#)

## Esempi di EventBridge eventi Amazon per Systems Manager

Di seguito sono riportati alcuni esempi, in formato JSON, di EventBridge eventi supportati per AWS Systems Manager

#### Tipi di eventi Systems Manager

- [AWS Systems Manager Eventi di automazione](#)
- [AWS Systems Manager Modifica calendario Eventi](#)
- [AWS Systems Manager Change Manager Eventi](#)
- [AWS Systems Manager Eventi di conformità](#)
- [AWS Systems Manager Intervallo di manutenzione Eventi](#)
- [AWS Systems Manager Parameter Store Eventi](#)
- [AWS Systems Manager OpsCenter Eventi](#)
- [AWS Systems Manager Run Command Eventi](#)
- [AWS Systems Manager State Manager Eventi](#)

## AWS Systems Manager Eventi di automazione

#### Status-change Notifica della fase di automazione

```
{
 "version": "0",
 "id": "eeca120b-a321-433e-9635-dab369006a6b",
 "detail-type": "EC2 Automation Step Status-change Notification",
```

```

"source": "aws.ssm",
"account": "123456789012",
"time": "2024-11-29T19:43:35Z",
"region": "us-east-1",
"resources": ["arn:aws:ssm:us-east-2:123456789012:automation-
execution/333ba70b-2333-48db-b17e-a5e69c6f4d1c",
 "arn:aws:ssm:us-east-2:123456789012:automation-definition/runcommand1:1"],
"detail": {
 "ExecutionId": "333ba70b-2333-48db-b17e-a5e69c6f4d1c",
 "Definition": "runcommand1",
 "DefinitionVersion": 1.0,
 "Status": "Success",
 "EndTime": "Nov 29, 2024 7:43:25 PM",
 "StartTime": "Nov 29, 2024 7:43:23 PM",
 "Time": 2630.0,
 "StepName": "runFixedCmds",
 "Action": "aws:runCommand"
}
}

```

## Status-changeNotifica di esecuzione dell'automazione

```

{
 "version": "0",
 "id": "d290ece9-1088-4383-9df6-cd5b4ac42b99",
 "detail-type": "EC2 Automation Execution Status-change Notification",
 "source": "aws.ssm",
 "account": "123456789012",
 "time": "2024-11-29T19:43:35Z",
 "region": "us-east-2",
 "resources": ["arn:aws:ssm:us-east-2:123456789012:automation-
execution/333ba70b-2333-48db-b17e-a5e69c6f4d1c",
 "arn:aws:ssm:us-east-2:123456789012:automation-definition/runcommand1:1"],
 "detail": {
 "ExecutionId": "333ba70b-2333-48db-b17e-a5e69c6f4d1c",
 "Definition": "runcommand1",
 "DefinitionVersion": 1.0,
 "Status": "Success",
 "StartTime": "Nov 29, 2024 7:43:20 PM",
 "EndTime": "Nov 29, 2024 7:43:26 PM",
 "Time": 5753.0,
 "ExecutedBy": "arn:aws:iam::123456789012:user/userName"
 }
}

```

```
}
```

## AWS Systems Manager Modifica calendario Eventi

Utilizza le informazioni contenute in questo argomento per pianificare e comprendere il comportamento degli EventBridge eventi per AWS Systems Manager Change Calendar.

### Note

Le modifiche di stato per i calendari condivisi da altri non Account AWS sono attualmente supportate.

### Modifica calendario integrazione con Amazon EventBridge

AWS Systems Manager Change Calendar si integra con Amazon EventBridge per notificarti le modifiche allo stato del calendario. Tieni presente i seguenti comportamenti relativi all'architettura di pianificazione sottostante:

#### Tempistica e affidabilità degli eventi

- EventBridge invia notifiche nel migliore dei modi con una tolleranza di pianificazione fino a 15 minuti.
- Gli eventi di modifica dello stato riflettono le transizioni generali dello stato del calendario, non i singoli eventi di quest'ultimo.
- Quando più eventi del calendario si verificano contemporaneamente, EventBridge genera un solo evento per ogni modifica effettiva dello stato del calendario.
- EventBridge attiva gli eventi solo quando lo stato generale del calendario passa (ad esempio, da CHIUSO a APERTO), non per i singoli eventi del calendario che non comportano un cambiamento di stato.
- Gli eventi di avviso che non modificano lo stato del calendario non attivano le notifiche. EventBridge

#### Modifiche agli eventi e considerazioni sulla tempistica

- Se modifichi gli eventi del calendario entro 15 minuti dall'ora di inizio o di fine pianificata, EventBridge potresti generare notifiche duplicate o perderne le notifiche.
- Questo comportamento si verifica, perché il sistema di pianificazione potrebbe non avere tempo sufficiente per aggiornare o annullare correttamente le notifiche precedentemente pianificate.

- Per gli eventi ricorrenti, questo comportamento influisce in genere solo sulla prima occorrenza dopo la modifica.

### Eventi adiacenti e sovrapposti

- Quando gli eventi del calendario sono programmati a distanza di cinque minuti l'uno dall'altro, è possibile che si verifichino o meno eventi di transizione di stato, a seconda dell'effettivo cambiamento di stato.
- La creazione di eventi sovrapposti in determinati ordini potrebbe generare EventBridge eventi aggiuntivi anche quando non si verifica alcun cambiamento di stato effettivo.
- Per garantire un comportamento prevedibile, evita di creare o modificare eventi del calendario prossimi ai tempi di esecuzione.

### Best practice

- Progetta le EventBridge regole e l'automazione a valle per gestire potenziali eventi duplicati.
- Implementa l'idempotenza nei flussi di lavoro di automazione, per evitare problemi dovuti alla duplicazione delle notifiche.
- Concedi un tempo di consegna sufficiente (almeno 15 minuti) quando crei o modifichi gli eventi del calendario.
- Testa a fondo EventBridge le tue integrazioni con i modelli specifici degli eventi del tuo calendario.

### Calendario APERTO

```
{
 "version": "0",
 "id": "47a3f03a-f30d-1011-ac9a-du3bdEXAMPLE",
 "detail-type": "Calendar State Change",
 "source": "aws.ssm",
 "account": "123456789012",
 "time": "2024-09-19T18:00:07Z",
 "region": "us-east-2",
 "resources": [
 "arn:aws:ssm:us-east-2:123456789012:document/MyCalendar"
],
 "detail": {
 "state": "OPEN",
 "atTime": "2024-09-19T18:00:07Z",
 "nextTransitionTime": "2024-10-11T18:00:07Z"
 }
}
```

```
}
```

## Calendario CHIUSO

```
{
 "version": "0",
 "id": "f30df03a-1011-ac9a-47a3-f761eEXAMPLE",
 "detail-type": "Calendar State Change",
 "source": "aws.ssm",
 "account": "123456789012",
 "time": "2024-09-17T21:40:02Z",
 "region": "us-east-2",
 "resources": [
 "arn:aws:ssm:us-east-2:123456789012:document/MyCalendar"
],
 "detail": {
 "state": "CLOSED",
 "atTime": "2024-08-17T21:40:00Z",
 "nextTransitionTime": "2024-09-19T18:00:07Z"
 }
}
```

## AWS Systems Manager Change Manager Eventi

### Notifica di aggiornamento dello stato della richiesta di modifica - Esempio 1

```
{
 "version": "0",
 "id": "feab80c1-a8ff-c721-b8b1-96ce70939696",
 "detail-type": "Change Request Status Update",
 "source": "aws.ssm",
 "account": "123456789012",
 "time": "2024-10-24T10:51:52Z",
 "region": "us-east-1",
 "resources": [
 "arn:aws:ssm:us-west-2:123456789012:opsitem/oi-12345abcdef",
 "arn:aws:ssm:us-west-2:123456789012:document/MyRunbook1"
],
 "detail": {
 "change-request-id": "d0585556-80f6-4522-8dad-dada6d45b67d",
 "change-request-title": "A change request title",
 "ops-item-id": "oi-12345abcdef",
 "ops-item-created-by": "arn:aws:iam::123456789012:user/JohnDoe",
 }
}
```

```

 "ops-item-created-time": "2024-10-24T10:50:33.180334Z",
 "ops-item-modified-by": "arn:aws:iam::123456789012:user/JohnDoe",
 "ops-item-modified-time": "2024-10-24T10:50:33.180340Z",
 "ops-item-status": "InProgress",
 "change-template-document-name": "MyChangeTemplate",
 "runbook-document-arn": "arn:aws:ssm:us-west-2:123456789012:document/MyRunbook1",
 "runbook-document-version": "1",
 "auto-approve": true,
 "approvers": [
 "arn:aws:iam::123456789012:user/JaneDoe"
]
 }
}

```

## Notifica di aggiornamento dello stato della richiesta di modifica - Esempio 2

```

{
 "version": "0",
 "id": "25ce6b03-2e4e-1a2b-2a8f-6c9de8d278d2",
 "detail-type": "Change Request Status Update",
 "source": "aws:ssm",
 "account": "123456789012",
 "time": "2024-10-24T10:51:52Z",
 "region": "us-east-1",
 "resources": [
 "arn:aws:ssm:us-west-2:123456789012:opsitem/oi-abcdef12345",
 "arn:aws:ssm:us-west-2:123456789012:document/MyRunbook1"
],
 "detail": {
 "change-request-id": "d0585556-80f6-4522-8dad-dada6d45b67d",
 "change-request-title": "A change request title",
 "ops-item-id": "oi-abcdef12345",
 "ops-item-created-by": "arn:aws:iam::123456789012:user/JohnDoe",
 "ops-item-created-time": "2024-10-24T10:50:33.180334Z",
 "ops-item-modified-by": "arn:aws:iam::123456789012:user/JohnDoe",
 "ops-item-modified-time": "2024-10-24T10:50:33.997163Z",
 "ops-item-status": "Rejected",
 "change-template-document-name": "MyChangeTemplate",
 "runbook-document-arn": "arn:aws:ssm:us-west-2:123456789012:document/MyRunbook1",
 "runbook-document-version": "1",
 "auto-approve": true,
 "approvers": [
 "arn:aws:iam::123456789012:user/JaneDoe"
]
 }
}

```

```
]
}
}
```

## AWS Systems Manager Eventi di conformità

Di seguito sono riportati alcuni esempi degli eventi relativi alla AWS Systems Manager conformità.

### Associazione conforme

```
{
 "version": "0",
 "id": "01234567-0123-0123-0123-012345678901",
 "detail-type": "Configuration Compliance State Change",
 "source": "aws.ssm",
 "account": "123456789012",
 "time": "2024-07-17T19:03:26Z",
 "region": "us-east-2",
 "resources": [
 "arn:aws:ssm:us-east-2:123456789012:managed-instance/i-01234567890abcdef"
],
 "detail": {
 "last-runtime": "2024-01-01T10:10:10Z",
 "compliance-status": "compliant",
 "resource-type": "managed-instance",
 "resource-id": "i-01234567890abcdef",
 "compliance-type": "Association"
 }
}
```

### Associazione Non-Compliant

```
{
 "version": "0",
 "id": "01234567-0123-0123-0123-012345678901",
 "detail-type": "Configuration Compliance State Change",
 "source": "aws.ssm",
 "account": "123456789012",
 "time": "2024-07-17T19:02:31Z",
 "region": "us-east-2",
 "resources": [
 "arn:aws:ssm:us-east-2:123456789012:managed-instance/i-01234567890abcdef"
],
```



```
"detail": {
 "last-runtime": "2024-01-01T10:10:10Z",
 "compliance-status": "non_compliant",
 "resource-type": "managed-instance",
 "resource-id": "i-01234567890abcdef",
 "compliance-type": "Association"
}
```

## Patch conforme

```
{
 "version": "0",
 "id": "01234567-0123-0123-0123-012345678901",
 "detail-type": "Configuration Compliance State Change",
 "source": "aws.123456789012",
 "account": "123456789012",
 "time": "2024-07-17T19:03:26Z",
 "region": "us-east-2",
 "resources": [
 "arn:aws:ssm:us-east-2:123456789012:managed-instance/i-01234567890abcdef"
],
 "detail": {
 "resource-type": "managed-instance",
 "resource-id": "i-01234567890abcdef",
 "compliance-status": "compliant",
 "compliance-type": "Patch",
 "patch-baseline-id": "PB789",
 "severity": "critical"
 }
}
```

## Patch Non-Compliant

```
{
 "version": "0",
 "id": "01234567-0123-0123-0123-012345678901",
 "detail-type": "Configuration Compliance State Change",
 "source": "aws.ssm",
 "account": "123456789012",
 "time": "2024-07-17T19:02:31Z",
 "region": "us-east-2",
 "resources": [
```

```

 "arn:aws:ssm:us-east-2:123456789012:managed-instance/i-01234567890abcdef"
],
 "detail": {
 "resource-type": "managed-instance",
 "resource-id": "i-01234567890abcdef",
 "compliance-status": "non_compliant",
 "compliance-type": "Patch",
 "patch-baseline-id": "PB789",
 "severity": "critical"
 }
}

```

## AWS Systems Manager Intervallo di manutenzione Eventi

Di seguito sono elencati alcuni esempi di eventi per Systems Manager Maintenance Windows.

### Registrazione di un target

I valori validi dello stato includono REGISTERED e DEREGISTERED.

```

{
 "version":"0",
 "id":"01234567-0123-0123-0123-0123456789ab",
 "detail-type":"Maintenance Window Target Registration Notification",
 "source":"aws.ssm",
 "account":"123456789012",
 "time":"2024-11-16T00:58:37Z",
 "region":"us-east-2",
 "resources":[
 "arn:aws:ssm:us-east-2:123456789012:maintenancewindow/mw-0ed7251d3fcf6e0c2",
 "arn:aws:ssm:us-east-2:123456789012:windowtarget/e7265f13-3cc5-4f2f-97a9-7d3ca86c32a6"
],
 "detail":{
 "window-target-id":"e7265f13-3cc5-4f2f-97a9-7d3ca86c32a6",
 "window-id":"mw-0ed7251d3fcf6e0c2",
 "status":"REGISTERED"
 }
}

```

### Tipo di esecuzione della finestra

I valori validi dello stato includono i seguenti elementi:

- CANCELLED
- CANCELLING
- FAILED
- IN\_PROGRESS
- PENDING
- SKIPPED\_OVERLAPPING
- SUCCESS TIMED\_OUT

```
{
 "version":"0",
 "id":"01234567-0123-0123-0123-0123456789ab",
 "detail-type":"Maintenance Window Execution State-change Notification",
 "source":"aws.ssm",
 "account":"123456789012",
 "time":"2025-06-02T14:52:18Z",
 "region":"us-east-2",
 "resources":[
 "arn:aws:ssm:us-east-2:123456789012:maintenancewindow/mw-0c50858d01EXAMPLE"
],
 "detail":{
 "start-time":"2025-06-02T14:48:28.039273Z",
 "end-time":"2025-06-02T14:52:18.083773Z",
 "window-id":"mw-0ed7251d3fcf6e0c2",
 "window-execution-id":"14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
 "status":"SUCCESS"
 }
}
```

### Tipo di esecuzione dell'attività

I valori validi dello stato includono IN\_PROGRESS, SUCCESS, FAILED e TIMED\_OUT.

```
{
 "version":"0",
 "id":"01234567-0123-0123-0123-0123456789ab",
 "detail-type":"Maintenance Window Task Execution State-change Notification",
 "source":"aws.ssm",
 "account":"123456789012",
 "time":"2025-06-02T14:52:18Z",
```

```

 "region": "us-east-2",
 "resources": [
 "arn:aws:ssm:us-east-2:123456789012:maintenancewindow/mw-0c50858d01EXAMPLE"
],
 "detail": {
 "start-time": "2025-06-02T14:48:28.039273Z",
 "task-execution-id": "6417e808-7f35-4d1a-843f-123456789012",
 "end-time": "2025-06-02T14:52:18.083773Z",
 "window-id": "mw-0ed7251d3fcf6e0c2",
 "window-execution-id": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
 "status": "SUCCESS"
 }
 }
}

```

## Attività del target elaborata

I valori validi dello stato includono IN\_PROGRESS, SUCCESS, FAILED e TIMED\_OUT.

```

{
 "version": "0",
 "id": "01234567-0123-0123-0123-0123456789ab",
 "detail-type": "Maintenance Window Task Target Invocation State-change Notification",
 "source": "aws:ssm",
 "account": "123456789012",
 "time": "2025-06-02T14:52:18Z",
 "region": "us-east-2",
 "resources": [
 "arn:aws:ssm:us-east-2:123456789012:maintenancewindow/mw-123456789012345678"
],
 "detail": {
 "start-time": "2025-06-02T14:48:28.039273Z",
 "end-time": "2025-06-02T14:52:18.083773Z",
 "window-id": "mw-0ed7251d3fcf6e0c2",
 "window-execution-id": "791b72e0-f0da-4021-8b35-f95dfEXAMPLE",
 "task-execution-id": "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE",
 "window-target-id": "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE",
 "status": "SUCCESS",
 "owner-information": "Owner"
 }
}

```

## Modifica dello stato della finestra

I valori validi dello stato includono ENABLED e DISABLED.

```
{
 "version": "0",
 "id": "01234567-0123-0123-0123-0123456789ab",
 "detail-type": "Maintenance Window State-change Notification",
 "source": "aws.ssm",
 "account": "123456789012",
 "time": "2024-11-16T00:58:37Z",
 "region": "us-east-2",
 "resources": [
 "arn:aws:ssm:us-east-2:123456789012:maintenancewindow/mw-0c50858d01EXAMPLE"
],
 "detail": {
 "window-id": "mw-0c50858d01EXAMPLE",
 "status": "DISABLED"
 }
}
```

## AWS Systems Manager Parameter Store Eventi

Di seguito sono elencati alcuni esempi di eventi per Systems Manager Parameter Store.

### Creazione di un parametro

```
{
 "version": "0",
 "id": "6a7e4feb-b491-4cf7-a9f1-bf3703497718",
 "detail-type": "Parameter Store Change",
 "source": "aws.ssm",
 "account": "123456789012",
 "time": "2024-05-22T16:43:48Z",
 "region": "us-east-2",
 "resources": [
 "arn:aws:ssm:us-east-2:123456789012:parameter/MyExampleParameter"
],
 "detail": {
 "operation": "Create",
 "name": "MyExampleParameter",
 "type": "String",
 "description": "Sample Parameter"
 }
}
```

```
}
```

## Aggiornamento di un parametro

```
{
 "version": "0",
 "id": "9547ef2d-3b7e-4057-b6cb-5fdf09ee7c8f",
 "detail-type": "Parameter Store Change",
 "source": "aws.ssm",
 "account": "123456789012",
 "time": "2024-05-22T16:44:48Z",
 "region": "us-east-2",
 "resources": [
 "arn:aws:ssm:us-east-2:123456789012:parameter/MyExampleParameter"
],
 "detail": {
 "operation": "Update",
 "name": "MyExampleParameter",
 "type": "String",
 "description": "Sample Parameter"
 }
}
```

## Eliminazione di parametro

```
{
 "version": "0",
 "id": "80e9b391-6a9b-413c-839a-453b528053af",
 "detail-type": "Parameter Store Change",
 "source": "aws.ssm",
 "account": "123456789012",
 "time": "2024-05-22T16:45:48Z",
 "region": "us-east-2",
 "resources": [
 "arn:aws:ssm:us-east-2:123456789012:parameter/MyExampleParameter"
],
 "detail": {
 "operation": "Delete",
 "name": "MyExampleParameter",
 "type": "String",
 "description": "Sample Parameter"
 }
}
```

```
}
```

## AWS Systems Manager OpsCenter Eventi

### Notifica di creazione di OpsCenter OpsItem

```
{
 "version": "0",
 "id": "aae66adc-7aac-f0c0-7854-7691e8c079b8",
 "detail-type": "OpsItem Create",
 "source": "aws.ssm",
 "account": "123456789012",
 "time": "2024-10-19T02:48:11Z",
 "region": "us-east-1",
 "resources": [
 "arn:aws:ssm:us-west-2:123456789012:opsitem/oi-123456abcdef"
],
 "detail": {
 "created-by": "arn:aws:iam::123456789012:user/JohnDoe",
 "created-time": "2024-10-19T02:46:53.629361Z",
 "source": "aws.ssm",
 "status": "Open",
 "ops-item-id": "oi-123456abcdef",
 "title": "An issue title",
 "ops-item-type": "/aws/issue",
 "description": "A long description may appear here"
 }
}
```

### Notifica di aggiornamento di OpsCenter OpsItem

```
{
 "version": "0",
 "id": "2fb5b168-b725-41dd-a890-29311200089c",
 "detail-type": "OpsItem Update",
 "source": "aws.ssm",
 "account": "123456789012",
 "time": "2024-10-19T02:48:11Z",
 "region": "us-east-1",
 "resources": [
 "arn:aws:ssm:us-west-2:123456789012:opsitem/oi-123456abcdef"
],
 "detail": {
```

```

 "created-by": "arn:aws:iam::123456789012:user/JohnDoe",
 "created-time": "2024-10-19T02:46:54.049271Z",
 "modified-by": "arn:aws:iam::123456789012:user/JohnDoe",
 "modified-time": "2024-10-19T02:46:54.337354Z",
 "source": "aws.ssm",
 "status": "Open",
 "ops-item-id": "oi-123456abcdef",
 "title": "An issue title",
 "ops-item-type": "/aws/issue",
 "description": "A long description may appear here"
 }
}

```

## AWS Systems Manager Run Command Eventi

### Run Command Status-change Notifica

```

{
 "version": "0",
 "id": "51c0891d-0e34-45b1-83d6-95db273d1602",
 "detail-type": "EC2 Command Status-change Notification",
 "source": "aws.ssm",
 "account": "123456789012",
 "time": "2024-07-10T21:51:32Z",
 "region": "us-east-2",
 "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-02573cafcfEXAMPLE"],
 "detail": {
 "command-id": "e8d3c0e4-71f7-4491-898f-c9b35bee5f3b",
 "document-name": "AWS-RunPowerShellScript",
 "expire-after": "2024-07-14T22:01:30.049Z",
 "parameters": {
 "executionTimeout": ["3600"],
 "commands": ["date"]
 },
 },
 "requested-date-time": "2024-07-10T21:51:30.049Z",
 "status": "Success"
}

```

### Run CommandNotifica di richiamo Status-change

```

{
 "version": "0",

```



```

 "id": "4780e1b8-f56b-4de5-95f2-95dbEXAMPLE",
 "detail-type": "EC2 Command Invocation Status-change Notification",
 "source": "aws.ssm",
 "account": "123456789012",
 "time": "2024-07-10T21:51:32Z",
 "region": "us-east-2",
 "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-02573cafcfEXAMPLE"],
 "detail": {
 "command-id": "e8d3c0e4-71f7-4491-898f-c9b35bee5f3b",
 "document-name": "AWS-RunPowerShellScript",
 "instance-id": "i-02573cafcfEXAMPLE",
 "requested-date-time": "2024-07-10T21:51:30.049Z",
 "status": "Success"
 }
 }
}

```

## AWS Systems Manager State Manager Eventi

### State Manager Modifica dello stato dell'associazione

```

{
 "version": "0",
 "id": "db839caf-6f6c-40af-9a48-25b2ae2b7774",
 "detail-type": "EC2 State Manager Association State Change",
 "source": "aws.ssm",
 "account": "123456789012",
 "time": "2024-05-16T23:01:10Z",
 "region": "us-east-2",
 "resources": [
 "arn:aws:ssm:us-east-2::document/AWS-RunPowerShellScript"
],
 "detail": {
 "association-id": "6e37940a-23ba-4ab0-9b96-5d0a1a05464f",
 "document-name": "AWS-RunPowerShellScript",
 "association-version": "1",
 "document-version": "Optional.empty",
 "targets": "[{\"key\": \"InstanceIds\", \"values\": [\"i-12345678\"]}]",
 "creation-date": "2024-02-13T17:22:54.458Z",
 "last-successful-execution-date": "2024-05-16T23:00:01Z",
 "last-execution-date": "2024-05-16T23:00:01Z",
 "last-updated-date": "2024-02-13T17:22:54.458Z",
 "status": "Success",
 "association-status-aggregated-count": "{\"Success\":1}",

```

```

 "schedule-expression":"cron(0 */30 * * * ? *)",
 "association-cwe-version":"1.0"
 }
}

```

## State Manager Modifica dello stato di associazione dell'istanza

```

{
 "version":"0",
 "id":"6a7e8feb-b491-4cf7-a9f1-bf3703467718",
 "detail-type":"EC2 State Manager Instance Association State Change",
 "source":"aws.ssm",
 "account":"123456789012",
 "time":"2024-02-23T15:23:48Z",
 "region":"us-east-2",
 "resources":[
 "arn:aws:ec2:us-east-2:123456789012:instance/i-12345678",
 "arn:aws:ssm:us-east-2:123456789012:document/my-custom-document"
],
 "detail":{
 "association-id":"34fcb7e0-9a14-4984-9989-0e04e3f60bd8",
 "instance-id":"i-02573cafcfEXAMPLE",
 "document-name":"my-custom-document",
 "document-version":"1",
 "targets":["{ \"key\": \"instanceids\", \"values\": [\"i-02573cafcfEXAMPLE\"] }"],
 "creation-date":"2024-02-23T15:23:48Z",
 "last-successful-execution-date":"2024-02-23T16:23:48Z",
 "last-execution-date":"2024-02-23T16:23:48Z",
 "status":"Success",
 "detailed-status":"",
 "error-code":"testErrorCode",
 "execution-summary":"testExecutionSummary",
 "output-url":"sampleurl",
 "instance-association-cwe-version":"1"
 }
}

```

## Scenari di esempio: obiettivi di Systems Manager nelle EventBridge regole di Amazon

Quando specifichi il target da invocare in una EventBridge regola Amazon, puoi scegliere tra oltre 20 tipi di target e aggiungere fino a cinque obiettivi a ciascuna regola.

Per le relative informazioni, consulta [Configurazione EventBridge per gli eventi di Systems Manager](#).

Tra i vari obiettivi, puoi scegliere tra Automazione eOpsCenter, che sono strumenti in Run Command AWS Systems Manager, come azioni mirate quando si verifica un EventBridge evento.

Di seguito sono riportati alcuni esempi di come è possibile utilizzare questi strumenti come obiettivo di una EventBridge regola.

### Esempi di automazione

È possibile configurare una EventBridge regola per avviare i flussi di lavoro di automazione quando si verificano eventi come i seguenti:

- Quando un CloudWatch allarme Amazon segnala che un nodo gestito non ha superato un controllo di stato (`StatusCheckFailed_Instance=1`), esegui il runbook di `AWSSupport-ExecuteEC2Rescue Automation` sul nodo.
- Quando un evento `EC2 Instance State-change Notification` si verifica perché è in esecuzione una nuova istanza Amazon Elastic Compute Cloud (Amazon EC2), eseguire il `AWS-AttachEBSVolume Runbook` di automazione sull'istanza.
- Quando viene creato e disponibile un volume Amazon Elastic Block Store (Amazon EBS), eseguire `AWS-CreateSnapshot runbook Automation` sul volume.

### OpsCenter esempi

Puoi configurare una EventBridge regola per crearne una nuova OpsItem quando si verificano incidenti come i seguenti:

- Problemi di prestazioni, ad esempio un evento di limitazione (della larghezza di banda della rete) per Amazon DynamoDB o prestazioni di volume ridotte di Amazon EBS.
- Un gruppo di Amazon EC2 Auto Scaling non riesce a lanciare un nodo o un flusso di lavoro di Systems Manager Automation non riesce.
- Un'istanza EC2 modifica lo stato da `Running` a `Stopped`.

### Run Command esempi

È possibile configurare una EventBridge regola per eseguire un documento Systems Manager Command Run Command quando si verificano eventi come i seguenti:

- Quando un gruppo Auto Scaling sta per terminare, uno script Run Command potrebbe acquisire i file di log dal nodo prima che venga terminato.
- Quando un nuovo nodo viene creato in un gruppo Auto Scaling, un'azione di destinazione Run Command può attivare il ruolo server Web o installare software sul nodo.
- Quando si scopre che un nodo gestito non è conforme, un'azione target Run Command potrebbe aggiornare le patch sul nodo eseguendo il documento AWS-RunPatchBaseline.

## Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS

Puoi configurare Amazon Simple Notification Service (Amazon SNS) per inviare notifiche sullo stato dei comandi inviati utilizzando Run Command o Maintenance Windows, che sono strumenti di AWS Systems Manager. Amazon SNS coordina e gestisce l'invio e la consegna delle notifiche ai clienti o agli endpoint che sono iscritti agli argomenti di Amazon SNS. È possibile ricevere una notifica ogni volta che un comando cambia di stato o passa a uno stato specifico, ad esempio Failed (Non riuscito) o Timed Out (Sottoposto a timeout). Quando si invia un comando a più nodi, è possibile ricevere una notifica per ciascuna copia del comando inviato a un determinato nodo. Ogni copia è denominata invocazione.

Amazon SNS può consegnare notifiche come HTTP o HTTPS POST, e-mail (SMTP, in testo normale o in formato JSON) oppure come messaggio inviato a una coda Amazon Simple Queue Service (Amazon SQS). Per ulteriori informazioni, consulta [Che cos'è Amazon SNS](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service. Per esempi della struttura dei dati JSON inclusi nella notifica Amazon SNS fornita da Run Command e Maintenance Windows, si veda [Esempi di notifiche Amazon SNS per AWS Systems Manager](#).

### Important

Prendi nota delle seguenti informazioni importanti.

- Gli argomenti FIFO di Amazon Simple Notification Service non sono supportati.
- Amazon Q Developer nelle applicazioni di chat non è supportato per il monitoraggio di Systems Manager con Amazon SNS. Se desideri utilizzare Amazon Q Developer nelle applicazioni di chat per monitorare Systems Manager, devi utilizzarlo con Amazon EventBridge. Per informazioni sul monitoraggio dell'utilizzo di Systems Manager EventBridge, consulta [Monitoraggio degli eventi di Systems Manager con Amazon](#)

[EventBridge](#). Per informazioni su Amazon EventBridge e Amazon Q Developer in chat applications, consulta [Tutorial: Creazione di una EventBridge regola che invia notifiche ad Amazon Q Developer in chat applications](#) nella Amazon Q Developer in chat applications Administrator Guide.

## Configura le notifiche Amazon SNS per AWS Systems Manager

Le attività di Run Command e Maintenance Windows registrate in una finestra di manutenzione possono inviare notifiche Amazon SNS relative alle attività del comando che passano negli stati seguenti:

- In Progress (In corso)
- Completato
- Non riuscito
- Timed Out (Timeout)
- Annullato

Per informazioni sulle condizioni che determinano il passaggio di un comando a uno di questi stati, si veda [Informazioni sugli stati dei comandi](#).

 **Note**

I comandi inviati mediante Run Command indicano anche gli stati In fase di eliminazione e In attesa. Questi stati non vengono acquisiti dalle notifiche Amazon SNS.

### Riepilogo dei comandi delle notifiche Amazon SNS

Se si configura Run Command o un'attività Run Command nella finestra di manutenzione per le notifiche Amazon SNS, Amazon SNS invia messaggi di riepilogo che includono le informazioni seguenti.

Campo	Tipo	Description
eventTime	Stringa	Ora di inizio dell'evento. Il timestamp è importante

Campo	Tipo	Description
		perché Amazon SNS non garantisce l'ordine di recapito dei messaggi. Esempio: 26/04/2016 T13:15:30Z
documentName	Stringa	Il nome del documento SSM usato per eseguire il comando.
commandId	Stringa	L'ID generato da Run Command dopo l'invio del comando.
expiresAfter	Data	Se si raggiunge questo istante prima che inizi l'esecuzione del comando, il comando non viene eseguito.
uscita S3BucketName	Stringa	Il bucket Amazon Simple Storage Service (Amazon S3) in cui devono essere archiviati e le risposte all'esecuzione del comando.
uscita S3KeyPrefix	Stringa	Il percorso della directory di Amazon S3 all'interno del bucket in cui devono essere archiviate le risposte all'esecuzione del comando.
richiesto DateTime	Stringa	Data e ora di invio della richiesta a questo nodo specifico.

Campo	Tipo	Description
instancelds	StringList	<p>I nodi a cui è destinato il comando.</p> <div> <p> <b>Note</b></p> <p>Gli ID di istanza sono inclusi nel messaggio di riepilogo solo se l'attività Run Command vi fa riferimento direttamente. Gli ID di istanza non sono inclusi nel messaggio di riepilogo se l'attività Run Command è stata eseguita con destinazioni basate su tag.</p> </div>
status	Stringa	Lo stato del comando.

## Invocation-based notifiche Amazon SNS

Se si invia un comando a più nodi, Amazon SNS può inviare messaggi relativi a ogni copia o chiamata del comando. I messaggi includono le informazioni riportate di seguito.

Campo	Tipo	Description
eventTime	Stringa	<p>Ora di inizio dell'evento.</p> <p>Il timestamp è importante perché Amazon SNS non garantisce l'ordine di recapito dei messaggi. Esempio: 26/04/2016 T13:15:30Z</p>

Campo	Tipo	Description
documentName	Stringa	Il nome del documento Systems Manager (document o SSM) usato per eseguire il comando.
richiesto DateTime	Stringa	Data e ora di invio della richiesta a questo nodo specifico.
commandId	Stringa	L'ID generato da Run Command dopo l'invio del comando.
instanceId	Stringa	L'istanza di destinazione per il comando.
status	Stringa	Lo stato del comando per questa invocazione.

Per configurare le notifiche di Amazon SNS quando un comando cambia di stato, eseguire le attività seguenti.

#### Note

Se non si sta configurando le notifiche Amazon SNS per la finestra di manutenzione, è possibile saltare l'attività 5 più avanti in questo argomento.

#### Argomenti

- [Attività 1: Creazione e iscrizione a un argomento Amazon SNS](#)
- [Attività 2: creazione di una policy IAM per le notifiche di Amazon SNS](#)
- [Attività 3: creazione di un ruolo IAM per le notifiche di Amazon SNS](#)
- [Attività 4: configurazione dell'accesso utente](#)
- [Attività 5: Associa la PassRole policy iam: al ruolo della finestra di manutenzione](#)



## Attività 1: Creazione e iscrizione a un argomento Amazon SNS

UnArgomento Amazon SNS è un canale di comunicazione che le attività Run Command e Run Command, registrate in una finestra di manutenzione, usano per inviare notifiche sullo stato dei comandi. Amazon SNS supporta diversi protocolli di comunicazione HTTP/S, tra cui e-mail e altri Servizi AWS come Amazon Simple Queue Service (Amazon SQS). Per iniziare rapidamente, consigliamo di scegliere il protocollo e-mail. Per ulteriori informazioni su come creare un argomento, consulta la pagina [Creazione di un argomento Amazon SNS](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service.

### Note

Dopo aver creato l'argomento, copiare o prendere nota del valore dell'ARN dell' argomento). Questo ARN dovrà essere specificato quando si invia un comando configurato per restituire le notifiche di stato.

Dopo aver creato l'argomento, effettuare la sottoscrizione specificando un Endpoint. Se si sceglie il protocollo e-mail, l'endpoint è l'indirizzo e-mail a cui si desidera ricevere le notifiche. Per ulteriori informazioni su come effettuare la sottoscrizione a un argomento, consultare [Sottoscrizione a un argomento di Amazon SNS](#) nella Guida per sviluppatori di Amazon Simple Notification Service.

Amazon SNS invia una e-mail di conferma da Notifiche AWS all'indirizzo e-mail specificato. Aprire la e-mail e selezionare il collegamento Confirm subscription (Conferma sottoscrizione).

Riceverai un messaggio di conferma da. AWS Amazon SNS è ora configurato per ricevere notifiche e inviare la notifica come e-mail all'indirizzo specificato.

## Attività 2: creazione di una policy IAM per le notifiche di Amazon SNS

Utilizza la seguente procedura per creare una policy personalizzata AWS Identity and Access Management (IAM) che fornisca le autorizzazioni per l'avvio delle notifiche Amazon SNS.

Per creare una policy IAM personalizzata per le notifiche di Amazon SNS

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, seleziona Policies (Policy) e Create Policy (Crea policy). (Se viene visualizzato il pulsante Get Started (Inizia), sceglierlo, quindi scegliere Create Policy (Crea policy)).

3. Scegliere la scheda JSON.
4. Sostituisci il contenuto predefinito con uno dei seguenti, a seconda che l'argomento Amazon SNS utilizzi la crittografia: AWS KMS

SNS topic not encrypted

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "sns:Publish"
],
 "Resource": "arn:aws:sns:us-east-1:111122223333:sns-topic-name"
 }
]
}
```

*region* rappresenta l'identificatore di una regione Regione AWS supportata da AWS Systems Manager, ad esempio *us-east-2* per la regione Stati Uniti orientali (Ohio). Per un elenco dei *region* valori supportati, vedere la colonna Regione negli endpoint [del servizio](#) Systems Manager in. Riferimenti generali di Amazon Web Services

*account-id* rappresenta l'identificatore a 12 cifre del tuo Account AWS, nel formato. 123456789012

*sns-topic-name* rappresenta il nome dell'argomento Amazon SNS che desideri utilizzare per la pubblicazione delle notifiche.

SNS topic encrypted

JSON

```
{
 "Version": "2012-10-17",
```

```

 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "sns:Publish"
],
 "Resource": "arn:aws:sns:us-east-1:111122223333:sns-topic-
name"
 },
 {
 "Effect": "Allow",
 "Action": [
 "kms:GenerateDataKey",
 "kms:Decrypt"
],
 "Resource": "arn:aws:kms:us-east-1:111122223333:key/kms-key-
id"
 }
]
 }
}

```

*region* rappresenta l'identificatore di una regione Regione AWS supportata da AWS Systems Manager, ad esempio *us-east-2* per la regione Stati Uniti orientali (Ohio). Per un elenco dei *region* valori supportati, vedere la colonna Regione negli endpoint [del servizio](#) Systems Manager in. Riferimenti generali di Amazon Web Services

*account-id* rappresenta l'identificatore a 12 cifre del tuo Account AWS, nel formato. 123456789012

*sns-topic-name* rappresenta il nome dell'argomento Amazon SNS che desideri utilizzare per la pubblicazione delle notifiche.

*kms-key-id* rappresenta l'ID della chiave KMS di crittografia simmetrica da utilizzare per crittografare e decrittografare l'argomento, nel AWS KMS formato. 1234abcd-12ab-34cd-56ef-12345EXAMPLE

 Note

L'utilizzo della crittografia è a pagamento. AWS KMS Per ulteriori informazioni, consulta [Gestire le chiavi e i costi di crittografia di Amazon SNS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

5. Scegli Successivo: Tag.
6. (Facoltativo) Aggiungere una o più coppie tag chiave-valore per organizzare, monitorare o controllare l'accesso per questa policy.
7. Scegli Prossimo: Rivedi.
8. Nella pagina Rivedi policy, per Nome inserisci un nome per la policy in linea. Ad esempio: **my-sns-publish-permissions**.
9. (Facoltativo) In Description (Descrizione), inserire una descrizione per la policy.
10. Scegliere Create Policy (Crea policy).

### Attività 3: creazione di un ruolo IAM per le notifiche di Amazon SNS

La seguente procedura consente di creare un ruolo IAM per le notifiche di Amazon SNS. Questo ruolo di servizio viene utilizzato da Systems Manager per avviare le notifiche Amazon SNS. In tutte le procedure successive, questo ruolo viene chiamato ruolo IAM Amazon SNS.

Per creare un ruolo di servizio IAM per le notifiche di Amazon SNS

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione della console IAM, scegliere Ruoli e quindi Crea ruolo.
3. Scegli il tipo di ruolo Servizio AWS, quindi scegli Systems Manager.
4. Scegli il caso d'uso Systems Manager. Quindi, seleziona Successivo.
5. Nella pagina Attach permissions policies (Collega policy di autorizzazioni), selezionare la casella a sinistra del nome della policy personalizzata creata nell'attività 2. Ad esempio: **my-sns-publish-permissions**.
6. (Facoltativo) Impostare un [limite delle autorizzazioni](#). Questa è una funzionalità avanzata disponibile per i ruoli di servizio, ma non per i ruoli collegati ai servizi.

Apri la sezione Permissions boundary (Limite delle autorizzazioni) e scegli Use a permissions boundary to control the maximum role permissions (Usa un limite delle autorizzazioni per controllare il numero massimo di autorizzazioni del ruolo). IAM include un elenco delle politiche AWS gestite e gestite dal cliente nel tuo account. Selezionare la policy da utilizzare per il limite delle autorizzazioni o scegliere Crea policy per aprire una nuova scheda del browser e creare una nuova policy da zero. Per ulteriori informazioni, consulta [Creating IAM policies](#) nella Guida per l'utente di IAM. Dopo aver creato la policy, chiudi la scheda e torna alla scheda originale per selezionare la policy da utilizzare per il limite delle autorizzazioni.

7. Scegli Avanti.
8. Se possibile, specifica un nome del ruolo o un suffisso del nome del ruolo per facilitare l'identificazione dello scopo del ruolo. I nomi dei ruoli devono essere univoci all'interno dell'Account AWS. Non si distinguono per caso. Ad esempio, non è possibile creare ruoli denominati sia **PRODRROLE** che **prodrole**. Poiché varie entità possono fare riferimento al ruolo, non è possibile modificare il nome del ruolo dopo averlo creato.
9. (Facoltativo) In Descrizione, inserisci una descrizione per il nuovo ruolo.
10. Scegli Modifica nelle sezioni Fase 1: seleziona le entità attendibili o Fase 2: seleziona autorizzazioni per modificare i casi d'uso e le autorizzazioni per il ruolo.
11. (Facoltativo) Aggiungi metadati all'utente collegando i tag come coppie chiave-valore. Per ulteriori informazioni sull'utilizzo di tag in IAM, consulta la sezione [Applicazione di tag alle risorse IAM](#) nella Guida per l'utente di IAM.
12. Rivedere il ruolo e scegliere Crea ruolo.
13. Selezionare il nome del ruolo, quindi copiare o annotare quanto indicato in Role ARN (ARN ruolo). Questo Amazon Resource Name (ARN) per il ruolo viene utilizzato quando si invia un comando configurato per restituire le notifiche Amazon SNS.
14. Tenere aperta la pagina Riepilogo.

## Attività 4: configurazione dell'accesso utente

Se a un'entità IAM (utente, ruolo o gruppo) vengono assegnate le autorizzazioni di amministratore, l'utente o il ruolo hanno l'accesso a Run Command e Maintenance Windows, strumenti di AWS Systems Manager.

Per le entità senza autorizzazioni di amministratore, un amministratore deve concedere le seguenti autorizzazioni all'entità IAM:

- La policy gestita AmazonSSMFullAccess o una policy che fornisce autorizzazioni analoghe.
- Le autorizzazioni iam:PassRole per il ruolo creato in [Attività 3: creazione di un ruolo IAM per le notifiche di Amazon SNS](#). Ad esempio:

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": "iam:PassRole",
 "Resource": "arn:aws:iam::111122223333:role/sns-role-name",
 "Condition": {
 "StringEquals": {
 "iam:PassedToService": "ssm.amazonaws.com"
 }
 }
 }
]
}
```

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 configurare l'accesso degli utenti e allegare la PassRole **policy** iam: a un account utente

1. Nel riquadro di navigazione IAM, selezionare Utenti, quindi selezionare l'account utente che si desidera configurare.
2. Nella scheda Autorizzazioni dell'elenco delle policy, verificare che sia presente la policy **AmazonSSMFullAccess** o una policy equivalente che assegni all'account le autorizzazioni di accesso a Systems Manager.
3. Scegliere Add inline policy (Aggiungi policy inline).
4. Nella pagina Create Policy (Crea policy), scegliere la scheda Visual editor (Editor visivo).
5. Selezionare Choose a service (Scegli un servizio) e quindi IAM..
6. Per Azioni, nella casella di testo Filtra azioni, inserisci **PassRole**, quindi seleziona la casella di controllo accanto a PassRole.
7. Per Resources (Risorse), verificare che l'opzione Specific (Specifico) sia selezionata, quindi scegliere Add ARN (Aggiungi ARN).
8. Nel campo Specify ARN for role (Specifica ARN per il ruolo), incollare l'ARN del ruolo IAM Amazon SNS copiato alla fine dell'attività 3. Il sistema popola automaticamente i campi Account e Role name with path (Nome ruolo con percorso).
9. Scegliere Add (Aggiungi).
10. Scegliere Review policy (Rivedi policy).
11. Nella pagina Review Policy (Rivedi policy), inserire un nome, quindi scegliere Create Policy (Crea policy).

## Attività 5: Associa la PassRole policy iam: al ruolo della finestra di manutenzione

Quando si registra un'attività Run Command con una finestra di manutenzione, occorre specificare un Amazon Resource Name (ARN) del ruolo di servizio. Questo ruolo di servizio viene utilizzato da Systems Manager per l'esecuzione di attività registrate nella finestra di manutenzione. Per configurare le notifiche Amazon SNS per un'attività registrata Run Command, collegare una policy **iam:PassRole** al ruolo di servizio della finestra specificato. Se non si intende configurare l'attività registrata per le notifiche Amazon SNS, questa attività può essere ignorata.

La policy `iam:PassRole` consente al ruolo di servizio Maintenance Windows di passare il ruolo IAM Amazon SNS creato nell'attività 3 al servizio Amazon SNS. La procedura seguente mostra come collegare la policy `iam:PassRole` al ruolo di servizio Maintenance Windows.

#### Note

Per inviare notifiche correlate alle attività Run Command registrate, occorre utilizzare un ruolo di servizio personalizzato per la finestra di manutenzione. Per informazioni, consultare [Configurazione Intervallo di manutenzione](#).

Se hai bisogno di creare un ruolo di servizio personalizzato per le attività della finestra di manutenzione, consulta la sezione [Configurazione Intervallo di manutenzione](#).

Per allegare la PassRole **policy** iam: alla tua Intervallo di manutenzione role

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, selezionare Roles (Ruoli) e selezionare il ruolo IAM Amazon SNS creato nell'attività 3.
3. Copiare o annotare l'ARN del ruolo e tornare alla sezione Roles (Ruoli) della console IAM.
4. Selezionare il ruolo di servizio personalizzato Maintenance Windows creato dall'elenco Nome ruolo.
5. Nella scheda Autorizzazioni, verifica che la policy AmazonSSMMaintenanceWindowRole sia elencata o che ce ne sia una analoga che conceda l'autorizzazione alle finestre di manutenzione per l'API di Systems Manager. In caso contrario, scegli Aggiungi autorizzazioni, Collega policy per collegarla.
6. Scegli Add permissions, Create inline policy (Aggiungi autorizzazioni, Crea policy inline).
7. Scegliere la scheda Visual Editor (Editor visivo).
8. In Service (Servizio) scegliere IAM.
9. Per Azioni, nella casella di testo Filtra azioni, inserisci **PassRole**, quindi seleziona la casella di controllo accanto a PassRole.
10. Per Resources (Risorse), scegliere Specific (Specifico), quindi scegliere Add ARN (Aggiungi ARN).
11. Nella casella Specify ARN for role (Specifica ARN per ruolo), incollare l'ARN del ruolo IAM Amazon SNS creato nell'attività 3 e quindi scegliere Add (Aggiungi).
12. Scegliere Esamina policy.



13. Nella pagina Rivedi policy, specifica un nome per la policy PassRole, quindi scegli Crea policy.

## Esempi di notifiche Amazon SNS per AWS Systems Manager

Puoi configurare Amazon Simple Notification Service (Amazon SNS) per inviare notifiche sullo stato dei comandi inviati utilizzando Run Command o Maintenance Windows, che sono strumenti di AWS Systems Manager.

### Note

In questa guida non viene spiegato come configurare le notifiche per Run Command o la Maintenance Windows. Per ulteriori informazioni sulla configurazione di Run Command o della Maintenance Windows per inviare notifiche Amazon SNS sullo stato dei comandi, consultare [Configura le notifiche Amazon SNS per AWS Systems Manager](#).

Gli esempi seguenti illustrano la struttura dell'output JSON restituito dalle notifiche Amazon SNS quando sono configurate per Run Command o la Maintenance Windows.

Esempio di output JSON per i messaggi di riepilogo dei comandi che utilizzano la definizione dell'ID di istanza

```
{
 "commandId": "a8c7e76f-15f1-4c33-9052-0123456789ab",
 "documentName": "AWS-RunPowerShellScript",
 "instanceIds": [
 "i-1234567890abcdef0",
 "i-9876543210abcdef0"
],
 "requestedDateTime": "2019-04-25T17:57:09.17Z",
 "expiresAfter": "2019-04-25T19:07:09.17Z",
 "outputS3BucketName": "amzn-s3-demo-bucket",
 "outputS3KeyPrefix": "runcommand",
 "status": "InProgress",
 "eventTime": "2019-04-25T17:57:09.236Z"
}
```

Esempio di output JSON per i messaggi di riepilogo dei comandi che utilizzano la definizione delle destinazioni con tag

```
{
 "commandId": "9e92c686-ddc7-4827-b040-0123456789ab",
 "documentName": "AWS-RunPowerShellScript",
 "instanceIds": [],
 "requestedDateTime": "2019-04-25T18:01:03.888Z",
 "expiresAfter": "2019-04-25T19:11:03.888Z",
 "outputS3BucketName": "",
 "outputS3KeyPrefix": "",
 "status": "InProgress",
 "eventTime": "2019-04-25T18:01:05.825Z"
}
```

Esempio di output JSON per i messaggi di chiamata

```
{
 "commandId": "ceb96b84-16aa-4540-91e3-925a9a278b8c",
 "documentName": "AWS-RunPowerShellScript",
 "instanceId": "i-1234567890abcdef0",
 "requestedDateTime": "2019-04-25T18:06:05.032Z",
 "status": "InProgress",
 "eventTime": "2019-04-25T18:06:05.099Z"
}
```

## Utilizzo Run Command per inviare un comando che restituisce notifiche di stato

Le procedure seguenti mostrano come utilizzare la AWS Command Line Interface (AWS CLI) o la AWS Systems Manager console per inviare un comando Run Command, configurata per restituire notifiche di stato.

### Invio di un Run Command che restituisce notifiche (console)

Utilizzare la procedura seguente per inviare un comando tramite Run Command, configurato per restituire le notifiche di stato con la console del Systems Manager.

Per inviare un comando che restituisca le notifiche (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli Run Command.

3. Seleziona Esegui comando.
4. Nell'elenco Command document (Documento comando), scegliere un documento di Systems Manager.
5. Nella sezione Command parameters (Parametri di comando) specificare i valori per i parametri necessari.
6. In Destinazioni, scegli i nodi gestiti in cui si desidera eseguire questa operazione specificando i tag, selezionando le istanze o i dispositivi edge manualmente o indicando un gruppo di risorse.

 Tip

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

7. In Altri parametri:
  - In Commento, digita le informazioni su questo comando.
  - In Timeout (secondi), specifica il numero di secondi che il sistema dovrà attendere prima di generare un errore per l'intera esecuzione del comando.
8. Per Controllo velocità:
  - In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti presi di mira, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.

9. (Facoltativo) Nella sezione Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Scrivi l'output del comando in un bucket S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

 Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

10. Nella sezione SNS Notifications (Notifiche SNS) scegliere Enable SNS notifications (Abilita le notifiche SNS).
11. In IAM role (Ruolo IAM), scegliere l'ARN del ruolo IAM Amazon SNS creato nell'attività 3 in [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).
12. In SNS topic (Argomento SNS) immettere l'ARN dell'argomento Amazon SNS da utilizzare.
13. Nel campo Event notifications (Notifiche eventi) scegliere gli eventi per cui si vogliono ricevere le notifiche.
14. In Notifiche di modifiche, scegli di ricevere notifiche solo per il riepilogo del comando (Modifica dello stato del comando) o per ogni copia di un comando inviata a più nodi (Modifica dello stato del comando su ogni istanza).
15. Scegli Esegui.
16. Controllare la propria e-mail per verificare di aver ricevuto un messaggio da Amazon SNS e aprire il messaggio e-mail. Amazon SNS può richiedere diversi minuti per inviare il messaggio e-mail.

## Invio di un Run Command che restituisce notifiche (CLI)

Utilizzare la procedura seguente per inviare un comando tramite Run Command configurato per restituire le notifiche di stato con AWS CLI.

Per inviare un comando che restituisca le notifiche (CLI)

1. Apri il. AWS CLI
2. Specificare i parametri nel comando seguente per definire le destinazioni in base agli ID dei nodi gestiti.

```
aws ssm send-command --instance-ids "ID-1, ID-2" --document-name "Name"
--parameters '{"commands":["input"]}' --service-role "SNSRoleARN" --
notification-config '{"NotificationArn":"SNSTopicName","NotificationEvents":
["All"],"NotificationType":"Command"}
```

Di seguito è riportato un esempio.

```
aws ssm send-command --instance-ids "i-02573cafcfEXAMPLE, i-0471e04240EXAMPLE"
--document-name "AWS-RunPowerShellScript" --parameters '{"commands":
["Get-Process"]}' --service-role "arn:aws:iam::111122223333:role/
SNS_Role" --notification-config '{"NotificationArn":"arn:aws:sns:us-
east-1:111122223333:SNSTopic","NotificationEvents":
["All"],"NotificationType":"Command"}
```

### Comandi alternativi

Specificare i parametri nel comando seguente per definire le destinazioni delle istanze gestite tramite i tag.

```
aws ssm send-command --targets "Key=tag:TagName,Values=TagKey" --document-name
"Name" --parameters '{"commands":["input"]}' --service-role "SNSRoleARN" --
notification-config '{"NotificationArn":"SNSTopicName","NotificationEvents":
["All"],"NotificationType":"Command"}
```

Di seguito è riportato un esempio.

```
aws ssm send-command --targets "Key=tag:Environment,Values=Dev" --
document-name "AWS-RunPowerShellScript" --parameters '{"commands":
["Get-Process"]}' --service-role "arn:aws:iam::111122223333:role/
SNS_Role" --notification-config '{"NotificationArn":"arn:aws:sns:us-
east-1:111122223333:SNSTopic","NotificationEvents":
["All"],"NotificationType":"Command"}
```

3. Premere Invio.

4. Controllare la propria e-mail per verificare di aver ricevuto un messaggio da Amazon SNS e aprire il messaggio e-mail. Amazon SNS può richiedere diversi minuti per inviare il messaggio e-mail.

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

## Utilizzare una finestra di manutenzione per inviare un comando che restituisca notifiche di stato

Le seguenti procedure mostrano come registrare un'Run Commandattività nella finestra di manutenzione utilizzando la AWS Systems Manager console o il AWS Command Line Interface (AWS CLI). Run Commandè uno strumento in AWS Systems Manager. Le procedure descrivono anche come configurare l'attività Run Command per restituire notifiche di stato.

Prima di iniziare

Se non sono state create una finestra di manutenzione o delle destinazioni registrate, consultare [Crea e gestisci finestre di manutenzione utilizzando la console](#) per i passi su come creare una finestra di manutenzione e registrare le destinazioni.

Per ricevere notifiche dal servizio Amazon Simple Notification Service (Amazon SNS), occorre collegare una policy `iam:PassRole` al ruolo di servizio della Maintenance Windows specificato nell'attività registrata. Se non non si sono aggiunte autorizzazioni `iam:PassRole` al ruolo di servizio delle Maintenance Windows, consultare [Attività 5: Associa la PassRole policy iam: al ruolo della finestra di manutenzione](#).

## Registrazione di un'attività Run Command in una finestra di manutenzione che restituisce notifiche (console)

Utilizzare la procedura seguente per registrare un'attività Run Command configurata per restituire notifiche di stato nella finestra di manutenzione con la console di Systems Manager.

Per registrare un'attività Run Command nella finestra di manutenzione che restituisce notifiche (console)

1. Apri la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.

2. Nel pannello di navigazione, scegli Maintenance Windows.
3. Selezionare la finestra di manutenzione per la quale si desidera registrare un'attività Run Command configurata per inviare notifiche Amazon Simple Notification Service (Amazon SNS).
4. Scegliere Actions (Operazioni) e successivamente Register Run command task (Registra attività di esecuzione comando).
5. (Facoltativo) Nel campo Name (Nome), inserire un nome per l'attività.
6. (Facoltativo) Specificare una descrizione nel campo Description (Descrizione).
7. In Command document (Documento comando), scegliere un documento comando.
8. In Task priority (Priorità attività), specificare una priorità per questa attività. Zero (0) indica la priorità più elevata. Le attività in una finestra di manutenzione sono programmate in ordine di priorità. Le attività con la stessa priorità vengono pianificate in parallelo.
9. Nella sezione Targets, selezionare un gruppo target registrato o selezionare target non registrati.
10. In Controllo velocità:
  - In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti come target, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che elaborano ancora il comando potrebbero inviare errori.
11. Nell'area Ruolo di servizio IAM, seleziona il ruolo di servizio Maintenance Windows che ha autorizzazioni `iam:PassRole` per il ruolo SNS.

 Note

Aggiungere autorizzazioni `iam:PassRole` al ruolo Maintenance Windows per consentire a Systems Manager di passare il ruolo SNS ad Amazon SNS. Se le autorizzazioni `iam:PassRole` non sono state aggiunte, consultare l'attività 5 nell'argomento

### Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS.

12. (Facoltativo) In Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Abilita output di scrittura in S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

#### Note

Le autorizzazioni S3 che consentono di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza assegnate al nodo gestito e non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova in un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato all'istanza disponga delle autorizzazioni necessarie per scrivere su quel bucket.

13. Nella sezione SNS notifications (Notifiche SNS), procedere come segue:
- Scegliere Enable SNS Notifications (Abilita notifiche SNS).
  - In IAM role (Ruolo IAM), scegliere l'Amazon Resource Name (ARN) del ruolo IAM Amazon SNS creato nell'attività 3 in [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#) per avviare Amazon SNS.
  - In SNS topic (Argomento SNS) immettere l'ARN dell'argomento Amazon SNS da utilizzare.
  - In Event type (Tipo di evento), scegliere gli eventi per i quali si desidera ricevere notifiche.
  - In Change notifications (Cambia notifiche) specificare se si vogliono ricevere notifiche per ogni copia di un comando inviato a più nodi (invocazioni) o il riepilogo del comando.
14. Nella sezione Parameters (Parametri), immettere i parametri necessari in base al documento del comando scelto.
15. Scegliere Register run command task (Registra attività di esecuzione comandi).
16. Dopo la successiva esecuzione della finestra di manutenzione, controllare la e-mail per verificare di aver ricevuto un messaggio da Amazon SNS e aprire il messaggio e-mail. Amazon SNS può richiedere diversi minuti per inviare il messaggio e-mail.



## Registrazione di un'attività Run Command in una finestra di manutenzione che restituisce notifiche (CLI)

Utilizzare la procedura seguente per registrare un'attività Run Command configurata per restituire le notifiche di stato alla finestra di manutenzione con AWS CLI.

Come registrare un'attività Run Command nella finestra di manutenzione che restituisce le notifiche (CLI)

### Note

Per gestire meglio le opzioni delle attività, questa procedura utilizza l'opzione di comando `--cli-input-json`, con i valori delle opzioni archiviati in un file JSON.

1. Nel computer locale, creare un file denominato `RunCommandTask.json`.
2. Incollare i contenuti seguenti nel file.

```
{
 "Name": "Name",
 "Description": "Description",
 "WindowId": "mw-0c50858d01EXAMPLE",
 "ServiceRoleArn": "arn:aws:iam::account-id:role/MaintenanceWindowIAMRole",
 "MaxConcurrency": "1",
 "MaxErrors": "1",
 "Priority": 3,
 "Targets": [
 {
 "Key": "WindowTargetIds",
 "Values": [
 "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
]
 }
],
 "TaskType": "RUN_COMMAND",
 "TaskArn": "CommandDocumentName",
 "TaskInvocationParameters": {
 "RunCommand": {
 "Comment": "Comment",
 "TimeoutSeconds": 3600,
 "NotificationConfig": {
```

```

 "NotificationArn": "arn:aws:sns:region:account-id:SNSTopicName",
 "NotificationEvents": [
 "All"
],
 "NotificationType": "Command"
 },
 "ServiceRoleArn": "arn:aws:iam::account-id:role/SNSIAMRole"
}
}
}

```

3. Sostituire i valori di esempio con le informazioni relative alle proprie risorse.

È anche possibile ripristinare le opzioni omesse in questo esempio se si desidera utilizzarle. Ad esempio, è possibile salvare l'output del comando in un bucket S3.

Per ulteriori informazioni, consulta [register-task-with-maintenance-window](#) nella documentazione di riferimento dei comandi della AWS CLI .

4. Salvare il file.
5. Nella directory sul computer locale in cui è stato salvato il file, eseguire questo comando.

```
aws ssm register-task-with-maintenance-window --cli-input-json file://
RunCommandTask.json
```

#### Important

Assicurarsi di includere `file://` prima del nome del file. Questo è obbligatorio in questo comando.

Se il comando viene eseguito correttamente, restituisce informazioni simili alle seguenti.

```

{
 "WindowTaskId": "j2l8d5b5c-mw66-tk4d-r3g9-1d4d1EXAMPLE"
}

```

6. Dopo la successiva esecuzione della finestra di manutenzione, controllare la e-mail per verificare di aver ricevuto un messaggio da Amazon SNS e aprire il messaggio e-mail. Amazon SNS può richiedere diversi minuti per inviare il messaggio e-mail.

Per ulteriori informazioni sulla registrazione delle attività per una finestra di manutenzione dalla riga di comando, consultare [Register tasks with the maintenance window \(Registrare le operazioni con la finestra di manutenzione\)](#).

# Integrazioni di prodotti e servizi con Systems Manager

Per impostazione predefinita, AWS Systems Manager si integra con Servizi AWS altri prodotti e servizi. Le informazioni seguenti possono essere utili per configurare Systems Manager per l'integrazione con i prodotti e i servizi utilizzati.

- [Integrazione con Servizi AWS](#)
- [Integrazione con altri prodotti e servizi](#)

## Integrazione con Servizi AWS

Tramite l'uso dei documenti Systems Manager Command (documenti SSM) e dei runbook di Automation, è possibile utilizzarli AWS Systems Manager per l'integrazione con. Servizi AWS Per ulteriori informazioni su queste risorse, vedere [AWS Systems Manager Documenti di](#).

Questa sezione contiene gli argomenti seguenti.

- [Utilizzo Parameter Store parametri in Amazon Elastic Kubernetes Service](#)
- [Esecuzione Ansible Playbook di GitHub](#)
- [Esegui script Python da GitHub](#)
- [Installa ASCP per Amazon EKS](#)
- [AWS Segreti ed esempi di codice del provider di configurazione](#)

Systems Manager è integrato con quanto segue. Servizi AWS

## Calcolo

Servizio	Description
Amazon Elastic Compute Cloud (Amazon EC2)	<a href="#">Amazon EC2</a> fornisce capacità di elaborazione scalabili in Cloud AWS. L'utilizzo di Amazon EC2 elimina la necessità di investire in hardware sin dall'inizio. Potrai quindi sviluppare e distribuire le applicazioni più velocemente. Puoi utilizzare Amazon EC2 per avviare il

Servizio	Description
	<p>numero di server virtuali necessari, configurare la sicurezza e i servizi di rete, nonché gestire l'archiviazione.</p> <p>Systems Manager consente di eseguire diverse attività sulle istanze EC2. Ad esempio, è possibile avviare, configurare, gestire, eseguire il mantenimento, risolvere i problemi e connettersi in modo sicuro alle istanze EC2. È inoltre possibile utilizzare Systems Manager per distribuire software, determinare lo stato di conformità e raccogliere l'inventario dalle istanze EC2.</p> <p>Ulteriori informazioni</p> <ul style="list-style-type: none"><li>• <a href="#">Utilizzo dei nodi gestiti</a></li><li>• <a href="#">AWS Systems Manager State Manager</a></li><li>• <a href="#">AWS Systems Manager Run Command</a></li><li>• <a href="#">AWS Systems Manager Patch Manager</a></li><li>• <a href="#">AWS Systems Manager Session Manager</a></li><li>• <a href="#">AWS Systems Manager Distributor</a></li><li>• <a href="#">AWS Systems Manager Conformità</a></li><li>• <a href="#">AWS Systems Manager Inventory</a></li></ul>

Servizio	Description
Amazon EC2 Auto Scaling	<p><a href="#">Auto Scaling</a> consente di assicurarsi di avere a disposizione il numero corretto di istanze EC2 per gestire il carico dell'applicazione. È possibile creare raccolte di istanze EC2, denominate gruppi con dimensionamento automatico.</p> <p>Systems Manager consente di automatizzare procedure comuni come l'applicazione di patch alla Amazon Machine Image (AMI) utilizzata nel modello Auto Scaling per il gruppo Auto Scaling.</p> <p>Ulteriori informazioni</p> <p><a href="#">Aggiornamento in corso AMI per gruppi Auto Scaling</a></p>
Amazon Elastic Container Service (Amazon ECS)	<p><a href="#">Amazon ECS</a> è un servizio rapido e altamente scalabile di gestione dei container che consente di eseguire, arrestare e gestire container Docker in un cluster.</p> <p>Systems Manager consente di gestire le istanze dei container in remoto e di inserire dati sensibili nei contenitori. Archivia i dati sensibili in Parameter Store parametri e fai riferimento ad essi nella definizione del contenitore.</p> <p>Ulteriori informazioni</p> <ul style="list-style-type: none"><li>• <a href="#">Gestione remota delle istanze di container mediante AWS Systems Manager</a></li><li>• <a href="#">Specifica dei dati sensibili mediante Systems ManagerParameter Store</a></li></ul>

Servizio	Description
AWS Lambda	<p><a href="#">Lambda</a> è un servizio di elaborazione che consente di eseguire codice senza fornire o gestire server. Lambda esegue il codice solo quando è necessario e si dimensiona automaticamente, da poche richieste al giorno a migliaia al secondo.</p> <p>Systems Manager consente di utilizzare le funzioni Lambda all'interno del contenuto del runbook di Automation utilizzando l'azione. <code>aws:invokeLambdaFunction</code></p> <p>Per utilizzare i parametri AWS Lambda delle funzioni Parameter Store in, è possibile utilizzare e l'estensione Lambda AWS Parameters and Secrets per recuperare i valori dei parametri e memorizzarli nella cache per un uso futuro.</p> <p>Ulteriori informazioni</p> <p><a href="#">Aggiorna un golden AMI utilizzando l'automazione, AWS Lambda e Parameter Store</a></p> <p><a href="#">Utilizzo Parameter Store parametri in AWS Lambda funzioni</a></p>

## Internet of Things (IoT)

Servizio	Description
AWS IoT Greengrass dispositivi principali	<p><a href="#">AWS IoT Greengrass</a> è un servizio di runtime edge IoT open source e cloud che ti aiuta a creare, distribuire e gestire applicazioni IoT sui tuoi dispositivi. Systems Manager offre</p>

Servizio	Description
	<p>supporto nativo per i dispositivi AWS IoT Greengrass principali.</p> <p>Ulteriori informazioni</p> <p><a href="#">Gestione dei dispositivi edge con Systems Manager</a></p>
AWS IoT dispositivi principali	<p><a href="#">AWS IoT</a> fornisce i servizi cloud che connettono i dispositivi IoT ad altri dispositivi e servizi AWS cloud. AWS IoT fornisce un software per dispositivi che può aiutarti a integrare i tuoi dispositivi IoT in soluzioni AWS IoT basate. Se i tuoi dispositivi sono in grado di connettersi a AWS IoT, AWS IoT puoi collegarli ai servizi cloud AWS forniti. Systems Manager supporta i dispositivi AWS IoT principali purché tali dispositivi siano configurati come nodi gestiti in un ambiente <a href="#">ibrido e multicloud</a>.</p> <p>Ulteriori informazioni</p> <p><a href="#">Gestione dei nodi in ambienti ibridi e multicloud con Systems Manager</a></p>

## Archiviazione

Servizio	Description
Amazon Simple Storage Service (Amazon S3)	<p><a href="#">Amazon S3</a> è un servizio di storage su Internet. È concepito per rendere più accessibili agli sviluppatori risorse informatiche su grande scala per il Web. Amazon S3 dispone di una semplice interfaccia web service che consente di archiviare e recuperare qualsiasi quantità</p>



Servizio	Description
	<p>di dati, in qualunque momento e ovunque sul Web.</p> <p>Systems Manager consente di eseguire script remoti e documenti SSM archiviati in Amazon S3. Distributor utilizza Amazon S3 per archiviare e i pacchetti. Puoi anche inviare output ad Amazon S3 per Run Command e Session Manager, strumenti di AWS Systems Manager.</p> <p>Ulteriori informazioni</p> <ul style="list-style-type: none"><li>• <a href="#">Esecuzione di script da Amazon S3</a></li><li>• <a href="#">Esecuzione di documenti da posizioni remote</a></li><li>• <a href="#">AWS Systems Manager Distributor</a></li><li>• <a href="#">Registrazione dei dati delle sessioni mediante Amazon S3 (console)</a></li></ul>

## Strumenti per developer

Servizio	Description
AWS CodeBuild	<p><a href="#">CodeBuild</a> è un servizio di compilazione completamente gestito nel cloud. CodeBuild compila il codice sorgente, esegue test unitari e produce artefatti pronti per l'implementazione. CodeBuild elimina la necessità di fornire, gestire e scalare i propri server di compilazione.</p> <p>Parameter Store consente di archiviare informazioni riservate relative alle specifiche e ai progetti di costruzione.</p>

Servizio	Description
	<p>Ulteriori informazioni</p> <ul style="list-style-type: none"> <li>• <a href="#">Riferimento alle specifiche di costruzione per CodeBuild</a></li> <li>• <a href="#">Crea un progetto di compilazione in AWS CodeBuild</a></li> </ul>
AWS CDK	<p>AWS Cloud Development Kit (AWS CDK) È un framework per definire l'infrastruttura cloud come codice, con linguaggi di programmazione, e distribuirla tramite AWS CloudFormation.</p> <p>Application Manager consente di visualizzare i costrutti CDK raggruppati come applicazioni, visualizzare la struttura dell'applicazione, comprese le risorse sottostanti, visualizzare gli avvisi, analizzare e risolvere i problemi operativi e tenere traccia dei costi nella console.</p> <p>Application Manager</p> <p>Ulteriori informazioni</p> <ul style="list-style-type: none"> <li>• <a href="#">Visualizzazione delle informazioni generali relative a un'applicazione</a></li> <li>• <a href="#">Visualizzazione delle risorse dell'applicazione</a></li> </ul>

## Sicurezza, identità e conformità

Servizio	Description
AWS Identity and Access Management (IAM)	<p><a href="#">IAM</a> è un servizio web che ti aiuta a controllare in modo sicuro l'accesso alle AWS risorse. Utilizza IAM per controllare chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) per l'utilizzo di risorse.</p>

Servizio	Description
	<p>Systems Manager consente di controllare l'accesso ai servizi tramite IAM.</p> <p>Ulteriori informazioni</p> <ul style="list-style-type: none"><li>• <a href="#">In che modo AWS Systems Manager funziona con IAM</a></li><li>• <a href="#">Operazioni, risorse e chiavi di condizione per AWS Systems Manager</a></li><li>• <a href="#">Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager</a></li></ul>
AWS Secrets Manager	<p><a href="#">Secrets Manager</a> fornisce una gestione più facile dei segreti. I segreti possono essere le credenziali dei database, le password, le chiavi API di terza parte e anche le parti di testo arbitrario.</p> <p>Parameter Store consente di recuperare i segreti di Secrets Manager se ne utilizzano altri Servizi AWS che già supportano i riferimenti ai Parameter Store parametri.</p> <p>Ulteriori informazioni</p> <p><a href="#">Referenziazione AWS Secrets Manager segreti di Parameter Store parametri</a></p>

Servizio	Description
AWS Security Hub CSPM	<p><a href="#">Security Hub CSPM</a> offre una visione completa degli avvisi di sicurezza ad alta priorità e dello stato di conformità in tutto il mondo. Account AWS Security Hub CSPM aggrega, organizza e assegna priorità agli avvisi di sicurezza, o ai risultati, provenienti da più utenti. Servizi AWS</p> <p>Quando attivi l'integrazione tra Security Hub CSPM e Security Hub CSPMPatch Manager, uno strumento in AWS Systems Manager dotazione, Security Hub CSPM monitora lo stato di applicazione delle patch delle flotte dal punto di vista della sicurezza. I dettagli sulla conformità delle patch vengono esportati automaticamente in Security Hub CSPM. Ciò consente di utilizzare un'unica visualizzazione per monitorare centralmente lo stato di conformità delle patch e tenere traccia di altri risultati di sicurezza. Puoi ricevere avvisi quando i nodi della tua flotta non sono conformi alle patch ed esaminare i risultati della conformità delle patch nella console Security Hub CSPM.</p> <p>Puoi anche integrare Security Hub CSPM con Explorer e, strumenti in. OpsCenter AWS Systems Manager L'integrazione con Security Hub CSPM consente di ricevere i risultati da Security Hub CSPM in e. Explorer OpsCenter I risultati del CSPM di Security Hub forniscono informazioni di sicurezza che puoi utilizzare in Explorer e OpsCenter per aggregare e intervenire sui tuoi problemi di sicurezza, prestazioni e operativi in. AWS Systems Manager</p>

Servizio	Description
	<p>L'utilizzo di Security Hub CSPM è a pagamento . Per ulteriori informazioni, consulta i prezzi di <a href="#">Security Hub CSPM</a>.</p> <p>Ulteriori informazioni</p> <ul style="list-style-type: none"><li>• <a href="#">Ricezione di risultati da AWS Security Hub CSPM in Explorer</a></li><li>• <a href="#">Comprensione OpsCenter integrazione con AWS Security Hub CSPM</a></li><li>• <a href="#">Integrazione Patch Manager con AWS Security Hub CSPM</a></li></ul>

## Crittografia e PKI

Servizio	Description
AWS Key Management Service (AWS KMS)	<p><a href="#">AWS KMS</a> è un servizio gestito che consente di creare e controllare le chiavi gestite dal cliente, le chiavi di crittografia utilizzate per crittografare i dati.</p> <p>Systems Manager consente di AWS KMS creare SecureString parametri e crittografare i dati delle Session Manager sessioni.</p> <p>Ulteriori informazioni</p> <ul style="list-style-type: none"><li>• <a href="#">AWS KMS crittografia per AWS Systems Manager Parameter Store SecureString parametri</a></li><li>• <a href="#">Attiva la crittografia delle chiavi KMS per i dati delle sessioni (console)</a></li></ul>

## Gestione e governance

Servizio	Description
AWS CloudFormation	<p><a href="#">CloudFormation</a> è un servizio che aiuta a modellare e configurare le risorse di Amazon Web Services, in modo da dedicare meno tempo alla gestione di tali risorse e concentrarsi invece sulle applicazioni eseguite in AWS.</p> <p>Parameter Store è una fonte per riferimenti dinamici. I riferimenti dinamici forniscono un modo compatto e potente per specificare valori esterni che vengono archiviati e gestiti in altri servizi nei modelli di CloudFormation stack.</p> <p>Ulteriori informazioni</p> <p><a href="#">Utilizzo di riferimenti dinamici per specificare valori di modello</a></p>
AWS CloudTrail	<p><a href="#">CloudTrail</a> è un modulo Servizio AWS che ti aiuta ad autorizzare la governance, la conformità e il controllo operativo e dei rischi dei tuoi Account AWS. Le azioni intraprese da un utente, ruolo o da un utente Servizio AWS vengono registrate come eventi in CloudTrail. Gli eventi includono le azioni intraprese in Console di gestione AWS, AWS Command Line Interface (AWS CLI), AWS SDK e API.</p> <p>L'integrazione di Systems Manager consente di acquisire la CloudTrail maggior parte delle chiamate API di Systems Manager sotto forma di eventi. Sono incluse le chiamate API avviate dalla console di Systems Manager e le chiamate effettuate alle API di Systems Manager.</p>

Servizio	Description
	<p>Ulteriori informazioni</p> <p><a href="#">Registrazione dei log AWS Systems Manager</a> <a href="#">Chiamate API con AWS CloudTrail</a></p>
Amazon Logs CloudWatch	<p><a href="#">Amazon CloudWatch Logs</a> ti consente di centralizzare i log di tutti i tuoi sistemi e applicazioni Servizi AWS che utilizzi. È quindi possibile visualizzarli, ricercarli per codici di errore o modelli specifici, filtrarli in base a campi specifici o archivarli in modo sicuro per analisi future.</p> <p>Systems Manager supporta l'invio di log per SSM AgentRun Command, e Session Manager verso CloudWatch Logs.</p> <p>Ulteriori informazioni</p> <ul style="list-style-type: none"><li>• <a href="#">Invio dei log dei nodi a CloudWatch registri unificati (CloudWatch agente)</a></li><li>• <a href="#">Configurazione di Amazon CloudWatch Logs per Run Command</a></li><li>• <a href="#">Registrazione dei dati della sessione tramite Amazon CloudWatch Logs (console)</a></li></ul>

Servizio	Description
Amazon EventBridge	<p><a href="#">EventBridge</a> fornisce un flusso quasi in tempo reale di eventi di sistema che descrive i cambiamenti nelle risorse di Amazon Web Services. Utilizzando semplici regole che puoi configurare rapidamente, puoi abbinare gli eventi e indirizzarli a una o più funzioni o flussi di destinazione. EventBridge viene a conoscenza dei cambiamenti operativi man mano che si verificano. EventBridge risponde a questi cambiamenti operativi e intraprende le azioni correttive necessarie. Queste operazioni includono l'invio di messaggi di risposta all'ambiente, l'attivazione di funzioni e l'acquisizione di informazioni sullo stato.</p> <p>Systems Manager dispone di più eventi supportati che EventBridge consentono di intraprendere azioni in base al contenuto di tali eventi.</p> <p>Ulteriori informazioni</p> <p><a href="#">Monitoraggio degli eventi di Systems Manager con Amazon EventBridge</a></p> <div><p> <b>Note</b></p><p>Amazon EventBridge è il modo preferito per gestire i tuoi eventi. CloudWatch Events e EventBridge sono lo stesso servizio e la stessa API di base, ma EventBridge offrono più funzionalità. Le modifiche apportate in uno dei due CloudWatch sistemi o EventBridge si riflettono in ciascuna console.</p></div>



Servizio	Description
	<p>Per ulteriori informazioni, consulta la <a href="#">Amazon EventBridge User Guide</a>.</p>
AWS Config	<p><a href="#">AWS Config</a> fornisce una visione dettagliata della configurazione delle AWS risorse nel tuo Account AWS. Questo include le relazioni tra le risorse e la maniera in cui sono state configurate. Ciò consente di vedere come le configurazioni e le relazioni cambiano nel tempo.</p> <p>Systems Manager è integrato e fornisce diverse regole che consentono di ottenere visibilità sulle istanze EC2. AWS Config Queste regole consentono di identificare quali istanze EC2 sono gestite da Systems Manager, configurazioni del sistema operativo, aggiornamenti a livello di sistema, applicazioni installate, configurazioni di rete e altro ancora.</p> <p>Ulteriori informazioni</p> <ul style="list-style-type: none"><li>• <a href="#">AWS Config tipi di risorse supportati</a></li><li>• <a href="#">Registrazione della configurazione del software per le istanze gestite</a></li><li>• <a href="#">Visualizzazione della cronologia e del monitoraggio delle modifiche di Inventory</a></li></ul>

Servizio	Description
AWS Trusted Advisor	<p><a href="#">Trusted Advisor</a> è uno strumento online che fornisce indicazioni in tempo reale per poter effettuare il provisioning delle tue risorse seguendo le best practice AWS .</p> <p>Systems Manager ospita Trusted Advisor ed è possibile visualizzare Trusted Advisor i dati inExplorer.</p> <p>Ulteriori informazioni</p> <ul style="list-style-type: none"><li>• <a href="#">AWS Systems Manager Explorer</a></li><li>• <a href="#">Guida introduttiva con AWS Trusted Advisor</a></li></ul>

Servizio	Description
AWS Organizations	<p><a href="#">Organizations</a> è un servizio di gestione degli account che consente di consolidare più account Account AWS in un'organizzazione creata e gestita centralmente. Organizations include funzionalità di gestione degli account e fatturazione consolidata che consentono di soddisfare al meglio le esigenze di budget, sicurezza e conformità dell'azienda.</p> <p>L'integrazione tra <a href="#">Change Manager</a> e organizzazioni consente di utilizzare un account amministratore delegato per gestire le richieste di modifica, i modelli di modifica e le approvazioni per l'intera organizzazione tramite un unico account.</p> <p>L'integrazione delle organizzazioni con <a href="#">Inventory</a>, uno strumento che <a href="#">Explorer</a> consente di aggregare i dati di inventario e operativi (OpsData) da più e. AWS Systems Manager Regioni AWS Account AWS</p> <p>L'integrazione tra Quick Setup e le organizzazioni automatizza le attività comuni di configurazione dei servizi e implementa le configurazioni dei servizi in base alle best practice in tutte le unità organizzative (OU).</p>

## Reti e distribuzione di contenuti

Servizio	Description
AWS PrivateLink	<p><a href="#">AWS PrivateLink</a> consente di connettere privatamente il tuo cloud privato virtuale (VPC) ai servizi endpoint supportati Servizi AWS e</p>

Servizio	Description
	<p>VPC senza richiedere un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. Direct Connect</p> <p>Systems Manager supporta i nodi gestiti che si connettono alle API di Systems Manager utilizzando AWS PrivateLink. Ciò migliora il livello di sicurezza dei nodi gestiti perché AWS PrivateLink limita tutto il traffico di rete tra i nodi gestiti, Systems Manager e Amazon EC2 alla rete Amazon. Ciò significa che non è necessario che i nodi gestiti abbiano accesso a Internet.</p> <p>Ulteriori informazioni</p> <p><a href="#">Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager</a></p>

## Analisi

Servizio	Description
Amazon Athena	<p><a href="#">Athena</a> è un servizio interattivo di esecuzione di query che consente l'analisi di dati direttamente in Amazon Simple Storage Service (Amazon S3) con SQL standard. Con poche azioni Console di gestione AWS, puoi indirizzare Athena ai tuoi dati archiviati in Amazon S3 e iniziare a utilizzare lo standard SQL per eseguire query una tantum e ottenere risultati in pochi secondi.</p> <p>Systems Manager Inventory si integra con Athena per aiutarti a interrogare i dati di inventario da più e. Regioni AWS Account</p>

Servizio	Description
	<p>AWS L'integrazione Athena utilizza la sincronizzazione dei dati delle risorse in modo da poter visualizzare i dati di inventario di tutti i nodi gestiti sulla pagina Vista dettagliata nella console Inventario di Systems Manager.</p> <p>Ulteriori informazioni</p> <ul style="list-style-type: none"><li>• <a href="#">Esecuzione di query sui dati di inventario da più regioni e account</a></li><li>• <a href="#">Procedura dettagliata: utilizzo di sincronizzazione dati risorsa per aggregare dati di inventario</a></li></ul>
AWS Glue	<p><a href="#">AWS Glue</a> è un servizio ETL (estrazione, trasformazione e caricamento) completamente gestito che consente di catalogare, pulire e migliorare la qualità dei dati in modo semplice e conveniente, oltre a trasferirli in modo sicuro tra datastore e flussi di dati.</p> <p>Systems Manager utilizza AWS Glue per scansionare i dati di inventario nel bucket S3.</p> <p>Ulteriori informazioni</p> <p><a href="#">Esecuzione di query sui dati di inventario da più regioni e account</a></p>

Servizio	Description
Amazon Quick	<p><a href="#">Quick</a> è un servizio di analisi aziendale che puoi utilizzare per creare visualizzazioni, eseguire analisi una tantum e ottenere informazioni aziendali dai tuoi dati. Si può rilevare automaticamente le origini dati AWS e funziona anche con le origini dati.</p> <p>La sincronizzazione dei dati della risorsa di Systems Manager invia i dati di inventario raccolti da tutti i nodi gestiti in un singolo bucket S3. Puoi utilizzare Quick per interrogare e analizzare i dati aggregati.</p> <p>Ulteriori informazioni</p> <ul style="list-style-type: none"><li>• <a href="#">Creazione di un Resource Data Sync per Inventario</a></li><li>• <a href="#">Procedura dettagliata: utilizzo di sincronizzazione dati risorsa per aggregare dati di inventario</a></li></ul>

## Integrazione di applicazioni

Servizio	Description
Amazon Simple Notification Service (Amazon SNS)	<p><a href="#">Amazon SNS</a> è un servizio Web che coordina e gestisce la consegna o l'invio di messaggi a clienti o endpoint iscritti.</p> <p>Systems Manager genera stati per più servizi che possono essere acquisiti dalle notifiche Amazon SNS.</p>

Servizio	Description
	<p>Ulteriori informazioni</p> <ul style="list-style-type: none"><li>• <a href="#">Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS</a></li><li>• <a href="#">Impostazione delle notifiche o delle azioni di attivazione basate su Parameter Store eventi</a></li></ul>

## Console di gestione AWS

Servizio	Description
AWS Resource Groups	<p><a href="#">I gruppi di risorse</a> organizzano le tue AWS risorse. I gruppi di risorse semplificano la gestione, il monitoraggio e l'automatizzazione delle attività per numeri elevati di risorse.</p> <p>Tipi di risorse di Systems Manager come nodi gestiti, documenti SSM, finestre di manutenzione, parametri Parameter Store e patch di base possono essere aggiunte ai gruppi di risorse.</p> <p>Ulteriori informazioni</p> <p><a href="#">Che cosa sono i AWS Resource Groups?</a></p>

### Argomenti

- [Esecuzione di script da Amazon S3](#)
- [Referenziazione AWS Secrets Manager segreti di Parameter Store parametri](#)
- [AWS KMS crittografia per AWS Systems Manager Parameter Store SecureString parametri](#)
- [Utilizzo Parameter Store parametri in Amazon Elastic Kubernetes Service](#)
- [Utilizzo Parameter Store parametri in AWS Lambda funzioni](#)

## Esecuzione di script da Amazon S3

Questa sezione illustra come scaricare ed eseguire script da Amazon Simple Storage Service (Amazon S3). Il seguente argomento include informazioni e terminologia relative ad Amazon S3. Per maggiori informazioni su Amazon S3, consulta la pagina [Cos'è Amazon S3?](#) Puoi eseguire diversi tipi di script, tra cui Ansible Playbooks, Python, Ruby, Shell e PowerShell.

È anche possibile scaricare una directory che includa più script. Quando si esegue lo script principale nella directory, vengono eseguiti AWS Systems Manager anche gli script di riferimento inclusi nella directory.

Tieni presenti le informazioni importanti sull'esecuzione di script da Amazon S3 riportate di seguito:

- Systems Manager non verifica che lo script possa essere eseguito su un nodo. Prima di scaricare ed eseguire lo script, verifica che il software necessario sia installato sul nodo. In alternativa, è possibile creare un documento composito che installi il software utilizzando uno degli strumenti Run Command o State Manager, quindi scarichi ed esegua AWS Systems Manager lo script.
- Verifica che il tuo utente, ruolo o gruppo disponga delle autorizzazioni AWS Identity and Access Management (IAM) necessarie per leggere dal bucket S3.
- Assicurati che il profilo dell'istanza sulle tue istanze Amazon Elastic Compute Cloud (Amazon EC2) disponga delle autorizzazioni necessarie. `s3:ListBucket` `s3:GetObject` Se il profilo dell'istanza non dispone di queste autorizzazioni, il sistema non riesce a scaricare lo script dal bucket S3. Per ulteriori informazioni, consulta [Utilizzo dei profili dell'istanza](#) in Guida per l'utente di IAM.

## Esecuzione di uno script Shell da Amazon S3

Le seguenti informazioni includono procedure per aiutarti a eseguire script da Amazon Simple Storage Service (Amazon S3) utilizzando la AWS Systems Manager console o (). AWS Command Line Interface AWS CLI Sebbene negli esempi vengano utilizzati script di shell, è possibile sostituirli con altri tipi di script.

### Esecuzione di uno script di shell da Amazon S3 (console)

### Esecuzione di uno script di shell da Amazon S3

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>



2. Nel pannello di navigazione, scegli Run Command.
3. Seleziona Esegui comando.
4. Nell'elenco Documento di comando, scegli **AWS-RunRemoteScript**.
5. In Parametri di comando, esegui le seguenti operazioni:
  - In Tipo di origine, seleziona S3.
  - Nella casella di testo Source Info (Informazioni origine), inserire le informazioni necessarie per accedere all'origine nel formato seguente. Sostituisci ogni *example resource placeholder* con le tue informazioni.

 Note

Sostituiscilo `https://s3.aws-api-domain` con l'URL del tuo bucket. Puoi copiare l'URL del bucket in Amazon S3 nella scheda Oggetti.

```
{"path": "https://s3.aws-api-domain/path to script"}
```

Di seguito è riportato un esempio di :

```
{"path": "https://amzn-s3-demo-bucket.s3.us-east-2.amazonaws.com/scripts/shell/helloWorld.sh"}
```

- Nel campo Riga di comando, inserisci i parametri per l'esecuzione di script. Ecco un esempio.

```
helloWorld.sh argument-1 argument-2
```
  - (Facoltativo) Nel campo Directory di lavoro, inserisci il nome di una directory sul nodo su cui si desidera scaricare ed eseguire lo script.
  - (Facoltativo) In Timeout di esecuzione, specifica il numero di secondi che il sistema dovrà attendere prima di interrompere l'esecuzione del comando di script.
6. Nella sezione Destinazioni, scegli i nodi gestiti in cui si desidera eseguire questa operazione specificando i tag, selezionando manualmente le istanze, i dispositivi edge o indicando un gruppo di risorse.

**Tip**

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

**7. In Altri parametri:**

- In Commento, digita le informazioni su questo comando.
- In Timeout (secondi), specifica il numero di secondi che il sistema dovrà attendere prima di generare un errore per l'intera esecuzione del comando.

**8. Per Controllo velocità:**

- In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

**Note**

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti presi di mira, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.
9. (Facoltativo) Nella sezione Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Scrivi l'output del comando in un bucket S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

**Note**

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle](#)

[autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

10. Se vuoi che vengano inviate notifiche sullo stato dell'esecuzione del comando, nella sezione Notifiche SNS selezionare la casella di controllo Abilita notifiche SNS.

Per ulteriori informazioni sulla configurazione delle notifiche Amazon SNS per Run Command, consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

11. Scegli Esegui.

Esecuzione di uno script di shell da Amazon S3 (riga di comando)

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Eseguire il seguente comando seguente. Sostituisci ogni *example resource placeholder* con le tue informazioni.

#### Note

Sostituisci `https://s3.aws-api-domain/script path` con l'URL del tuo bucket. Puoi copiare l'URL del bucket in Amazon S3 nella scheda Objects (Oggetti).

Linux & macOS

```
aws ssm send-command \
 --document-name "AWS-RunRemoteScript" \
 --output-s3-bucket-name "amzn-s3-demo-bucket" \
 --output-s3-key-prefix "key-prefix" \
 --targets "Key=InstanceIds,Values=instance-id" \
 --parameters '["sourceType":["S3"],"sourceInfo":["{"path\\":\\"https://
s3.aws-api-domain/script path\\"}"],"commandLine":["script name and arguments"]]'
```

## Windows

```
aws ssm send-command ^
 --document-name "AWS-RunRemoteScript" ^
 --output-s3-bucket-name "amzn-s3-demo-bucket" ^
 --output-s3-key-prefix "key-prefix" ^
 --targets "Key=InstanceIds,Values=instance-id" ^
 --parameters "sourceType"="S3",sourceInfo='{\"path\": \"https://s3.aws-api-
domain/script path\"}',"commandLine"="script name and arguments"
```

## PowerShell

```
Send-SSMCommand `
 -DocumentName "AWS-RunRemoteScript" `
 -OutputS3BucketName "amzn-s3-demo-bucket" `
 -OutputS3KeyPrefix "key-prefix" `
 -Target @{Key="InstanceIds";Values=@("instance-id")} `
 -Parameter @{
 sourceType = "S3";
 sourceInfo = '{"path": "s3://bucket-name/path/to/script"}';
 commandLine = "script name and arguments"
 }
```

## Referenziazione AWS Secrets Manager segreti di Parameter Store parametri

AWS Secrets Manager ti aiuta a organizzare e gestire importanti dati di configurazione come credenziali, password e chiavi di licenza. Parameter Store è integrato con Secrets Manager in modo da poter recuperare i segreti di Secrets Manager quando ne usi altri Servizi AWS che già supportano i riferimenti ai Parameter Store parametri. Questi servizi includono Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS), AWS Lambda CloudFormation AWS CodeBuild AWS CodeDeploy, e altri strumenti di Systems Manager. Avvalendoti di Parameter Store per fare riferimento ai segreti di Secrets Manager, configura un processo coerente e sicuro per la chiamata e l'utilizzo di segreti e dati di riferimento in script di configurazione e codice.

Per ulteriori informazioni su Secrets Manager, consulta [What Is? AWS Secrets Manager](#) nella Guida AWS Secrets Manager per l'utente.

## Restrizioni

Nell'utilizzo di Parameter Store per fare riferimento ai segreti di Secrets Manager, tieni presenti le seguenti restrizioni:

- È possibile recuperare i segreti di Secrets Manager solo utilizzando le operazioni [GetParameter](#) e [GetParameters](#) API. Le operazioni di modifica e le operazioni API avanzate di interrogazione, come [DescribeParameters](#) e [GetParametersByPath](#), non sono supportate in Secrets Manager.
- Puoi usare AWS Command Line Interface (AWS CLI) e AWS Tools for Windows PowerShell gli SDK per recuperare un segreto utilizzando. Parameter Store
- I segreti di Secrets Manager in Parameter Store devono avere il prefisso di `/aws/reference/secretsmanager/`. Di seguito vengono mostrati gli esempi:

```
/aws/reference/secretsmanager/CFCreds1
```

```
/aws/reference/secretsmanager/myapp/db/password
```

- Parameter Store rispetta le politiche AWS Identity and Access Management (IAM) associate ai segreti di Secrets Manager. Se, ad esempio, non vi ha accesso, l'Utente 1 non può nemmeno recuperare il Segreto A tramite Parameter Store.
- I parametri che fanno riferimento ai segreti di Secrets Manager non ammettono l'utilizzo del controllo delle versioni Parameter Store o le funzionalità della cronologia.
- Parameter Store rispetta le fasi delle versioni Secrets Manager. Nel caso di riferimento a una fase di versione, sono ammessi numeri, lettere, un punto (.), un trattino (-) o un trattino basso (\_). Eventuali altri simboli specificati nella fase della versione comportano l'esito negativo del tentativo di riferimento.

## Come fare riferimento a un segreto di Secrets Manager utilizzando Parameter Store

La procedura riportata di seguito illustra come fare riferimento a un segreto di Secrets Manager utilizzando API di Parameter Store. La procedura fa riferimento ad altre procedure riportate nella Guida per l'utente di AWS Secrets Manager .

### Note

Prima di iniziare, verifica di disporre dell'autorizzazione necessaria per fare riferimento a segreti di Secrets Manager nei parametri Parameter Store. Se si dispone delle autorizzazioni di amministratore in Secrets Manager e Systems Manager, è possibile fare riferimento ai

segreti o recuperarli con API Parameter Store. Se si fa riferimento a un segreto di Secrets Manager in un parametro Parameter Store senza disporre dell'autorizzazione di accesso al segreto, il tentativo di riferimento ha esito negativo. Per ulteriori informazioni, consulta [Autenticazione e controllo degli accessi AWS Secrets Manager](#) nella Guida per l'utente di AWS Secrets Manager .

 Important

Parameter Store funge da servizio di trasferimento per i riferimenti a segreti di Secrets Manager. Parameter Store non conserva dati o metadati relativi ai segreti. Il riferimento è stateless.

Per fare riferimento a un segreto di Secrets Manager utilizzando Parameter Store

1. Creazione di un segreto in Secrets Manager. Per ulteriori informazioni, consulta [Creare e gestire i segreti con AWS Secrets Manager](#).
2. Fai riferimento a un segreto utilizzando AWS CLI, AWS Tools for Windows PowerShell, o l'SDK. Quando si fa riferimento a un segreto di Secrets Manager, il nome del parametro deve iniziare con il seguente percorso riservato: `/aws/reference/secretsmanager/`. Una volta specificato questo percorso, Systems Manager è in condizione di recuperare il segreto da Secrets Manager invece che da Parameter Store. Ecco alcuni esempi di nomi che fanno riferimento correttamente ai segreti di Secrets Manager, CFCreds1 e DBPass, con Parameter Store.
  - `/aws/reference/secretsmanager/CFCreds1`
  - `/aws/reference/secretsmanager/DBPass`

Ecco un esempio di codice Java che fa riferimento a una chiave di accesso e a una chiave segreta archiviate in Secrets Manager. Questo codice esemplificativo configura un client Amazon DynamoDB. Il codice recupera i dati di configurazione e le credenziali da Parameter Store. I dati di configurazione sono memorizzati come parametro di stringa in Parameter Store, mentre le credenziali risultano archiviate su Secrets Manager. Anche se archiviati in servizi diversi, entrambi i set di dati possono essere fruiti accedendo da Parameter Store, tramite l'API `GetParameter`.

```

/**
 * Initialize Systems Manager client with default credentials
 */
AWSSimpleSystemsManagement ssm =
 AWSSimpleSystemsManagementClientBuilder.defaultClient();

...

/**
 * Example method to launch DynamoDB client with credentials different from default
 * @return DynamoDB client
 */
AmazonDynamoDB getDynamoDbClient() {
 //Getting AWS credentials from Secrets Manager using GetParameter
 BasicAWSCredentials differentAWSCreds = new BasicAWSCredentials(
 getParameter("/aws/reference/secretsmanager/access-key"),
 getParameter("/aws/reference/secretsmanager/secret-key"));

 //Initialize the DynamoDB client with different credentials
 final AmazonDynamoDB client = AmazonDynamoDBClient.builder()
 .withCredentials(new AWSStaticCredentialsProvider(differentAWSCreds))
 .withRegion(getParameter("region")) //Getting configuration from
Parameter Store
 .build();
 return client;
}

/**
 * Helper method to retrieve parameter value
 * @param parameterName identifier of the parameter
 * @return decrypted parameter value
 */
public GetParameterResult getParameter(String parameterName) {
 GetParameterRequest request = new GetParameterRequest();
 request.setName(parameterName);
 request.setWithDecryption(true);
 return ssm.newGetParameterCall().call(request).getParameter().getValue();
}

```

Ecco alcuni AWS CLI esempi. Utilizza il comando `aws secretsmanager list-secrets` per trovare i nomi dei tuoi segreti.

## AWS CLI Esempio 1: riferimento utilizzando il nome del segreto

### Linux & macOS

```
aws ssm get-parameter \
 --name /aws/reference/secretsmanager/s1-secret \
 --with-decryption
```

### Windows

```
aws ssm get-parameter ^
 --name /aws/reference/secretsmanager/s1-secret ^
 --with-decryption
```

Il comando restituisce informazioni simili alle seguenti.

```
{
 "Parameter": {
 "Name": "/aws/reference/secretsmanager/s1-secret",
 "Type": "SecureString",
 "Value": "F1*MEishm!al875",
 "Version": 0,
 "SourceResult":
 "{
 \"CreatedDate\": 1526334434.743,
 \"Name\": \"s1-secret\",
 \"VersionId\": \"aaabbbccc-1111-222-333-123456789\",
 \"SecretString\": \"F1*MEishm!al875\",
 \"VersionStages\": [\"AWSCURRENT\"],
 \"ARN\": \"arn:aws:secretsmanager:us-
east-2:123456789012:secret:s1-secret-E18LRP\"
 }"
 "LastModifiedDate": 2018-05-14T21:47:14.743Z,
 "ARN": "arn:aws:secretsmanager:us-east-2:123456789012:secret:s1-secret-
E18LRP",
 }
}
```

## AWS CLI Esempio 2: riferimento che include l'ID della versione



## Linux & macOS

```
aws ssm get-parameter \
 --name /aws/reference/secretsmanager/s1-secret:11111-aaa-bbb-ccc-123456789 \
 --with-decryption
```

## Windows

```
aws ssm get-parameter ^
 --name /aws/reference/secretsmanager/s1-secret:11111-aaa-bbb-ccc-123456789 ^
 --with-decryption
```

Il comando restituisce informazioni simili alle seguenti.

```
{
 "Parameter": {
 "Name": "/aws/reference/secretsmanager/s1-secret",
 "Type": "SecureString",
 "Value": "Fl*MEishm!al875",
 "Version": 0,
 "SourceResult":
 "{
 \"CreatedDate\": 1526334434.743,
 \"Name\": \"s1-secret\",
 \"VersionId\": \"11111-aaa-bbb-ccc-123456789\",
 \"SecretString\": \"Fl*MEishm!al875\",
 \"VersionStages\": [\"AWSCURRENT\"],
 \"ARN\": \"arn:aws:secretsmanager:us-
east-2:123456789012:secret:s1-secret-E18LRP\"
 }"
 "Selector": ":11111-aaa-bbb-ccc-123456789"
 }
 "LastModifiedDate": 2018-05-14T21:47:14.743Z,
 "ARN": "arn:aws:secretsmanager:us-east-2:123456789012:secret:s1-secret-
E18LRP",
}
```

## AWS CLI Esempio 3: riferimento che include la fase della versione

## Linux & macOS

```
aws ssm get-parameter \
 --name /aws/reference/secretsmanager/s1-secret:AWSCURRENT \
 --with-decryption
```

## Windows

```
aws ssm get-parameter ^
 --name /aws/reference/secretsmanager/s1-secret:AWSCURRENT ^
 --with-decryption
```

Il comando restituisce informazioni simili alle seguenti.

```
{
 "Parameter": {
 "Name": "/aws/reference/secretsmanager/s1-secret",
 "Type": "SecureString",
 "Value": "Fl*MEishm!al875",
 "Version": 0,
 "SourceResult":
 "{
 \"CreatedDate\": 1526334434.743,
 \"Name\": \"s1-secret\",
 \"VersionId\": \"11111-aaa-bbb-ccc-123456789\",
 \"SecretString\": \"Fl*MEishm!al875\",
 \"VersionStages\": [\"AWSCURRENT\"],
 \"ARN\": \"arn:aws:secretsmanager:us-
east-2:123456789012:secret:s1-secret-E18LRP\"
 }"
 "Selector": ":AWSCURRENT"
 }
 "LastModifiedDate": 2018-05-14T21:47:14.743Z,
 "ARN": "arn:aws:secretsmanager:us-east-2:123456789012:secret:s1-secret-
E18LRP",
}
```

# AWS KMS crittografia per AWS Systems Manager Parameter Store

## SecureString parametri

Con AWS Systems Manager Parameter Store, è possibile creare [SecureString parametri](#), che sono parametri con un nome di parametro in testo semplice e un valore di parametro crittografato. Parameter Store utilizza AWS KMS per crittografare e decrittografare i valori dei parametri.

### SecureString

Con Parameter Store, è possibile creare, archiviare e gestire i dati come parametri con valori. È possibile creare un parametro in Parameter Store e utilizzarlo in più applicazioni e servizi soggetti a policy e autorizzazioni che tu stesso stabilisci. Quando è necessario modificare il valore di un parametro, è sufficiente modificare un'istanza anziché gestire modifiche soggette a errori apportate a numerose fonti. Parameter Store supporta una struttura gerarchica per i nomi dei parametri. È quindi possibile qualificare un parametro per usi specifici.

Per gestire i dati sensibili, puoi creare dei SecureString parametri. Parameter Store utilizza AWS KMS keys per crittografare i valori dei SecureString parametri quando li si crea o si modifica. Utilizza inoltre le chiavi KMS per decrittare i valori dei parametri al momento dell'accesso. È possibile utilizzare la [Chiave gestita da AWS](#) che Parameter Store crea per l'account, oppure specificare la propria [chiave gestita dal cliente](#).

#### Important

Parameter Store supporta solo [chiavi KMS simmetriche](#). Non è possibile utilizzare una [chiave KMS asimmetrica](#) per crittografare i parametri. Per informazioni su come determinare se una chiave KMS è o meno asimmetrica, consulta [Identifica i diversi tipi di chiavi](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Parameter Store supporta due livelli di parametri SecureString: standard e avanzati. I parametri standard, che non possono superare i 4096 byte, sono crittografati e decrittati direttamente con la chiave KMS specificata. Per crittografare e decrittografare i parametri SecureString avanzati, Parameter Store utilizza la crittografia a busta con [AWS Encryption SDK](#). È possibile convertire un parametro SecureString standard in un parametro avanzato, ma non è possibile convertire un parametro avanzato in uno standard. Per ulteriori informazioni sulla differenza tra parametri SecureString standard e avanzati, consulta [Scelta dei livelli di parametri in Parameter Store](#).

## Protezione dei parametri standard SecureString

Parameter Store non esegue alcuna operazione di crittografia. Al contrario, si basa su AWS KMS per crittografare e decrittografare i valori dei parametri SecureString. Quando si crea o si modifica un valore di SecureString parametro standard, Parameter Store chiama l'[operazione AWS KMS Encrypt](#). Questa operazione usa una chiave KMS di crittografia simmetrica direttamente per crittografare il valore del parametro anziché utilizzare la chiave KMS per generare una [chiave dei dati](#).

È possibile selezionare la chiave KMS utilizzata da Parameter Store per crittografare il valore del parametro. Non specificando una chiave KMS, Parameter Store usa la Chiave gestita da AWS generata automaticamente da Systems Manager nell'account. Questa chiave KMS ha l'alias `aws/ssm`.

Per visualizzare la chiave `aws/ssm` KMS predefinita per il tuo account, utilizza l'[DescribeKey](#) operazione nell' AWS KMS API. L'esempio seguente utilizza il `describe-key` comando in AWS Command Line Interface (AWS CLI) con il nome `aws/ssm` alias.

```
aws kms describe-key \
 --key-id alias/aws/ssm
```

Per creare un SecureString parametro standard, utilizzate l'[PutParameter](#) operazione nell'API Systems Manager. Ometti il parametro `Tier` o specifica un valore `Standard`, che è l'impostazione predefinita. Includi un parametro `Type` con un valore `SecureString`. Per specificare una chiave KMS, utilizza il parametro `KeyId`. L'impostazione predefinita è Chiave gestita da AWS per il tuo account, `aws/ssm`.

Parameter Store quindi chiama l' AWS KMS Encrypt operazione con la chiave KMS e il valore del parametro in chiaro. AWS KMS restituisce il valore del parametro crittografato, che viene Parameter Store memorizzato con il nome del parametro.

L'esempio seguente utilizza il [comando](#) `put-parameter` di Systems Manager e il relativo `--type` parametro in AWS CLI per creare un SecureString parametro. Poiché il comando omette i parametri opzionali `--tier` e `--key-id`, Parameter Store crea un parametro SecureString standard e lo crittografa con la Chiave gestita da AWS.

```
aws ssm put-parameter \
 --name MyParameter \
 --value "secret_value" \
 --type SecureString
```

Il seguente esempio simile utilizza il parametro `--key-id` per specificare una [chiave gestita dal cliente](#). L'esempio utilizza un ID chiave KMS per identificare la chiave KMS. Tuttavia, è possibile utilizzare qualsiasi identificatore di chiave KMS valido. Poiché il comando omette il parametro `Tier` (`--tier`), Parameter Store crea un parametro `SecureString` standard, non uno avanzato.

```
aws ssm put-parameter \
 --name param1 \
 --value "secret" \
 --type SecureString \
 --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Quando si ottiene un parametro `SecureString` da Parameter Store, il valore è crittografato. Per ottenere un parametro, utilizzate l'[GetParameter](#) operazione nell'API Systems Manager.

L'esempio seguente utilizza il [comando](#) `get-parameter` di Systems Manager nel file da cui AWS CLI ottenere il `MyParameter` parametro Parameter Store senza decrittografarne il valore.

```
aws ssm get-parameter --name MyParameter
```

```
{
 "Parameter": {
 "Type": "SecureString",
 "Name": "MyParameter",
 "Value": "AQECAHgn0kMR0h5LaLXkA4j0+vYi6tmM17Lg"
 }
}
```

Per decrittografare il valore del parametro prima di restituirlo, impostare il parametro `WithDecryption` di `GetParameter` su `true`. Quando si utilizza `WithDecryption`, Parameter Store chiama l'[operazione AWS KMS](#) `Decrypt` per conto dell'utente per decrittografare il valore del parametro. Di conseguenza, la richiesta `GetParameter` restituisce il parametro con un valore di parametro in testo normale, come mostrato nel seguente esempio.

```
aws ssm get-parameter \
 --name MyParameter \
 --with-decryption
```

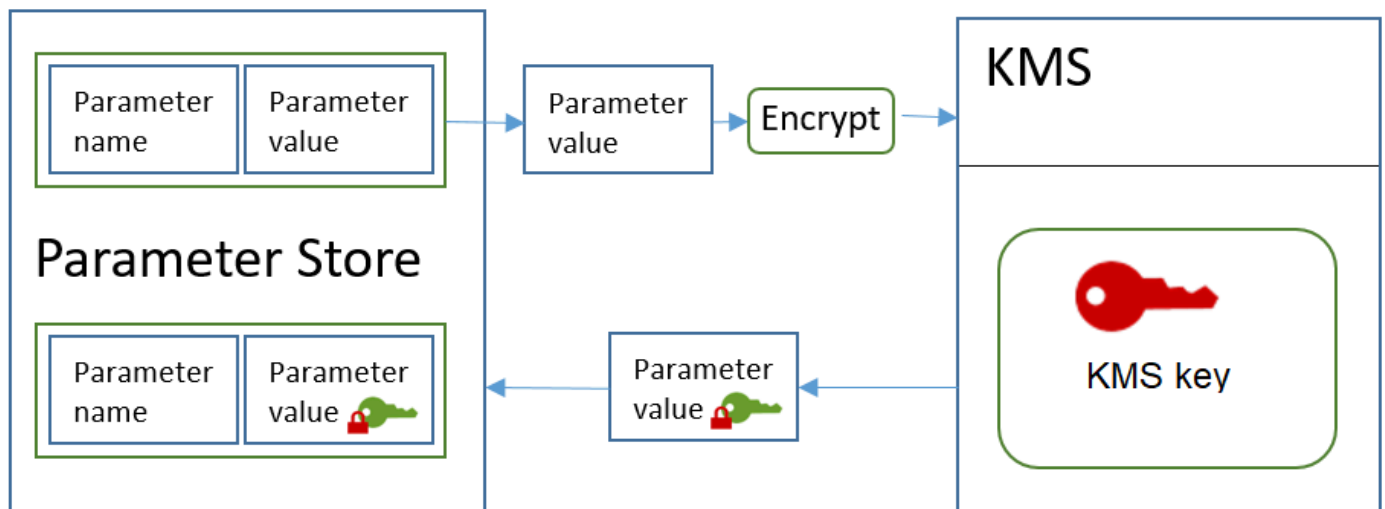
```
{
```

```
"Parameter": {
 "Type": "SecureString",
 "Name": "MyParameter",
 "Value": "secret_value"
}
```

Il seguente flusso di lavoro mostra il modo in cui Parameter Store utilizza una chiave KMS per crittografare e decrittare un parametro SecureString standard.

### Crittografare un parametro standard

1. Quando si utilizza `PutParameter` per creare un parametro SecureString, Parameter Store invia una richiesta `Encrypt` a AWS KMS. Questa richiesta include il valore del parametro in testo normale, la chiave KMS scelta e il [contesto di crittografia di Parameter Store](#). Durante la trasmissione a AWS KMS, il valore in testo normale del SecureString parametro è protetto da Transport Layer Security (TLS).
2. AWS KMS crittografa il valore del parametro con la chiave KMS e il contesto di crittografia specificati. Restituisce il testo criptato a Parameter Store, che memorizza il nome e il valore crittografato del parametro.



### Decrittografia di un parametro standard

1. Quando si include il `WithDecryption` parametro in una `GetParameter` richiesta, Parameter Store invia una `Decrypt` richiesta a AWS KMS con il valore del SecureString parametro crittografato e il contesto [di](#) Parameter Store crittografia.

2. AWS KMS utilizza la stessa chiave KMS e il contesto di crittografia fornito per decrittografare il valore crittografato. Restituisce il valore del parametro in testo normale (decrittografato) a Parameter Store. Durante la trasmissione, i dati in testo normale sono protetti da TLS.
3. Parameter Store restituisce il valore del parametro in testo normale nella risposta `GetParameter`.

## Protezione dei parametri avanzati SecureString

Quando si utilizza `PutParameter` per creare un `SecureString` parametro avanzato, Parameter Store utilizza la crittografia a [inviluppo](#) con AWS Encryption SDK e una crittografia simmetrica AWS KMS key per proteggere il valore del parametro. Ogni valore di parametro avanzato è crittografato con una chiave di dati univoca e la chiave di dati è crittografata con una chiave KMS. È possibile utilizzare la [Chiave gestita da AWS](#) per l'account (aws/ssm) o qualsiasi chiave gestita dal cliente.

[AWS Encryption SDK](#) è una libreria open source lato client, che consente di crittografare e decrittografare i dati utilizzando gli standard di settore e le best practice. È supportata su più piattaforme e in più linguaggi di programmazione, compresa un'interfaccia a riga di comando. È possibile visualizzare il codice sorgente e contribuire al suo sviluppo in GitHub.

Per ogni valore di `SecureString` parametro, Parameter Store chiama per AWS Encryption SDK crittografare il valore del parametro utilizzando una chiave di dati univoca che AWS KMS genera ([GenerateDataKey](#)). AWS Encryption SDK Restituisce Parameter Store un messaggio [crittografato](#) che include il valore del parametro crittografato e una copia crittografata della chiave dati univoca. Parameter Store memorizza l'intero messaggio crittografato nel valore del `SecureString` parametro. Quindi, quando si ottiene un valore di `SecureString` parametro avanzato, Parameter Store utilizza il AWS Encryption SDK per decrittografare il valore del parametro. Ciò richiede una chiamata a per AWS KMS decrittografare la chiave di dati crittografata.

Per creare un `SecureString` parametro avanzato, utilizzate l'[PutParameter](#) operazione nell'API Systems Manager. Imposta il valore del parametro `Tier` su `Advanced`. Includi un parametro `Type` con un valore `SecureString`. Per specificare una chiave KMS, utilizza il parametro `KeyId`. L'impostazione predefinita è Chiave gestita da AWS per il tuo account, aws/ssm.

```
aws ssm put-parameter \
 --name MyParameter \
 --value "secret_value" \
 --type SecureString \
 --tier Advanced
```

Il seguente esempio simile utilizza il parametro `--key-id` per specificare una [chiave gestita dal cliente](#). L'esempio utilizza l'Amazon Resource Name (ARN) della chiave KMS. Tuttavia, puoi utilizzare qualsiasi identificatore di chiave KMS valido.

```
aws ssm put-parameter \
 --name MyParameter \
 --value "secret_value" \
 --type SecureString \
 --tier Advanced \
 --key-id arn:aws:kms:us-
east-2:987654321098:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Quando si ottiene un `SecureString` parametro da Parameter Store, il suo valore è il messaggio crittografato restituito. AWS Encryption SDK Per ottenere un parametro, utilizzate l'[GetParameter](#) operazione nell'API di Systems Manager.

L'esempio seguente utilizza l'operazione `GetParameter` di Systems Manager per ottenere il parametro `MyParameter` da Parameter Store senza decrittare il valore.

```
aws ssm get-parameter --name MyParameter
```

```
{
 "Parameter": {
 "Type": "SecureString",
 "Name": "MyParameter",
 "Value": "AQECAHgn0kMR0h5LaLXkA4j0+vYi6tmM17Lg"
 }
}
```

Per decrittografare il valore del parametro prima di restituirlo, impostare il parametro `WithDecryption` di `GetParameter` su `true`. Quando lo usi `WithDecryption`, Parameter Store chiama l'[operazione AWS KMS](#) `Decrypt` per tuo conto per decrittografare il valore del parametro. Di conseguenza, la richiesta `GetParameter` restituisce il parametro con un valore di parametro in testo normale, come mostrato nel seguente esempio.

```
aws ssm get-parameter \
 --name MyParameter \
 --with-decryption
```

```
{
```



```
"Parameter": {
 "Type": "SecureString",
 "Name": "MyParameter",
 "Value": "secret_value"
}
```

Non è possibile convertire un SecureString parametro avanzato in uno standard. Tuttavia, è possibile convertire uno standard SecureString in uno avanzato. Per convertire un parametro SecureString standard in uno SecureString avanzato, utilizza l'operazione PutParameter con il parametro Overwrite. Type deve essere SecureString e il valore Tier deve essere Advanced. Il KeyId parametro, che identifica una chiave gestita dal cliente, è facoltativo. Se lo Parameter Store ometti, utilizza la Chiave gestita da AWS per l'account. È possibile specificare qualsiasi chiave KMS che il principale è autorizzato a utilizzare, anche se è stata utilizzata un'altra chiave KMS per crittografare il parametro standard.

Quando si utilizza il parametro Overwrite, Parameter Store utilizza AWS Encryption SDK per crittografare il valore del parametro. Quindi memorizza il nuovo messaggio crittografato in Parameter Store.

```
aws ssm put-parameter \
 --name myStdParameter \
 --value "secret_value" \
 --type SecureString \
 --tier Advanced \
 --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
 --overwrite
```

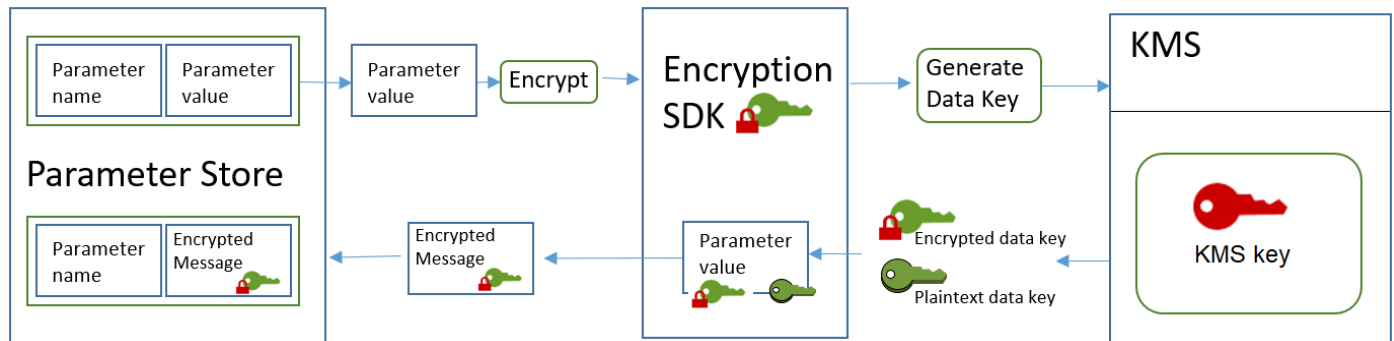
Il seguente flusso di lavoro mostra il modo in cui Parameter Store utilizza una chiave KMS per crittografare e decrittare un parametro SecureString avanzato.

### Crittografare un parametro avanzato

1. Quando si utilizza PutParameter per creare un SecureString parametro avanzato, Parameter Store utilizza il simbolo AWS Encryption SDK e AWS KMS per crittografare il valore del parametro. Parameter Store chiama il AWS Encryption SDK con il valore del parametro, la chiave KMS specificata e il contesto di [Parameter Store crittografia](#).
2. AWS Encryption SDK invia una [GenerateDataKey](#) richiesta a AWS KMS con l'identificatore della chiave KMS specificata e il Parameter Store contesto di crittografia. AWS KMS restituisce due

copie della chiave dati univoca: una in testo normale e una crittografata con la chiave KMS. Il contesto di crittografia viene utilizzato per crittografare la chiave di dati.

3. AWS Encryption SDK Utilizza la chiave dati in testo normale per crittografare il valore del parametro. Restituisce un [messaggio crittografato](#) che include il valore di parametro crittografato, la chiave di dati crittografata e altri dati, tra cui il contesto di crittografia Parameter Store.
4. Parameter Store memorizza il messaggio crittografato come valore del parametro.



## Decrittografare un parametro avanzato

1. È possibile includere il parametro `WithDecryption` in una richiesta `GetParameter` per ottenere un parametro `SecureString` avanzato. In questo caso, Parameter Store passa il [messaggio crittografato](#) dal valore di parametro a un metodo di decrittografia di AWS Encryption SDK.
2. AWS Encryption SDK Chiama l'operazione AWS KMS [Decrypt](#). Trasferisce la chiave di dati crittografata e il contesto di crittografia Parameter Store dal messaggio crittografato.
3. AWS KMS utilizza la chiave KMS e il contesto di Parameter Store crittografia per decrittografare la chiave di dati crittografata. Quindi restituisce la chiave di dati in testo normale (decrittografato) a AWS Encryption SDK.
4. AWS Encryption SDK Utilizza la chiave dati in testo normale per decrittografare il valore del parametro. Restituisce il valore del parametro in testo normale a Parameter Store.
5. Parameter Store verifica il contesto di crittografia e restituisce il valore del parametro in testo normale nella risposta `GetParameter`.

## Impostazione delle autorizzazioni per crittografare e decrittografare i valori dei parametri

Per crittografare un valore di parametro `SecureString` standard, l'utente necessita dell'autorizzazione `kms:Encrypt`. Per crittografare un valore di parametro `SecureString`

avanzato, l'utente necessita dell'autorizzazione `kms:GenerateDataKey`. Per decrittografare entrambi i tipi di valori di parametri `SecureString`, l'utente necessita dell'autorizzazione `kms:Decrypt`.

È possibile utilizzare le politiche AWS Identity and Access Management (IAM) per consentire o negare a un utente l'autorizzazione a chiamare il Systems Manager e le operazioni. `PutParameter` `GetParameter`

Inoltre, quando si utilizzano chiavi gestite dal cliente per crittografare i valori dei parametri `SecureString`, è possibile utilizzare le policy IAM e le policy della chiave per gestire le autorizzazioni di crittografia e decrittazione. Tuttavia, non è possibile definire policy di controllo degli accessi per la chiave KMS `aws/ssm` predefinita. Per informazioni dettagliate sul controllo dell'accesso a chiavi gestite dal cliente, consulta [Autorizzazioni e accesso con chiave KSM](#) nella Guida per gli sviluppatori di AWS Key Management Service .

L'esempio seguente mostra una policy IAM progettata per parametri `SecureString` standard. Questa consente all'utente di chiamare l'operazione `PutParameter` di Systems Manager su tutti i parametri nel percorso `FinancialParameters`. La policy consente inoltre all'utente di chiamare l'AWS KMS Encryptoperazione su un esempio di chiave gestita dal cliente.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:PutParameter"
],
 "Resource": "arn:aws:ssm:us-east-1:111122223333:parameter/FinancialParameters/*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "kms:Encrypt"
],
 "Resource": "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
 }
]
}
```

```
]
 }
}
```

L'esempio seguente mostra una policy IAM progettata per parametri SecureString avanzati. Questa consente all'utente di chiamare l'operazione `PutParameter` di Systems Manager su tutti i parametri nel percorso `ReservedParameters`. La policy consente inoltre all'utente di richiamare l'AWS KMS `GenerateDataKey` operazione su un esempio di chiave gestita dal cliente.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:PutParameter"
],
 "Resource": "arn:aws:ssm:us-east-1:111122223333:parameter/ReservedParameters/*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "kms:GenerateDataKey"
],
 "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-id"
 }
]
}
```

L'esempio finale mostra anche una policy IAM che può essere utilizzata per parametri SecureString standard o avanzati. Questa consente all'utente di chiamare le operazioni `GetParameter` di Systems Manager (e le operazioni correlate) su tutti i parametri nel percorso `ITParameters`. La policy consente inoltre all'utente di richiamare l'AWS KMS `Decrypt` operazione su un esempio di chiave gestita dal cliente.

## JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:GetParameter*"
],
 "Resource": "arn:aws:ssm:us-east-1:111122223333:parameter/ITParameters/*"
 },
 {
 "Effect": "Allow",
 "Action": [
 "kms:Decrypt"
],
 "Resource": "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
 }
]
}
```

## Parameter Store contesto di crittografia

Un contesto di crittografia è un set di coppie chiave-valore che contiene dati arbitrari non segreti. Quando si include un contesto di crittografia in una richiesta di crittografia dei dati, associa AWS KMS crittograficamente il contesto di crittografia ai dati crittografati. Lo stesso contesto di crittografia sia necessario per decrittografare i dati.

È inoltre possibile utilizzare il contesto di crittografia per identificare un'operazione di crittografia nei record e nei log di controllo. Il contesto di crittografia viene visualizzato in testo normale nei log, ad esempio nei log di [AWS CloudTrail](#).

Accetta AWS Encryption SDK anche un contesto di crittografia, sebbene lo gestisca in modo diverso. Parameter Store fornisce il contesto di crittografia al metodo di crittografia. Associa AWS Encryption SDK crittograficamente il contesto di crittografia ai dati crittografati. Include il contesto di crittografia in testo normale nell'intestazione del messaggio crittografato restituito. Tuttavia, a differenza dei metodi di AWS Encryption SDK decrittografia AWS KMS, non accettano un contesto di crittografia

come input. Invece, quando decrittografa i dati, AWS Encryption SDK ottiene il contesto di crittografia dal messaggio crittografato. Parameter Store verifica che il contesto di crittografia includa il valore previsto prima di restituire all'utente il valore del parametro in testo normale.

Parameter Store usa il seguente contesto di crittografia in tutte le operazioni di crittografia:

- Chiave: `PARAMETER_ARN`
- Valore: l'ARN (Amazon Resource Name) del parametro crittografato.

Il formato del contesto di crittografia è il seguente:

```
"PARAMETER_ARN": "arn:aws:ssm:region-id:account-id:parameter/parameter-name"
```

Ad esempio, Parameter Store include questo contesto di crittografia nelle chiamate per crittografare e decrittografare il parametro in un esempio e in una regione. MyParameter Account AWS

```
"PARAMETER_ARN": "arn:aws:ssm:us-east-2:111122223333:parameter/MyParameter"
```

Se il parametro è in un percorso gerarchico Parameter Store, il nome e il percorso sono inclusi nel contesto di crittografia. Ad esempio, questo contesto di crittografia viene utilizzato per crittografare e decrittografare il MyParameter parametro nel /ReadableParameters percorso in un esempio e in un'area. Account AWS

```
"PARAMETER_ARN": "arn:aws:ssm:us-east-2:111122223333:parameter/ReadableParameters/
MyParameter"
```

È possibile decrittografare il valore di un `SecureString` parametro crittografato richiamando l'AWS KMS Decrypt operazione con il contesto di crittografia corretto e il valore del parametro crittografato restituito dall'operazione Systems Manager. `GetParameter` Tuttavia, consigliamo di decrittografare i valori dei parametri Parameter Store usando l'operazione `GetParameter` con il parametro `WithDecryption`.

È possibile anche includere il contesto di crittografia nella policy IAM. Ad esempio, è possibile consentire a un utente di decrittografare solo un determinato valore di parametro o un set di valori di parametri.

La seguente istruzione di esempio della policy IAM consente all'utente di ottenere il valore del parametro `MyParameter` e di decrittare il valore utilizzando la chiave KMS specificata. Tuttavia le autorizzazioni si applicano solo quando il contesto di crittografia corrisponde alla stringa specificata.

Queste autorizzazioni non si applicano a qualsiasi altro parametro o chiave KMS e la chiamata a `GetParameter` ha esito negativo se il contesto di crittografia non corrisponde alla stringa.

Prima di utilizzare un'istruzione politica come questa, sostituiscila *example ARNs* con valori validi.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "ssm:GetParameter*"
],
 "Resource": "arn:aws:ssm:us-east-1:111122223333:parameter/MyParameter"
 },
 {
 "Effect": "Allow",
 "Action": [
 "kms:Decrypt"
],
 "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-id",
 "Condition": {
 "StringEquals": {
 "kms:EncryptionContext:PARAMETER_ARN": "arn:aws:ssm:us-east-1:111122223333:parameter/MyParameter"
 }
 }
 }
]
}
```

## Risoluzione dei problemi chiave di KMS in Parameter Store

Per eseguire qualsiasi operazione su un `SecureString` parametro, è Parameter Store necessario essere in grado di utilizzare la chiave AWS KMS KMS specificata per l'operazione prevista. La maggior parte degli errori di Parameter Store relativi alle chiavi KMS sono causati da uno dei seguenti motivi:

- Le credenziali utilizzate da un'applicazione non hanno l'autorizzazione per eseguire l'operazione specificata sulla chiave KMS.

Per risolvere questo errore, eseguire l'applicazione con credenziali differenti o modificare l'IAM o la policy della chiave che impedisce l'operazione. Per assistenza con AWS KMS IAM e le politiche chiave, consulta Accesso con chiave [KMS e autorizzazioni](#) nella Guida per gli AWS Key Management Service sviluppatori.

- La chiave KMS non è stata trovata.

In genere questo accade quando si utilizza un identificatore errato per la chiave KMS. [Trova gli identificatori corretti](#) per la chiave KMS e riprova il comando.

- La chiave KMS non è abilitata. In questo caso, Parameter Store restituisce un'InvalidKeyException con un messaggio di errore dettagliato da AWS KMS. Se lo stato della chiave KMS è Disabled, [abilitalo](#). Se è Pending Import, completa la [procedura di importazione](#). Se lo stato di chiave è Pending Deletion, [annulla l'eliminazione della chiave](#) o utilizza un'altra chiave KMS.

Per trovare lo stato [della](#) chiave di una chiave KMS, usa l'[DescribeKey](#) operazione.

## Utilizzo Parameter Store parametri in Amazon Elastic Kubernetes Service

Per visualizzare i parametri provenienti da Parameter Store uno strumento o da file montati in Amazon EKS Pods AWS Systems Manager, puoi utilizzare AWS Secrets and Configuration Provider for the Kubernetes Secrets Store CSI Driver. L'ASCP funziona con Amazon Elastic Kubernetes Service 1.17+ che esegue un gruppo di nodi Amazon EC2. AWS Fargate i gruppi di nodi non sono supportati.

Con ASCP, è possibile archiviare e gestire il parametro in Parameter Store e recuperarlo tramite i carichi di lavoro in esecuzione su Amazon EKS. Se il tuo parametro contiene molteplici coppie chiave-valore in formato JSON, puoi scegliere quali montare in Amazon EKS. L'ASCP utilizza la sintassi JMESPath per interrogare le coppie chiave-valore nel tuo segreto. L'ASCP funziona anche con AWS Secrets Manager i segreti.

L'ASCP offre due metodi di autenticazione con Amazon EKS. Il primo approccio utilizza i ruoli IAM per gli account di servizio (IRSA). Il secondo approccio utilizza Pod Identity. Ogni approccio ha i suoi vantaggi e casi d'uso.



## ASCP con ruoli IAM per gli account di servizio (IRSA)

L'ASCP con IAM Roles for Service Accounts (IRSA) ti consente di montare parametri da file Parameter Store come nei tuoi Amazon EKS Pod. Questo approccio è adatto quando:

- È necessario montare i parametri come file nei Pod.
- Stai usando la versione 1.17 o quella successiva di Amazon EKS con i gruppi di nodi di Amazon EC2.
- Vuoi recuperare coppie chiave-valore specifiche dai parametri. JSON-formatted

Per ulteriori informazioni, consulta [Utilizzo AWS Segreti e CSI del provider di configurazione con ruoli IAM per gli account di servizio \(IRSA\)](#).

## ASCP con Pod Identity

### [ASCP con EKS Pod Identity](#)

L'ASCP con il metodo Pod Identity migliora la sicurezza e semplifica la configurazione per l'accesso ai parametri in Parameter Store. Questo approccio è utile quando:

- È necessaria una gestione delle autorizzazioni più granulare a livello di pod.
- Stai utilizzando la versione 1.24 o quella successiva di Amazon EKS.
- Desideri prestazioni e scalabilità migliorate.

Per ulteriori informazioni, consulta [Utilizzo AWS Segreti e CSI del provider di configurazione con identità Pod per Amazon EKS](#).

## Scelta dell'approccio giusto

Considera i seguenti fattori al momento di decidere tra ASCP con IRSA e ASCP con Pod Identity:

- Versione di Amazon EKS: Pod Identity richiede la versione 1.24 o quella successiva di Amazon EKS, mentre il driver CSI funziona con la versione 1.17 o quella successiva di Amazon EKS.
- Requisiti di sicurezza: Pod Identity offre un controllo più granulare a livello di pod.
- Prestazioni: Pod Identity generalmente offre prestazioni migliori in ambienti su larga scala.
- Complessità: Pod Identity semplifica la configurazione eliminando la necessità di account di servizio separati.

Scegli il metodo più adatto ai tuoi requisiti specifici e all'ambiente Amazon EKS.

## Installa ASCP per Amazon EKS

Questa sezione spiega come installare AWS Secrets and Configuration Provider per Amazon EKS. Con ASCP, puoi montare parametri Parameter Store e segreti da AWS Secrets Manager file in Amazon EKS Pods.

### Prerequisiti

- Cluster Amazon EKS
  - Versione 1.24 o successiva per Pod Identity
  - Versione 1.17 o successiva per IRSA
- AWS CLI Installato e configurato
- kubectl installato e configurato per il cluster Amazon EKS
- Helm (versione 3.0 o successiva)

### Installa e configura l'ASCP

L'ASCP è disponibile GitHub nel repository [secrets-store-csi-provider-aws](https://github.com/kubernetes-sigs/secrets-store-csi-provider-aws). Il repository contiene anche file YAML di esempio per la creazione e il montaggio di un segreto tramite la modifica del valore objectType da secretsmanager a ssmparameter.

Durante l'installazione, puoi configurare l'ASCP per utilizzare un endpoint FIPS. Per un elenco degli endpoint di Systems Manager, consulta gli [endpoint del servizio di Systems Manager](#) nella Riferimenti generali di Amazon Web Services.

### Installazione dell'ASCP con l'utilizzo di Helm

1. Per assicurarti che il repository punti al grafico più recente, utilizza `helm repo update`.
2. Aggiungi il grafico dei driver CSI di Secrets Store.

```
helm repo add secrets-store-csi-driver https://kubernetes-sigs.github.io/secrets-store-csi-driver/charts
```

3. Installare il grafico. Per configurare la limitazione (della larghezza di banda della rete), aggiungi il seguente flag: `--set-json 'k8sThrottlingParams={"qps": "number of queries per second", "burst": "number of queries per second"}`

```
helm install -n kube-system csi-secrets-store secrets-store-csi-driver/secrets-store-csi-driver
```

#### 4. Aggiungi il grafico ASCP.

```
helm repo add aws-secrets-manager https://aws.github.io/secrets-store-csi-driver-provider-aws
```

#### 5. Installare il grafico. Per utilizzare un endpoint FIPS, aggiungi il seguente flag: `--set useFipsEndpoint=true`

```
helm install -n kube-system secrets-provider-aws aws-secrets-manager/secrets-store-csi-driver-provider-aws
```

### Installazione utilizzando lo YAML nel repository

- Utilizza i seguenti comandi:

```
helm repo add secrets-store-csi-driver https://kubernetes-sigs.github.io/secrets-store-csi-driver/charts
helm install -n kube-system csi-secrets-store secrets-store-csi-driver/secrets-store-csi-driver
kubectl apply -f https://raw.githubusercontent.com/aws/secrets-store-csi-driver-provider-aws/main/deployment/aws-provider-installer.yaml
```

### Verifica le installazioni

Per verificare le installazioni del cluster EKS, del driver CSI di Secrets Store e del plug-in ASCP, procedi nel seguente modo:

#### 1. Verifica il cluster EKS:

```
eksctl get cluster --name clusterName
```

Questo comando deve restituire informazioni sul cluster.

#### 2. Verifica l'installazione del driver CSI di Secrets Store:

```
kubectl get pods -n kube-system -l app=secrets-store-csi-driver
```

Dovresti vedere dei pod in esecuzione con nomi come `csi-secrets-store-secrets-store-csi-driver-xxx`.

### 3. Verifica l'installazione del plugin ASCP:

#### YAML installation

```
$ kubectl get pods -n kube-system -l app=csi-secrets-store-provider-aws
```

Output di esempio:

NAME	READY	STATUS	RESTARTS	AGE
csi-secrets-store-provider-aws-12345	1/1	Running	0	2m

#### Helm installation

```
$ kubectl get pods -n kube-system -l app=secrets-store-csi-driver-provider-aws
```

Output di esempio:

NAME	READY	STATUS	RESTARTS
secrets-provider-aws-secrets-store-csi-driver-provider-67890	1/1	Running	0
AGE	2m		

Dovresti vedere dei pod nello stato Running.

Dopo aver eseguito questi comandi, se tutto è impostato correttamente, dovresti vedere tutti i componenti in esecuzione senza errori. In caso di problemi, potrebbe essere necessario risolverli controllando i log dei pod specifici che presentano problemi.

#### Risoluzione dei problemi

##### 1. Per controllare i log del provider ASCP, esegui:

```
kubectl logs -n kube-system -l app=csi-secrets-store-provider-aws
```

2. Controlla lo stato di tutti i pod nel namespace kube-system.

*default placeholder text* Sostituiscilo con il tuo ID pod:

```
kubectl -n kube-system get pods
```

```
kubectl -n kube-system logs pod/pod-id
```

Tutti i pod relativi al driver CSI e all'ASCP devono essere nello stato "In esecuzione".

3. Controlla la versione del driver CSI:

```
kubectl get csidriver secrets-store.csi.k8s.io -o yaml
```

Questo comando deve restituire informazioni sul driver CSI installato.

## Risorse aggiuntive

Per ulteriori informazioni su come utilizzare ASCP con Amazon EKS, consulta le seguenti risorse:

- [Utilizzo di Pod Identity con Amazon EKS](#)
- [AWS Il driver CSI di Secrets Store è attivo GitHub](#)

## Utilizzo AWS Segreti e CSI del provider di configurazione con identità Pod per Amazon EKS

L'integrazione di AWS Secrets and Configuration Provider con il Pod Identity Agent per Amazon Elastic Kubernetes Service offre sicurezza avanzata, configurazione semplificata e prestazioni migliorate per le applicazioni in esecuzione su Amazon EKS. Pod Identity semplifica l'autenticazione AWS Identity and Access Management (IAM) per Amazon EKS durante il recupero di parametri o segreti da Secrets Manager. AWS Systems Manager Parameter Store

Amazon EKS Pod Identity semplifica il processo di configurazione delle autorizzazioni IAM per le applicazioni Kubernetes consentendo quest'azione direttamente tramite le interfacce Amazon EKS, riducendo il numero di passaggi ed eliminando la necessità di passare da Amazon EKS ai servizi

IAM. [Pod Identity consente l'uso di un singolo ruolo IAM su più cluster senza aggiornare le policy di attendibilità e supporta i tag delle sessioni di ruolo](#) per un controllo degli accessi più granulare. Questo approccio non solo semplifica la gestione delle policy consentendo il riutilizzo delle policy di autorizzazione tra i ruoli, ma migliora anche la sicurezza consentendo l'accesso alle AWS risorse in base ai tag corrispondenti.

Come funziona

1. Pod Identity assegna un ruolo IAM al pod.
2. ASCP utilizza questo ruolo per autenticarsi con. Servizi AWS
3. Se autorizzato, ASCP recupera i parametri richiesti e li rende disponibili al pod.

Per ulteriori informazioni, consulta [Scopri come funziona Amazon EKS Pod Identity](#) nella Guida per l'utente di Amazon EKS.

Prerequisiti

 Important

Pod Identity è supportato solo per Amazon EKS nel cloud. Non è supportato per [Amazon EKS Anywhere](#) o per i cluster [Servizio Red Hat OpenShift su AWS](#) Kubernetes autogestiti sulle istanze Amazon EC2.

- Cluster Amazon EKS (versione 1.24 o successiva)
- Accesso al cluster AWS CLI Amazon EKS tramite `kubectl`
- (Facoltativo) Accesso a due Account AWS per l'accesso tra più account

Installazione dell'agente Amazon EKS Pod Identity

Per utilizzare Pod Identity con il tuo cluster, devi installare il componente aggiuntivo dell'agente Amazon EKS Pod Identity.

Installare l'agente Pod Identity

- Installa il componente aggiuntivo agente Pod Identity sul tuo cluster.

*default placeholder text* Sostituiscili con i tuoi valori:

```
eksctl create addon \
 --name eks-pod-identity-agent \
 --cluster clusterName \
 --region region
```

## Configura ASCP con Pod Identity

1. Crea una policy di autorizzazioni che conceda l'autorizzazione `ssm:GetParameters` e `ssm:DescribeParameters` ai parametri a cui il pod deve accedere.
2. Crea un ruolo IAM che può essere assunto dal servizio principale Amazon EKS per Pod Identity:

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "pods.eks.amazonaws.com"
 },
 "Action": [
 "sts:AssumeRole",
 "sts:TagSession"
]
 }
]
}
```

Allega la policy IAM al ruolo.

Sostituisci il *default placeholder text* con i tuoi valori:

```
aws iam attach-role-policy \
 --role-name MY_ROLE \
 --policy-arn POLICY_ARN
```

3. Crea un'associazione Pod Identity. Per un esempio, consulta [Crea un'associazione Pod Identity](#) nella Guida per l'utente Amazon EKS
4. Crea il `SecretProviderClass` che specifica quali parametri o segreti montare nel pod:

```
kubectl apply -f kubectl apply -f https://raw.githubusercontent.com/aws/secrets-store-csi-driver-provider-aws/main/examples/ExampleSecretProviderClass-PodIdentity.yaml
```

La differenza fondamentale in `SecretProviderClass` tra IRSA e Pod Identity è il parametro `usePodIdentity` facoltativo. Si tratta di un campo facoltativo che determina l'approccio di autenticazione. Quando non è specificato, per impostazione predefinita utilizzare i ruoli IAM per gli account di servizio (IRSA).

- Per utilizzare EKS Pod Identity, utilizza uno qualsiasi di questi valori: "true", "True", "TRUE", "t", "T".
- Per utilizzare in modo esplicito IRSA, imposta uno qualsiasi di questi valori: "false", "False", "FALSE", "f", or "F".

5. Distribuisci il pod che monta i parametri o i segreti in `/mnt/secrets-store`:

```
kubectl apply -f kubectl apply -f https://raw.githubusercontent.com/aws/secrets-store-csi-driver-provider-aws/main/examples/ExampleDeployment-PodIdentity.yaml
```

6. Se utilizzi un cluster Amazon EKS privato, assicurati che il VPC in cui si trova il cluster abbia un AWS STS endpoint. Per informazioni sulla creazione di un endpoint, consulta [Endpoint VPC di interfaccia](#) nella Guida per l'utente AWS Identity and Access Management .

Verifica il montaggio del segreto

Per verificare che il parametro o il segreto siano montati correttamente, eseguire il comando riportato di seguito.

Sostituiscili *default placeholder text* con i tuoi valori:

```
kubectl exec -it $(kubectl get pods | awk '/pod-identity-deployment/{print $1}' | head -1) -- cat /mnt/secrets-store/MyParameter
```



Per configurare Amazon EKS Pod Identity per accedere ai parametri in Parameter Store

1. Crea una policy di autorizzazioni che conceda l'autorizzazione `ssm:GetParameters` e `ssm:DescribeParameters` ai parametri a cui il pod deve accedere.
2. Crea un parametro in Parameter Store se non ne hai già uno. Per informazioni, consulta [Creazione in corso Parameter Store parametri in Systems Manager](#).

## Risoluzione dei problemi

È possibile visualizzare la maggior parte degli errori descrivendo l'implementazione del pod.

Per visualizzare i messaggi di errore per il container

1. È possibile ottenere un elenco di nomi di pod con il comando seguente. Se non si sta utilizzando il namespace predefinito, utilizzare `-n namespace`.

```
kubectl get pods
```

2. Per descrivere il Pod, nel comando seguente, `pod-id` utilizza l'ID Pod dei Pod che hai trovato nel passaggio precedente. Se non si sta utilizzando lo spazio dei nomi predefinito, utilizzare `-n NAMESPACE`.

```
kubectl describe pod/pod-id
```

Come visualizzare gli errori per l'ASCP

- Per trovare maggiori informazioni nei log del provider, nel comando seguente, `PODID` utilizza l'ID del Pod `csi-secrets-store-provider-aws`.

```
kubectl -n kube-system get pods
kubectl -n kube-system logs pod/pod-id
```

## Utilizzo AWS Segreti e CSI del provider di configurazione con ruoli IAM per gli account di servizio (IRSA)

### Prerequisiti

- Cluster Amazon EKS (versione 1.17 o successiva)

- Accesso AWS CLI e cluster Amazon EKS tramite `kubectl`

## Configurazione del controllo degli accessi

L'ASCP recupera il Pod Identity di Amazon EKS e lo scambia con il ruolo IAM. Le autorizzazioni vengono impostate in una policy IAM per quel ruolo IAM. Quando l'ASCP assume il ruolo IAM, ottiene l'accesso ai parametri autorizzati. Altri container non possono accedere ai parametri a meno che non vengano associati anche al ruolo IAM.

Per concedere al tuo Amazon EKS Pod l'accesso ai parametri in Parameter Store

1. Crea una policy di autorizzazioni che conceda l'autorizzazione `ssm:GetParameters` e `ssm:DescribeParameters` ai parametri a cui il pod deve accedere.
2. Crea un provider OpenID Connect (OIDC) IAM per il cluster se non ne è già presente uno. Per ulteriori informazioni, consulta [Crea un provider IAM OIDC per il tuo cluster](#) nella Guida per l'utente di Amazon EKS.
3. Crea un [Ruolo IAM per l'account del servizio](#) e collega la policy ad esso. Per ulteriori informazioni, consulta [Crea un ruolo IAM per un account del servizio](#) nella Guida per l'utente di Amazon EKS.
4. Se utilizzi un cluster Amazon EKS privato, assicurati che il VPC in cui si trova il cluster abbia un AWS STS endpoint. Per informazioni sulla creazione di un endpoint, consulta [Endpoint VPC di interfaccia](#) nella Guida per l'utente AWS Identity and Access Management .

## Identifica i parametri da montare

Per determinare quali parametri monta l'ASCP in Amazon EKS come file sul file system, è necessario creare un file [SecretProviderClass](#) YAML. Il `SecretProviderClass` elenca i parametri da montare e il nome del file con cui montarli. Il `SecretProviderClass` deve trovarsi nello stesso namespace del pod Amazon EKS a cui fa riferimento.

## Monta i parametri come file

Le seguenti istruzioni mostrano come montare i parametri come file utilizzando file YAML di esempio e. [ExampleSecretProviderClass.yaml](#) [ExampleDeployment.yaml](#)

Per montare i parametri in Amazon EKS

1. Applica il `SecretProviderClass` al pod:

```
kubectl apply -f ExampleSecretProviderClass.yaml
```

## 2. Distribuisci il pod:

```
kubectl apply -f ExampleDeployment.yaml
```

## 3. L'ASCP monta i file.

### Risoluzione dei problemi

È possibile visualizzare la maggior parte degli errori descrivendo l'implementazione del pod.

Per visualizzare i messaggi di errore per il container

1. È possibile ottenere un elenco di nomi di pod con il comando seguente. Se non si sta utilizzando il namespace predefinito, utilizzare -n *name-space*.

```
kubectl get pods
```

2. Per descrivere il Pod, nel comando seguente, *pod-id* utilizza l'ID del Pod dei Pod che hai trovato nel passaggio precedente. Se non si sta utilizzando lo spazio dei nomi predefinito, utilizzare -n *nameSpace*.

```
kubectl describe pod/pod-id
```

### Come visualizzare gli errori per l'ASCP

- Per trovare maggiori informazioni nei log del provider, nel comando seguente, *pod-id* utilizza l'ID del Pod `csi-secrets-store-provider-aws`.

```
kubectl -n kube-system get pods
kubectl -n kube-system logs Pod/pod-id
```

- Verifica che il **SecretProviderClass** sia installato:

```
kubectl get crd secretproviderclasses.secrets-store.csi.x-k8s.io
```

Questo comando deve restituire informazioni sulla definizione delle risorse personalizzate `SecretProviderClass`.

- `SecretProviderClass` Verifica che l'oggetto sia stato creato.

```
kubectl get secretproviderclass SecretProviderClassName -o yaml
```

## AWS Segreti ed esempi di codice del provider di configurazione

### Esempi di autenticazione e controllo degli accessi ASCP

Esempio: policy IAM che consente al servizio Amazon EKS Pod Identity (`pods.eks.amazonaws.com`) di assumere il ruolo e contrassegnare la sessione:

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "pods.eks.amazonaws.com"
 },
 "Action": [
 "sts:AssumeRole",
 "sts:TagSession"
]
 }
]
}
```

### SecretProviderClass

Puoi utilizzare YAML per descrivere quali parametri montare in Amazon EKS utilizzando l'ASCP. Per alcuni esempi, consulta [SecretProviderClass utilizzo](#).

## SecretProviderClass Struttura YAML

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
 name: name
spec:
 provider: aws
 parameters:
 region:
 failoverRegion:
 pathTranslation:
 usePodIdentity:
 preferredAddressType:
 objects:
```

Il campo parametri contiene i dettagli della richiesta di montaggio:

### region

(Facoltativo) Il valore Regione AWS del parametro. Se non utilizzi questo campo, l'ASCP cerca la Regione dall'annotazione sul nodo. Questa ricerca aggiunge un sovraccarico alle richieste di montaggio, quindi consigliamo di fornire la Regione per i cluster che utilizzano un numero elevato di pod.

Se specifichi anche il `failoverRegion`, l'ASCP tenta di recuperare il parametro da entrambe le Regioni. Se una delle Regioni restituisce un errore 4xx, ad esempio per un problema di autenticazione, l'ASCP non monta nessuno dei due parametri. Se il parametro viene recuperato correttamente da `region`, l'ASCP monta quel valore del parametro. Se il parametro non viene recuperato correttamente da `region`, ma viene correttamente recuperato da `failoverRegion`, l'ASCP monta quel valore del parametro.

### failoverRegion

(Facoltativo) Se si include questo campo, l'ASCP tenta di recuperare il parametro dalle Regioni definite in `region` e in questo campo. Se una delle Regioni restituisce un errore 4xx, ad esempio per un problema di autenticazione, l'ASCP non monta nessuno dei due parametri. Se il parametro viene recuperato correttamente da `region`, l'ASCP monta quel valore del parametro. Se il parametro non viene recuperato correttamente da `region`, ma viene correttamente recuperato da `failoverRegion`, l'ASCP monta quel valore del parametro. Per un esempio su come utilizzare questo campo, consulta la sezione [Multi-Region failover dei parametri](#).

## pathTranslation

(Facoltativo) Un singolo carattere di sostituzione da utilizzare se il nome del file in Amazon EKS conterrà il carattere separatore di percorso, come barra (/) su Linux. L'ASCP non è in grado di creare un file montato che contiene un carattere separatore di percorso. Invece, l'ASCP sostituisce il carattere separatore di percorso con un carattere diverso. Se non utilizzi questo campo, il carattere sostitutivo è il carattere di sottolineatura (\_), quindi ad esempio, `My/Path/Parameter` monta come `My_Path_Parameter`.

Per impedire la sostituzione dei caratteri, immettere la stringa `False`.

## **usePodIdentity**

(Facoltativo) Determina l'approccio di autenticazione. Se non specificato, il valore predefinito è ruoli IAM per gli account di servizio (IRSA).

- Per utilizzare EKS Pod Identity, utilizza uno qualsiasi di questi valori: `"true"`, `"True"`, `"TRUE"`, `"t"` o `"T"`.
- Per utilizzare in modo esplicito IRSA, imposta uno qualsiasi dei seguenti valori: `"false"`, `"False"`, `"FALSE"`, `"f"`, or `"F"`.

## **preferredAddressType**

(Facoltativo) Specifica il tipo di indirizzo IP preferito per la comunicazione con gli endpoint dell'agente Pod Identity. Il campo è applicabile solo quando si utilizza la funzionalità EKS Pod Identity e verrà ignorato quando si utilizza IAM I ruoli for Service non Accounts. Values fanno distinzione tra maiuscole e minuscole. I valori validi sono:

- `"ipv4"`, `"IPv4"` oppure `"IPV4"`: forza l'uso dell'endpoint IPv4 dell'agente Pod Identity
- `"ipv6"`, `"IPv6"` oppure `"IPV6"`: forza l'uso dell'endpoint IPv6 dell'agente Pod Identity
- non specificato: utilizza la selezione automatica degli endpoint, provando prima l'endpoint IPv4 e tornando all'endpoint IPv6, se IPv4 dà errore

## objects

Una stringa contenente una dichiarazione YAML dei segreti da montare. Si consiglia di utilizzare una stringa multiriga YAML o un carattere pipe (`()`).

## objectName

Obbligatorio. Specifica il nome del parametro o del segreto da recuperare. Per `Parameter Store`, questo è il [Name](#) del parametro e può essere sia il nome che l'ARN completo del

parametro. Per Secrets Manager questo è il parametro [SecretId](#) e può essere sia il nome descrittivo sia l'ARN completo del segreto.

#### objectType

Obbligatorio se non si utilizza un ARN di Secrets Manager per `objectName`. Per Parameter Store, utilizza `ssmparameter`. Per Secrets Manager, utilizza `secretsmanager`.

#### objectAlias

(Facoltativo) Il nome file del segreto nel pod Amazon EKS. Se non indichi questo campo, `objectName` viene visualizzato come nome del file.

#### objectVersion

(Facoltativo) Il numero ID del parametro. Non è consigliato, perché è necessario aggiornare l'ID di versione ogni volta che si aggiorna il parametro. Per impostazione predefinita viene utilizzata la versione più recente. Se includi un `failoverRegion`, questo campo rappresenta l'`objectVersion` primario.

#### oggetto VersionLabel

(Facoltativo) L'alias per la versione. Il valore predefinito è la versione più recente `AWSCURRENT`. Se includi un `failoverRegion`, questo campo rappresenta l'`objectVersionLabel` primario.

#### jmesPath

(Facoltativo) Una mappa delle chiavi nel parametro per i file da montare in Amazon EKS. Per utilizzare questo campo, il valore del parametro deve essere in formato JSON.

L'esempio seguente mostra l'aspetto di un parametro codificato JSON.

```
{
 "username" : "myusername",
 "password" : "mypassword"
}
```

Le chiavi sono `username` e `password`. Il valore associato a `username` è `myusername` e il valore associato a `password` è `mypassword`.

Se si utilizza questo campo, è necessario includere i sottocampi `path` e `objectAlias`.

## path

Una chiave di una coppia chiave-valore nel JSON del valore del parametro. Se il campo contiene un trattino, usa le virgolette singole per evitarlo, ad esempio: `path: '"hyphenated-path"'`

## objectAlias

Il nome del file da montare nel pod Amazon EKS. Se il campo contiene un trattino, usa le virgolette singole per evitarlo, ad esempio: `objectAlias: '"hyphenated-alias"'`

## **failoverObject**

(Facoltativo) Se specifichi questo campo, l'ASCP tenta di recuperare sia il parametro specificato nel campo `objectName` primario che quello specificato nel sottocampo `failoverObject objectName`. Se uno dei due restituisce un errore 4xx, ad esempio per un problema di autenticazione, l'ASCP non monta nessuno dei due parametri. Se si riesce a recuperare il parametro dal `objectName` primario, l'ASCP monta quel valore del parametro. Se il parametro non viene recuperato correttamente dal `objectName` primario, ma viene recuperato correttamente dal `objectName` di failover, l'ASCP monta quel valore del parametro. Se si include questo campo, è necessario includere il campo `objectAlias`. Per un esempio su come utilizzare questo campo, consulta la sezione [Failover su un parametro diverso](#).

In genere, si utilizza questo campo quando il parametro di failover non è una replica. Per un esempio su come specificare una replica, consulta la sezione [Multi-Region failover dei parametri](#).

## objectName

Il nome o l'ARN completi del parametro di failover. Se utilizzi un ARN, la Regione nell'ARN deve corrispondere al campo `failoverRegion`.

## objectVersion

(Facoltativo) Il numero ID del parametro. Deve corrispondere all'`objectVersion` primaria. Non è consigliato, perché è necessario aggiornare l'ID di versione ogni volta che si aggiorna il parametro. Per impostazione predefinita viene utilizzata la versione più recente.

## oggetto VersionLabel

(Facoltativo) L'alias per la versione. Il valore predefinito è la versione più recente `AWSCURRENT`.



Crea una `SecretProviderClass` configurazione di base per montare i parametri nei tuoi Amazon EKS Pods.

## Pod Identity

`SecretProviderClass` per utilizzare un parametro nello stesso cluster Amazon EKS:

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
 name: aws-parameter-store
spec:
 provider: aws
 parameters:
 objects: |
 - objectName: "MyParameter"
 objectType: "ssmparameter"
 usePodIdentity: "true"
```

## IRSA

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
 name: deployment-aws-parameter
spec:
 provider: aws
 parameters:
 objects: |
 - objectName: "MyParameter"
 objectType: "ssmparameter"
```

## SecretProviderClass utilizzo

Usa questi esempi per creare configurazioni `SecretProviderClass` per diversi scenari.

Esempio: montaggio di parametri per nome o ARN

Questo esempio mostra come montare tre diversi tipi di parametri:

- Un parametro specificato dall'ARN completo

- Un parametro specificato dal nome
- Una versione parametrica di un segreto

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
 name: aws-parameters
spec:
 provider: aws
 parameters:
 objects: |
 - objectName: "arn:aws:ssm:us-east-2:777788889999:parameter:MyParameter2-d4e5f6"
 - objectName: "MyParameter3"
 objectType: "ssmparameter"
 - objectName: "MyParameter4"
 objectType: "ssmparameter"
 objectVersionLabel: "AWSCURRENT"
```

Esempio: montaggio di coppie chiave-valore da un parametro

Questo esempio mostra come montare coppie chiave-valore specifiche da un JSON-formatted parametro:

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
 name: aws-parameters
spec:
 provider: aws
 parameters:
 objects: |
 - objectName: "arn:aws:ssm:us-east-2:777788889999:parameter:MyParameter-a1b2c3"
 jmesPath:
 - path: username
 objectAlias: dbusername
 - path: password
 objectAlias: dbpassword
```

Esempio: esempi di configurazione di failover

Questi esempi mostrano come configurare il failover per i parametri.

## Multi-Region failover dei parametri

Questo esempio mostra come configurare il failover automatico per un parametro replicato su più regioni:

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
 name: aws-parameters
spec:
 provider: aws
 parameters:
 region: us-east-1
 failoverRegion: us-east-2
 objects: |
 - objectName: "MyParameter"
```

## Failover su un parametro diverso

Questo esempio mostra come configurare il failover su un parametro diverso (non una replica):

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
 name: aws-parameters
spec:
 provider: aws
 parameters:
 region: us-east-1
 failoverRegion: us-east-2
 objects: |
 - objectName: "arn:aws:ssm:us-east-1:777788889999:parameter:MyParameter-a1b2c3"
 objectAlias: "MyMountedParameter"
 failoverObject:
 - objectName: "arn:aws:ssm:us-
east-2:777788889999:parameter:MyFailoverParameter-d4e5f6"
```

## Risorse aggiuntive

Per ulteriori informazioni su come utilizzare ASCP con Amazon EKS, consulta le seguenti risorse:

- [Utilizzo di Pod Identity con Amazon EKS](#)
- [AWS Secrets Store CSI Driver attivo GitHub](#)

## Utilizzo Parameter Store parametri in AWS Lambda funzioni

Parameter Store consente di archiviare, organizzare e recuperare in modo sicuro i dati di configurazione su larga scala. Supporta un'ampia gamma di casi d'uso, dalla gestione dei valori di configurazione in testo normale, come le stringhe di connessione al database e le impostazioni delle applicazioni, alla gestione di dati sensibili come segreti per ambienti a basso rischio. Parameter Store è progettato per semplificare la gestione della configurazione tra gli ambienti, consentendo ai team di standardizzare il modo in cui le applicazioni accedono ai dati critici senza codificare i valori o affidarsi a soluzioni di storage frammentate.

Se gestisci credenziali che richiedono la rotazione automatica, l'accesso tra più account o una registrazione di controllo granulare, ti consigliamo di utilizzarle. [AWS Secrets Manager](#) Secrets Manager è stato creato appositamente per la gestione di informazioni segrete quali credenziali di database, chiavi API e informazioni segrete supportate da software di terze parti. Per ulteriori informazioni, vedi [Che cos'è? AWS Secrets Manager](#) nella Guida AWS Secrets Manager per l'utente.

Per utilizzare Parameter Store i parametri nelle AWS Lambda funzioni senza utilizzare un SDK, puoi utilizzare l'estensione Lambda AWS Parameters and Secrets. Questa estensione recupera i valori dei parametri e li memorizza nella cache per usarli in futuro. L'utilizzo dell'estensione Lambda può ridurre i costi riducendo il numero di chiamate API a Parameter Store. Può inoltre migliorare la latenza perché il recupero di un parametro memorizzato nella cache è più rapido rispetto al recupero da Parameter Store.

Un'estensione Lambda è un processo complementare che si aggiunge alle funzionalità di una normale funzione Lambda. Un'estensione è come un client che viene eseguito in parallelo a una chiamata Lambda. Questo client parallelo può interfacciarsi con la funzione in qualsiasi momento del suo ciclo di vita. Per ulteriori informazioni sulle estensioni Lambda, consulta [API delle estensioni Lambda](#) nella Guida per gli sviluppatori di AWS Lambda .

L'estensione Lambda AWS Parameters and Secrets funziona sia per che. Parameter Store AWS Secrets Manager Per sapere come utilizzare l'estensione Lambda con i segreti di Secrets Manager, consulta [Usare AWS Secrets Manager i segreti nelle AWS Lambda funzioni](#) nella Guida per l'AWS Secrets Manager utente.

Informazioni correlate

[Utilizzo dell'estensione AWS Parameter and Secrets Lambda per memorizzare nella cache parametri e segreti](#) (AWS Compute Blog)

## Come funziona l'estensione

Per utilizzare i parametri in una funzione Lambda senza l'estensione Lambda, devi configurare la funzione Lambda in modo da ricevere gli aggiornamenti di configurazione mediante l'integrazione con l'operazione API `GetParameter` per Parameter Store.

Quando si utilizza l'estensione Lambda AWS Parameters and Secrets, l'estensione recupera il valore del parametro Parameter Store e lo memorizza nella cache locale. Quindi, il valore memorizzato nella cache viene utilizzato per ulteriori invocazioni fino alla scadenza. I valori memorizzati nella cache scadono una volta raggiunto il time-to-live (TTL). È possibile configurare il valore TTL utilizzando la [variabile d'ambiente](#) `SSM_PARAMETER_STORE_TTL`, come spiegato più avanti in questo argomento.

Se il TTL della cache configurata non è scaduto, sarà utilizzato il valore del parametro memorizzato nella cache. Se il tempo è scaduto, il valore memorizzato nella cache viene invalidato e il valore del parametro sarà recuperato da Parameter Store.

Inoltre, il sistema rileva i valori dei parametri utilizzati di frequente e li mantiene nella cache mentre cancella quelli scaduti o non utilizzati.

### Dettagli di implementazione

Utilizza i seguenti dettagli per aiutarti a configurare l'estensione Lambda AWS Parameters and Secrets.

### Autenticazione

Per autorizzare e autenticare le richieste Parameter Store, l'estensione utilizza le stesse credenziali utilizzate per eseguire la funzione Lambda stessa. Pertanto, il ruolo AWS Identity and Access Management (IAM) utilizzato per eseguire la funzione deve disporre delle seguenti autorizzazioni con cui interagire: Parameter Store

- `ssm:GetParameter`: obbligatorio per recuperare i parametri da Parameter Store
- `kms:Decrypt`: obbligatorio se stai recuperando i parametri `SecureString` da Parameter Store

Per ulteriori informazioni, consulta [Ruolo di esecuzione di AWS Lambda](#) nella Guida per gli sviluppatori di AWS Lambda .

### Istanziamento

Per la maggior parte delle funzioni Lambda, Lambda crea istanze separate corrispondenti al livello di concorrenza richiesto dalla funzione. Ogni istanza è isolata e mantiene la propria cache locale

dei dati di configurazione. Per ulteriori informazioni sulle istanze Lambda e sulla simultaneità, consulta [Configurazione della simultaneità riservata](#) nella Guida per gli sviluppatori di AWS Lambda .

Per le funzioni che utilizzano Lambda Managed Instances, un singolo ambiente di esecuzione serve più invocazioni simultanee, quindi tali invocazioni condividono un'istanza dell'estensione e una cache locale. Per ulteriori informazioni, consulta [Lambda Managed Instances nella Developer Guide](#). AWS Lambda

Nessuna dipendenza dall'SDK

L'estensione Lambda AWS Parameters and Secrets funziona indipendentemente da qualsiasi libreria di linguaggi AWS SDK. Non è necessario un AWS SDK per effettuare richieste GET a. Parameter Store Tuttavia, consigliamo di utilizzare un AWS SDK per recuperare il token di sessione per l'intestazione della richiesta, come descritto più avanti in questo argomento.

Porta Localhost

Utilizza `localhost` nelle tue richieste GET. L'estensione effettua le richieste alla porta 2773 di localhost. Per utilizzare l'estensione, non è necessario specificare un endpoint esterno o interno. È possibile configurare la porta impostando la [variabile di ambiente](#) `PARAMETERS_SECRETS_EXTENSION_HTTP_PORT`.

Ad esempio, in Python, il tuo URL GET potrebbe avere un aspetto simile al seguente esempio.

```
parameter_url = ('http://localhost:' + port + '/systemsmanager/parameters/get/?
name=' + ssm_parameter_path)
```

Modifiche al valore di un parametro prima della scadenza del TTL

L'estensione non rileva le modifiche al valore del parametro e non esegue un aggiornamento automatico prima della scadenza del TTL. Se modifichi il valore di un parametro, le operazioni che utilizzano il valore del parametro memorizzato nella cache potrebbero avere esito negativo fino al successivo aggiornamento della cache. Se prevedi modifiche frequenti al valore di un parametro, ti consigliamo di impostare un valore TTL più breve.

Richiesta dell'intestazione

Per recuperare i parametri dalla cache delle estensioni, l'intestazione della richiesta GET deve includere un riferimento `X-Aws-Parameters-Secrets-Token`. Imposta il token sul token di sessione della tua funzione. Per la maggior parte delle funzioni, questo è fornito nella variabile

di `AWS_SESSION_TOKEN` ambiente. Tuttavia, Lambda non imposta questa variabile di ambiente in tutte le modalità di inizializzazione. Ad esempio, se la tua funzione utilizza SnapStart, ottiene invece le credenziali da un endpoint del contenitore. Per recuperare il token di sessione in modo affidabile in tutte le modalità di inizializzazione, leggete il token dalla catena di fornitori di credenziali di un AWS SDK anziché dalla variabile di ambiente. Questa intestazione indica che la richiesta proviene dall'ambiente Lambda.

## Esempio

L'esempio seguente in Python mostra una richiesta di base per recuperare il valore di un parametro memorizzato nella cache. Risolve il token di sessione all'interno della funzione handler, non al momento dell'inizializzazione, in modo che il token rimanga aggiornato dopo un ripristino. SnapStart

```
import urllib.request
import urllib.error
import json
import boto3

def lambda_handler(event, context):
 # Resolve the session token from the credential provider chain so that this
 # works across all initialization modes, including SnapStart.
 credentials = boto3.Session().get_credentials()
 if credentials is None:
 raise RuntimeError('Failed to resolve AWS credentials')
 session_token = credentials.get_frozen_credentials().token

 # Retrieve /my/parameter from Parameter Store using extension cache
 req = urllib.request.Request('http://localhost:2773/systemsmanager/parameters/
get?name=%2Fmy%2Fparameter')
 req.add_header('X-Aws-Parameters-Secrets-Token', session_token)
 try:
 config = urllib.request.urlopen(req).read()
 except urllib.error.URLError as e:
 raise RuntimeError('Failed to retrieve parameter') from e

 return json.loads(config)
```

## Supporto ARM

L'estensione supporta l'architettura ARM nella maggior parte delle Regioni AWS in cui sono supportate le architetture x86\_64 e x86. Quando si vuole utilizzare l'architettura ARM, suggeriamo

di verificare che la propria architettura sia supportata. Per un elenco completo degli ARN di estensione, consulta [AWS Parametri e segreti Lambda Extension ARN](#).

## Registrazione dei log

Lambda registra le informazioni di esecuzione sull'estensione insieme alla funzione utilizzando Amazon Logs. CloudWatch Per impostazione predefinita, l'estensione registra una quantità minima di informazioni su CloudWatch. Per registrare ulteriori dettagli, imposta la [variabile di ambiente](#) `PARAMETERS_SECRETS_EXTENSION_LOG_LEVEL` su `DEBUG`.

## Aggiunta dell'estensione a una funzione Lambda

Per utilizzare l'estensione Lambda AWS Parameters and Secrets, aggiungi l'estensione alla tua funzione Lambda come livello.

Per aggiungere l'estensione alla funzione,utilizza uno dei metodi descritti di seguito.

### Console di gestione AWS (opzione Aggiungi livello)

1. Apri la AWS Lambda console all'indirizzo <https://console.aws.amazon.com/lambda/>.
2. Scegliere la funzione. Nell'area Livelli, scegli Aggiungi un livello.
3. Nell'area Scegli un livello, scegli l'opzione livelli AWS .
4. Per i AWS livelli, scegli AWS- Parameters-and-Secrets-Lambda-Extension, scegli una versione, quindi scegli Aggiungi.

### Console di gestione AWS (Specifica l'opzione ARN)

1. Apri la AWS Lambda console all'indirizzo. <https://console.aws.amazon.com/lambda/>
2. Scegliere la funzione. Nell'area Livelli, scegli Aggiungi un livello.
3. Nell'area Scegli un livello, scegli l'opzione Specifica un ARN.
4. Per Specifica un ARN, inserisci l'[estensione ARN per la tua Regione AWS architettura](#), quindi scegli Aggiungi.

## AWS Command Line Interface

Esegui il comando seguente nell' AWS CLI. Sostituisci ogni *example resource placeholder* con le tue informazioni.

```
aws lambda update-function-configuration \
 --function-name function-name \
 --layers layer-ARN
```



## Informazioni correlate

### [Uso dei livelli con la funzione Lambda](#)

### [Configurazione delle estensioni \(archivio di file .zip\)](#)

## AWS Parametri e segreti: variabili di ambiente Lambda Extension

È possibile configurare l'estensione modificando le seguenti variabili di ambiente. Per visualizzare le impostazioni correnti, imposta `PARAMETERS_SECRETS_EXTENSION_LOG_LEVEL` su `DEBUG`. Per ulteriori informazioni, consulta [Utilizzo delle variabili di AWS Lambda ambiente](#) nella Guida per gli AWS Lambda sviluppatori.

#### Note

AWS Lambda registra i dettagli operativi sull'estensione Lambda e sulla funzione Lambda in Amazon CloudWatch Logs.

Variabile di ambiente	Informazioni	Richiesto	Valori validi	Valore predefinito
<code>SSM_PARAMETER_STORE_TIMEOUT_MILLIS</code>	Il timeout, in millisecondi, per le richieste a Parameter Store.  Il valore 0 (zero) indica l'assenza di timeout.	No	Tutti i numeri interi	0 (zero)
<code>SECRETS_MANAGER_TIMEOUT_MILLIS</code>	Il timeout, in millisecondi, per le richieste a Gestione dei segreti.	No	Tutti i numeri interi	0 (zero)

Variabile di ambiente	Informazioni	Richiesto	Valori validi	Valore predefinito
	Il valore 0 (zero) indica l'assenza di timeout.			
SSM_PARAMETER_STORE_TTL	La durata massima valida, in secondi, di un parametro nella cache prima che venga invalidato. Un valore pari a 0 (zero) indica che la cache deve essere bypassata. Questa variabile viene ignorata se il valore per <code>PARAMETER_STORE_EXTENSION_CACHE_SIZE</code> è 0 (zero).	No	Da 0 (zero) a 300 s (cinque minuti)	300 s (cinque minuti)

Variabile di ambiente	Informazioni	Richiesto	Valori validi	Valore predefinito
SECRETS_MANAGER_TTL	La durata massima valida, in secondi, di un parametro nella cache prima che venga invalidato. Un valore pari a 0 (zero) indica che la cache è bypassata. Questa variabile viene ignorata se il valore per PARAMETER_STORE_SECRETS_EXTENSION_CACHE_SIZE è 0 (zero).	No	Da 0 (zero) a 300 s (cinque minuti)	300 s (5 minuti)
PARAMETER_STORE_SECRETS_EXTENSION_CACHE_ENABLED	Determina se la cache per l'estensione è abilitata. Valori del valore: TRUE   FALSE	No	TRUE   FALSE	TRUE

Variabile di ambiente	Informazioni	Richiesto	Valori validi	Valore predefinito
PARAMETER_STORE_EXTENSION_CACHE_SIZE	La dimensione massima della cache in termini di numero di elementi. Un valore pari a 0 (zero) indica che la cache è bypassata. Questa variabile viene ignorata se entrambi i valori TTL della cache sono 0 (zero).	No	Da 0 (zero) a 1000	1000
PARAMETER_STORE_EXTENSION_HTTP_PORT	La porta per il server HTTP locale.	No	1 - 65535	2773

Variabile di ambiente	Informazioni	Richiesto	Valori validi	Valore predefinito
PARAMETER_STORE_EXTENSION_MAX_CONNECTIONS	Numero massimo di connessioni per i client HTTP utilizzati dall'estensione per effettuare richieste a Parameter Store o a Gestione dei segreti. Si tratta di una configurazione per client per il numero di connessioni che sia il client di Secrets Manager che il client Parameter Store effettuano ai servizi di backend.	No	Minimo 1; nessun limite massimo.	3

Variabile di ambiente	Informazioni	Richiesto	Valori validi	Valore predefinito
PARAMETER_STORE_EXTENSION_LOG_LEVEL	<p>Il livello di dettaglio riportato nei log per l'estensione.</p> <p>Consigliamo di utilizzare DEBUG per maggiori dettagli sulla configurazione della cache durante la configurazione e il test dell'estensione.</p> <p>I log per le operazioni Lambda vengono automaticamente inviati a un gruppo di CloudWatch log associato.</p>	No	DEBUG   WARN   ERROR   NONE   INFO	INFO

## Comandi di esempio per l'utilizzo di AWS Systems Manager Parameter Store and AWS Secrets Manager Estensione

Gli esempi in questa sezione illustrano le azioni API da utilizzare con l' AWS Secrets Manager estensione AWS Systems Manager Parameter Store and.

## Comandi di esempio per Parameter Store

L'estensione Lambda utilizza l'accesso in sola lettura all'GetParameterazione API.

Per chiamare questa operazione, effettua una chiamata HTTP GET simile alla seguente. Questo formato di comando consente l'accesso ai parametri del livello di parametri standard.

```
GET http://localhost:port/systemsmanager/parameters/get?name=parameter-name&version=version&label=label&withDecryption={true|false}
```

In questo esempio, *parameter-name* rappresenta il nome completo del parametro. Per un parametro non presente in una gerarchia, usa un nome come `MyParameter`. Per un parametro gerarchico, usa il URL-encoded percorso, ad esempio per. `%2FDev%2FProduction%2FEast%2FProject-ABC%2FMyParameter` /Dev/Production/East/Project-ABC/MyParameter

### Note

Quando utilizzi le chiamate GET, i valori dei parametri devono essere codificati in modo che HTTP conservi caratteri speciali. Ad esempio, invece di formattare un percorso gerarchico come `/a/b/c`, codifica caratteri che potrebbero essere interpretati come parte dell'URL, come `%2Fa%2Fb%2Fc`.

*versione* *label* sono i selettori disponibili per l'uso con l'azione. `GetParameter`

```
GET http://localhost:port/systemsmanager/parameters/get/?name=MyParameter&version=5
```

Per chiamare un parametro in una gerarchia, effettuate una chiamata HTTP GET simile alla seguente.

```
GET http://localhost:port/systemsmanager/parameters/get?name=%2Fa%2Fb%2F&label=release
```

Per chiamare un parametro pubblico (globale), effettuate una chiamata HTTP GET simile alla seguente.

```
GET http://localhost:port/systemsmanager/parameters/get/?name=%2Faws%2Fservice%20list%2F...
```

Per effettuare una chiamata HTTP GET a un segreto di Gestione dei segreti utilizzando i riferimenti Parameter Store, effettua una chiamata HTTP GET simile alla seguente.

```
GET http://localhost:port/systemsmanager/parameters/get?name=%2Faws%2Freference%2Fsecretsmanager%2F...
```

Per effettuare una chiamata utilizzando il nome della risorsa Amazon (ARN) per un parametro, effettua una chiamata HTTP GET simile alla seguente.

```
GET http://localhost:port/systemsmanager/parameters/get?name=arn:aws:ssm:us-east-1:123456789012:parameter/MyParameter
```

Per effettuare una chiamata che accede a un parametro SecureString con decrittografia, effettua una chiamata HTTP GET simile alla seguente.

```
GET http://localhost:port/systemsmanager/parameters/get?name=MyParameter&withDecryption=true
```

È possibile specificare che i parametri non vengano decrittografati omettendo `withDecryption` o impostandolo esplicitamente su `false`. È possibile anche specificare una versione o un'etichetta, ma non entrambe. In questo caso, sarà utilizzato solo la prima di queste inserita dopo il punto interrogativo (?) nell'URL.

## AWS Parametri e segreti Lambda Extension ARN

L'ultimo Amazon Resource Name (ARN) per l'estensione Lambda viene pubblicato come parametro pubblico in Systems Manager Parameter Store per ogni architettura supportata. Puoi recuperare l'ARN più recente a livello di codice utilizzando AWS CLI o CloudFormation per assicurarti che l'applicazione faccia sempre riferimento alla versione dell'estensione più recente senza aggiornamenti manuali. Questa sezione spiega come recuperare l'ARN a livello di codice e fornisce tabelle che elencano i valori ARN correnti per ciascuna architettura come riferimento manuale.

### Recupero della versione ARN più recente dell'estensione Lambda

Le ultime versioni ARN dell'estensione Lambda vengono archiviate come parametri pubblici nelle seguenti posizioni. Puoi fare riferimento a questi parametri pubblici nel tuo codice per recuperarli:

- `x86_64://aws-parameters-and-secrets-lambda- /latest aws/service extension/x86`
- `arm64://aws/service/aws-parameters-and-secrets-lambda- extension/arm64 /latest`



## AWS CLI

Per recuperare le ultime versioni di ARN utilizzando il, esegui i seguenti comandi. AWS CLI

x86\_64

```
aws ssm get-parameter --name "/aws/service/aws-parameters-and-secrets-lambda-extension/x86/latest" --query "Parameter.Value" --output text
```

arm64

```
aws ssm get-parameter --name "/aws/service/aws-parameters-and-secrets-lambda-extension/arm64/latest" --query "Parameter.Value" --output text
```

## AWS CloudFormation

Quando si distribuiscono funzioni Lambda utilizzando CloudFormation, è possibile risolvere i parametri direttamente durante la creazione e gli aggiornamenti dello stack, come mostrato nel seguente esempio di modelli YAML. Questo metodo garantisce che la funzione utilizzi sempre l'ultima versione dell'estensione senza richiedere aggiornamenti manuali.

x86\_64

```
Resources:
 MyFunction:
 Type: AWS::Lambda::Function
 Properties:
 FunctionName: my-function
 Runtime: python3.11
 Handler: index.handler
 Code:
 ZipFile: |
 def handler(event, context):
 return {'statusCode': 200}
 Layers:
 - !Sub '{{resolve:ssm:/aws/service/aws-parameters-and-secrets-lambda-extension/x86/latest}}'
 Role: !GetAtt MyFunctionRole.Arn
```

arm64

```
Layers:
```

```
- !Sub '{{resolve:ssm:/aws/service/aws-parameters-and-secrets-lambda-extension/arm64/latest}}'
```

#### Note

La `{{resolve:ssm:parameter-name}}` sintassi recupera automaticamente il valore del parametro durante le operazioni sullo stack. Ciò garantisce l'implementazione sempre con l'ARN corrente.

## Estensione ARN più recente

Le tabelle seguenti riportano gli ARN delle estensioni per le architetture e le regioni supportate.

### Argomenti

- [ARN di estensione per x86\\_64 and x86 architetture](#)
- [ARN di estensione per ARM64 and Mac con processore Apple architetture](#)

## ARN di estensione per x86\_64 and x86 architetture

Ultimo aggiornamento: 21 agosto 2026

Region	ARN
Stati Uniti orientali (Ohio)	arn:aws:lambda:us-east-2:590474943231:layer:AWS-Parameters-and-Secrets-Lambda-Extension:133
Stati Uniti orientali (Virginia settentrionale)	arn:aws:lambda:us-east-1:177933569100:layer:AWS-Parameters-and-Secrets-Lambda-Extension:116
Stati Uniti occidentali (California settentrionale)	arn:aws:lambda:us-west-1:997803712105:layer:AWS-Parameters-and-Secrets-Lambda-Extension:113

Region	ARN
Stati Uniti occidentali (Oregon)	<code>arn:aws:lambda:us-west-2:345057560386:layer:AWS-Parameters-and-Secrets-Lambda-Extension:116</code>
Africa (Città del Capo)	<code>arn:aws:lambda:af-south-1:317013901791:layer:AWS-Parameters-and-Secrets-Lambda-Extension:124</code>
Asia Pacifico (Hong Kong)	<code>arn:aws:lambda:ap-east-1:768336418462:layer:AWS-Parameters-and-Secrets-Lambda-Extension:121</code>
Asia Pacifico (Taipei)	<code>arn:aws:lambda:ap-east-2:890742577149:layer:AWS-Parameters-and-Secrets-Lambda-Extension:93</code>
Regione Asia Pacifico (Hyderabad)	<code>arn:aws:lambda:ap-south-2:070087711984:layer:AWS-Parameters-and-Secrets-Lambda-Extension:115</code>
Asia Pacifico (Giacarta)	<code>arn:aws:lambda:ap-southeast-3:490737872127:layer:AWS-Parameters-and-Secrets-Lambda-Extension:118</code>
Asia Pacifico (Melbourne)	<code>arn:aws:lambda:ap-southeast-4:090732460067:layer:AWS-Parameters-and-Secrets-Lambda-Extension:108</code>

Region	ARN
Asia Pacifico (Malesia)	<code>arn:aws:lambda:ap-southeast-5:381492012281:layer:AWS-Parameters-and-Secrets-Lambda-Extension:107</code>
Asia Pacifico (Nuova Zelanda)	<code>arn:aws:lambda:ap-southeast-6:995508174458:layer:AWS-Parameters-and-Secrets-Lambda-Extension:102</code>
Asia Pacifico (Mumbai)	<code>arn:aws:lambda:ap-south-1:176022468876:layer:AWS-Parameters-and-Secrets-Lambda-Extension:111</code>
Asia Pacifico (Osaka)	<code>arn:aws:lambda:ap-northeast-3:576959938190:layer:AWS-Parameters-and-Secrets-Lambda-Extension:118</code>
Asia Pacifico (Seoul)	<code>arn:aws:lambda:ap-northeast-2:738900069198:layer:AWS-Parameters-and-Secrets-Lambda-Extension:123</code>
Asia Pacifico (Singapore)	<code>arn:aws:lambda:ap-southeast-1:044395824272:layer:AWS-Parameters-and-Secrets-Lambda-Extension:125</code>
Asia Pacifico (Sydney)	<code>arn:aws:lambda:ap-southeast-2:665172237481:layer:AWS-Parameters-and-Secrets-Lambda-Extension:129</code>

Region	ARN
Asia Pacifico (Thailandia)	<code>arn:aws:lambda:ap-southeast-7:941377119484:layer:AWS-Parameters-and-Secrets-Lambda-Extension:108</code>
Asia Pacifico (Tokyo)	<code>arn:aws:lambda:ap-northeast-1:133490724326:layer:AWS-Parameters-and-Secrets-Lambda-Extension:124</code>
Canada (Centrale)	<code>arn:aws:lambda:ca-central-1:200266452380:layer:AWS-Parameters-and-Secrets-Lambda-Extension:132</code>
Canada occidentale (Calgary)	<code>arn:aws:lambda:ca-west-1:243964427225:layer:AWS-Parameters-and-Secrets-Lambda-Extension:95</code>
Cina (Pechino)	<code>arn:aws-cn:lambda:cn-north-1:287114880934:layer:AWS-Parameters-and-Secrets-Lambda-Extension:118</code>
Cina (Ningxia)	<code>arn:aws-cn:lambda:cn-northwest-1:287310001119:layer:AWS-Parameters-and-Secrets-Lambda-Extension:118</code>
Europa (Francoforte)	<code>arn:aws:lambda:eu-central-1:187925254637:layer:AWS-Parameters-and-Secrets-Lambda-Extension:125</code>

Region	ARN
Europa (Irlanda)	<code>arn:aws:lambda:eu-west-1:015030872274:layer:AWS-Parameters-and-Secrets-Lambda-Extension:118</code>
Europa (Londra)	<code>arn:aws:lambda:eu-west-2:133256977650:layer:AWS-Parameters-and-Secrets-Lambda-Extension:123</code>
Europa (Milano)	<code>arn:aws:lambda:eu-south-1:325218067255:layer:AWS-Parameters-and-Secrets-Lambda-Extension:119</code>
Europa (Parigi)	<code>arn:aws:lambda:eu-west-3:780235371811:layer:AWS-Parameters-and-Secrets-Lambda-Extension:121</code>
Regione Europa (Spagna)	<code>arn:aws:lambda:eu-south-2:524103009944:layer:AWS-Parameters-and-Secrets-Lambda-Extension:114</code>
AWS European Sovereign Cloud (Germania)	<code>arn:aws-eusc:lambda:eusc-de-east-1:041683371183:layer:AWS-Parameters-and-Secrets-Lambda-Extension:5</code>
Europa (Stoccolma)	<code>arn:aws:lambda:eu-north-1:427196147048:layer:AWS-Parameters-and-Secrets-Lambda-Extension:119</code>

Region	ARN
Israele (Tel Aviv)	<code>arn:aws:lambda:il-central-1:148806536434:layer:AWS-Parameters-and-Secrets-Lambda-Extension:95</code>
Regione Europa (Zurigo)	<code>arn:aws:lambda:eu-central-2:772501565639:layer:AWS-Parameters-and-Secrets-Lambda-Extension:102</code>
Regione Messico (centrale)	<code>arn:aws:lambda:mx-central-1:241533131596:layer:AWS-Parameters-and-Secrets-Lambda-Extension:92</code>
Medio Oriente (Bahrein)	<code>arn:aws:lambda:me-south-1:832021897121:layer:AWS-Parameters-and-Secrets-Lambda-Extension:58</code>
Medio Oriente (Emirati Arabi Uniti)	<code>arn:aws:lambda:me-central-1:858974508948:layer:AWS-Parameters-and-Secrets-Lambda-Extension:60</code>
Sud America (San Paolo)	<code>arn:aws:lambda:sa-east-1:933737806257:layer:AWS-Parameters-and-Secrets-Lambda-Extension:127</code>
AWS GovCloud (US-East)	<code>arn:aws-us-gov:lambda:us-gov-east-1:129776340158:layer:AWS-Parameters-and-Secrets-Lambda-Extension:106</code>

Region	ARN
AWS GovCloud (US-West)	<code>arn:aws-us-gov:lambda:us-gov-west-1:127562683043:layer:AWS-Parameters-and-Secrets-Lambda-Extension:120</code>

ARN di estensione per ARM64 and Mac con processore Apple architetture

Ultimo aggiornamento: 21 agosto 2026

Region	ARN
Stati Uniti orientali (Ohio)	<code>arn:aws:lambda:us-east-2:590474943231:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:133</code>
Stati Uniti orientali (Virginia settentrionale)	<code>arn:aws:lambda:us-east-1:177933569100:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:116</code>
Regione Stati Uniti occidentali (California settentrionale)	<code>arn:aws:lambda:us-west-1:997803712105:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:110</code>
Stati Uniti occidentali (Oregon)	<code>arn:aws:lambda:us-west-2:345057560386:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:116</code>
Regione Africa (Città del Capo)	<code>arn:aws:lambda:af-south-1:317013901791:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:121</code>



Region	ARN
Regione Asia Pacifico (Hong Kong)	<code>arn:aws:lambda:ap-east-1:768336418462:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:118</code>
Asia Pacifico (Taipei)	<code>arn:aws:lambda:ap-east-2:890742577149:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:89</code>
Regione Asia Pacifico (Hyderabad)	<code>arn:aws:lambda:ap-south-2:070087711984:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:107</code>
Regione Asia Pacifico (Giacarta)	<code>arn:aws:lambda:ap-southeast-3:490737872127:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:115</code>
Asia Pacifico (Melbourne)	<code>arn:aws:lambda:ap-southeast-4:090732460067:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:107</code>
Asia Pacifico (Malesia)	<code>arn:aws:lambda:ap-southeast-5:381492012281:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:107</code>
Asia Pacifico (Nuova Zelanda)	<code>arn:aws:lambda:ap-southeast-6:995508174458:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:100</code>

Region	ARN
Asia Pacifico (Mumbai)	<code>arn:aws:lambda:ap-south-1:176022468876:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:111</code>
Asia Pacifico (Osaka)	<code>arn:aws:lambda:ap-northeast-3:576959938190:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:115</code>
Regione Asia Pacifico (Seoul)	<code>arn:aws:lambda:ap-northeast-2:738900069198:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:120</code>
Asia Pacifico (Singapore)	<code>arn:aws:lambda:ap-southeast-1:044395824272:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:125</code>
Asia Pacifico (Sydney)	<code>arn:aws:lambda:ap-southeast-2:665172237481:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:129</code>
Asia Pacifico (Thailandia)	<code>arn:aws:lambda:ap-southeast-7:941377119484:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:107</code>
Asia Pacifico (Tokyo)	<code>arn:aws:lambda:ap-northeast-1:133490724326:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:124</code>

Region	ARN
Regione Canada (Centrale)	<code>arn:aws:lambda:ca-central-1:200266452380:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:129</code>
Canada occidentale (Calgary)	<code>arn:aws:lambda:ca-west-1:243964427225:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:94</code>
Cina (Pechino)	<code>arn:aws-cn:lambda:cn-north-1:287114880934:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:107</code>
Cina (Ningxia)	<code>arn:aws-cn:lambda:cn-northwest-1:287310001119:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:107</code>
Europa (Francoforte)	<code>arn:aws:lambda:eu-central-1:187925254637:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:125</code>
Europa (Irlanda)	<code>arn:aws:lambda:eu-west-1:015030872274:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:118</code>
Europa (Londra)	<code>arn:aws:lambda:eu-west-2:133256977650:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:123</code>

Region	ARN
Regione Europa (Milano)	<code>arn:aws:lambda:eu-south-1:325218067255:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:116</code>
Regione Europa (Parigi)	<code>arn:aws:lambda:eu-west-3:780235371811:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:118</code>
Regione Europa (Spagna)	<code>arn:aws:lambda:eu-south-2:524103009944:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:106</code>
Regione Europa (Stoccolma)	<code>arn:aws:lambda:eu-north-1:427196147048:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:116</code>
Israele (Tel Aviv)	<code>arn:aws:lambda:il-central-1:148806536434:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:94</code>
Regione Europa (Zurigo)	<code>arn:aws:lambda:eu-central-2:772501565639:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:94</code>
Regione Messico (centrale)	<code>arn:aws:lambda:mx-central-1:241533131596:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:91</code>

Region	ARN
Regione Medio Oriente (Bahrein)	<code>arn:aws:lambda:me-south-1:832021897121:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:55</code>
Medio Oriente (Emirati Arabi Uniti)	<code>arn:aws:lambda:me-central-1:858974508948:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:49</code>
Regione Sud America (San Paolo)	<code>arn:aws:lambda:sa-east-1:933737806257:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:124</code>
AWS GovCloud (US-East)	<code>arn:aws-us-gov:lambda:us-gov-east-1:129776340158:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:106</code>
AWS GovCloud (US-West)	<code>arn:aws-us-gov:lambda:us-gov-west-1:127562683043:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:109</code>

## Integrazione con altri prodotti e servizi

AWS Systems Manager ha un'integrazione integrata per i prodotti e i servizi mostrati nella tabella seguente.

Servizio	Description
Ansible	<a href="#">Ansible</a> è una piattaforma di automazione IT che semplifica l'implementazione di applicazioni e sistemi.

Servizio	Description
	<p>Systems Manager fornisce il documento Systems Manager (documento SSM) <code>AWS-ApplyAnsiblePlaybooks</code> che consente di creare State Manager associazioni che eseguono Ansible playbook.</p> <p>Ulteriori informazioni</p> <p><a href="#">Creazione di associazioni che funzionano Ansible playbook</a></p>
Chef	<p><a href="#">Chef</a> è uno strumento di automazione IT che semplifica l'implementazione di applicazioni e sistemi.</p> <p>Systems Manager fornisce il documento <code>AWS-ApplyChefRecipes</code> SSM, che consente di creare associazioni in State Manager uno strumento che esegue AWS Systems Manager ricette. Chef</p> <p>Ulteriori informazioni</p> <p><a href="#">Creazione di associazioni che vengono eseguite Chef recipes</a></p> <p>Systems Manager si integra anche con i profili <a href="#">Chef InSpec</a>, che consentono di eseguire analisi della conformità e di visualizzare nodi conformi e non conformi.</p> <p>Ulteriori informazioni</p> <p><a href="#">Utilizzo Chef InSpec profili con Systems Manager Compliance</a></p>

Servizio	Description
GitHub	<p><a href="#">GitHub</a> fornisce hosting per il controllo delle versioni di sviluppo software e la collaborazione.</p> <p>Systems Manager fornisce il documento <code>SSMAWS-RunDocument</code> , che consente di eseguire altri documenti SSM archiviati in GitHub, e il documento <code>SSMAWS-RunRemoteScript</code> , che consente di eseguire gli script archiviati in GitHub.</p> <p>Ulteriori informazioni</p> <ul style="list-style-type: none"><li>• <a href="#">Esecuzione di documenti da posizioni remote</a></li><li>• <a href="#">Esecuzione di script da GitHub</a></li></ul>
Jenkins	<p><a href="#">Jenkins</a> è un server di automazione open source che consente agli sviluppatori di creare, testare e distribuire in modo affidabile il proprio software.</p> <p>L'automazione può essere utilizzata come fase successiva alla compilazione per preinstallare le versioni delle applicazioni in (). Amazon Machine Images AMIs</p> <p>Ulteriori informazioni</p> <p><a href="#">Aggiornamento in corso AMI utilizzando l'automazione e Jenkins</a></p>

Servizio	Description
ServiceNow	<p><a href="#">ServiceNow</a> è un sistema di gestione dei servizi aziendali che consente di gestire i servizi e le operazioni IT.</p> <p>Automazione, Change Manager, Incident Manager e OpsCenter, tutti strumenti di Systems Manager, si integrano con ServiceNow utilizzando AWS Service Management Connector. Con questa integrazione, puoi visualizzare, creare, aggiornare, aggiungere corrispondenza e risolvere i Supporto AWS casi da ServiceNow.</p> <p>Ulteriori informazioni</p> <p><a href="#">Integrazione con ServiceNow</a></p>



Servizio	Description
Terraform	<p>HashiCorp <a href="#">Terraform</a> è uno strumento software open source di infrastructure as code (IaC) che fornisce un flusso di lavoro con interfaccia a riga di comando (CLI) per gestire vari servizi cloud. Per Systems Manager, sarà possibile utilizzare Terraform per gestire o eseguire il provisioning di quanto segue:</p> <p>Risorse</p> <ul style="list-style-type: none"><li>• <a href="#">aws_ssm_activation</a></li><li>• <a href="#">aws_ssm_association</a></li><li>• <a href="#">aws_ssm_default_patch_baseline</a></li><li>• <a href="#">aws_ssm_document</a></li><li>• <a href="#">aws_ssm_maintenance_window</a></li><li>• <a href="#">aws_ssm_maintenance_window_target</a></li><li>• <a href="#">aws_ssm_maintenance_window_task</a></li><li>• <a href="#">aws_ssm_parameter</a></li><li>• <a href="#">aws_ssm_patch_baseline</a></li><li>• <a href="#">aws_ssm_patch_group</a></li><li>• <a href="#">aws_ssm_resource_data_sync</a></li><li>• <a href="#">aws_ssm_service_setting</a></li></ul> <p>Origine dati</p> <ul style="list-style-type: none"><li>• <a href="#">aws_ssm_document</a></li><li>• <a href="#">aws_ssm_instances</a></li><li>• <a href="#">ssm_maintenance_windows</a></li><li>• <a href="#">aws_ssm_parameter</a></li><li>• <a href="#">aws_ssm_parameters_by_path</a></li><li>• <a href="#">aws_ssm_patch_baseline</a></li></ul>

## Argomenti

- [Esecuzione di script da GitHub](#)
- [Utilizzo Chef InSpec profili con Systems Manager Compliance](#)
- [Integrazione con ServiceNow](#)

## Esecuzione di script da GitHub

Questo argomento descrive come utilizzare il documento Systems Manager predefinito (documento SSM) da cui AWS-RunRemoteScript scaricare scriptGitHub, inclusi Ansible Playbook, Python, Ruby e script. PowerShell Utilizzando questo documento SSM, non è più necessario trasferire manualmente gli script in Amazon Elastic Compute Cloud (Amazon EC2) o inserirli in documenti SSM. AWS Systems Manager l'integrazione con GitHub promuove l'infrastruttura come codice, riducendo il tempo necessario per gestire i nodi e standardizzare le configurazioni in tutta la flotta.

È anche possibile creare documenti SSM personalizzati che consentano di scaricare ed eseguire script o altri documenti SSM da sedi remote. Per ulteriori informazioni, consulta [Creazione di documenti compositi](#).

È anche possibile scaricare una directory che includa più script. Quando si esegue lo script principale nella directory, Systems Manager esegue anche eventuali script di riferimento (finché sono inclusi nella directory).

Tieni presenti le informazioni importanti sull'esecuzione di script da GitHub, riportate di seguito.

- Systems Manager non verifica che lo script possa essere eseguito su un nodo. Prima di scaricare ed eseguire lo script, verifica che il software necessario sia installato sul nodo. In alternativa, è possibile creare un documento composito che installi il software utilizzando uno Run Command o State Manager, gli strumenti in AWS Systems Manager esso contenuti, quindi scarichi ed esegua lo script.
- Dovrai personalmente accertarti del soddisfacimento di tutti i requisiti di GitHub. tra cui, se necessario, l'aggiornamento del token di accesso. Assicurati di non superare il numero di richieste autenticate o non autenticate. Per ulteriori informazioni, consulta la documentazione GitHub.
- I repository di GitHub Enterprise non sono supportati.

## Esecuzione Ansible Playbook di GitHub

Questa sezione illustra le procedure che consentono di eseguire playbook Ansible da GitHub con la console o la AWS Command Line Interface (AWS CLI).

### Prima di iniziare

Se intendi eseguire uno script archiviato in un GitHub archivio privato, crea un AWS Systems Manager SecureString parametro per il token di accesso GitHub di sicurezza. Non è possibile accedere a uno script in un archivio privato di GitHub trasferendo manualmente il token su SSH. Il token di accesso deve essere trasferito come parametro SecureString di Systems Manager. Per ulteriori informazioni sulla creazione di un parametro SecureString, consulta [Creazione in corso Parameter Store parametri in Systems Manager](#).

### Esegui un Ansible Playbook di GitHub (console)

#### Esegui un Ansible Playbook di GitHub

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Run Command.
3. Seleziona Esegui comando.
4. Nell'elenco Documento di comando, scegli **AWS-RunRemoteScript**.
5. In Parametri di comando, esegui le seguenti operazioni:
  - In Tipo di origine, seleziona GitHub.
  - Nella casella Informazioni sull'origine, inserisci le informazioni necessarie per accedere all'origine nel formato seguente.

```
{
 "owner": "owner_name",
 "repository": "repository_name",
 "getOptions": "branch:branch_name",
 "path": "path_to_scripts_or_directory",
 "tokenInfo": "{{ssm-secure:SecureString_parameter_name}}"
}
```

Questo esempio scarica un file denominato `webserver.yml`.

```
{
 "owner": "TestUser1",
 "repository": "GitHubPrivateTest",
 "getOptions": "branch:myBranch",
 "path": "scripts/webserver.yml",
 "tokenInfo": "{{ssm-secure:mySecureStringParameter}}"
}
```

#### Note

"branch" è necessario solo se il documento SSM è memorizzato in un ramo diverso da master.

Per utilizzare la versione degli script che si trovano in un particolare commit nel repository, usa commitID con getOptions invece di branch. Ad esempio:

"getOptions": "commitID:bbc1ddb94...b76d3bEXAMPLE",

- Nel campo Riga di comando, inserisci i parametri per l'esecuzione di script. Ecco un esempio.

**ansible-playbook -i \\\"localhost,\\\" --check -c local webserver.yml**

- (Facoltativo) Nel campo Directory di lavoro, inserisci il nome di una directory sul nodo su cui si desidera scaricare ed eseguire lo script.
  - (Facoltativo) In Timeout di esecuzione, specifica il numero di secondi che il sistema dovrà attendere prima di interrompere l'esecuzione del comando di script.
6. Nella sezione Destinazioni, scegli i nodi gestiti in cui si desidera eseguire questa operazione specificando i tag, selezionando manualmente le istanze, i dispositivi edge o indicando un gruppo di risorse.

#### Tip

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

7. In Altri parametri:

- In Commento, digita le informazioni su questo comando.

- In Timeout (secondi), specifica il numero di secondi che il sistema dovrà attendere prima di generare un errore per l'intera esecuzione del comando.

8. Per Controllo velocità:

- In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti presi di mira, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.

9. (Facoltativo) Nella sezione Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Scrivi l'output del comando in un bucket S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

 Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

10. Se vuoi che vengano inviate notifiche sullo stato dell'esecuzione del comando, nella sezione Notifiche SNS selezionare la casella di controllo Abilita notifiche SNS.

Per ulteriori informazioni sulla configurazione delle notifiche Amazon SNS per Run Command, consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

## 11. Scegli Esegui.

Esegui un Ansible Playbook di GitHub utilizzando il AWS CLI

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Il comando seguente consente di scaricare ed eseguire uno script da GitHub.

```
aws ssm send-command \
 --document-name "AWS-RunRemoteScript" \
 --instance-ids "instance-IDs" \
 --parameters '{"sourceType":["GitHub"],"sourceInfo":[{"owner\
 \":\"owner_name\", \"repository\": \"repository_name\", \"path\
 \": \"path_to_file_or_directory\", \"tokenInfo\": \"{ssm-
 secure:name_of_your_SecureString_parameter}\" }"],"commandLine":
 [\"commands_to_run\"]}'
```

Ecco un comando di esempio da eseguire su una macchina Linux locale.

```
aws ssm send-command \
 --document-name "AWS-RunRemoteScript" \
 --instance-ids "i-02573cafEXAMPLE" \
 --parameters '{"sourceType":["GitHub"],"sourceInfo":[{"owner\
 \":\"TestUser1\", \"repository\": \"GitHubPrivateTest\", \"path\
 \": \"scripts/webserver.yml\", \"tokenInfo\": \"{ssm-secure:mySecureStringParameter}\" }"],"commandLine":
 [\"ansible-playbook -i \\\\\"localhost,\\\" --check -c local webserver.yml\"]}'
```

## Esegui script Python da GitHub

Questa sezione include procedure per aiutarti a eseguire script Python GitHub utilizzando la AWS Systems Manager console o (). AWS Command Line Interface AWS CLI

## Esecuzione di uno script Python da GitHub (console)

### Esecuzione di uno script Python da GitHub

1. Apri la AWS Systems Manager console all'indirizzo. <https://console.aws.amazon.com/systems-manager/>
2. Nel pannello di navigazione, scegli Run Command.
3. Seleziona Esegui comando.
4. Nell'elenco Documento sui comandi, scegli **AWS-RunRemoteScript**.
5. In Parametri di comando, esegui le seguenti operazioni:
  - In Source Type (Tipo di origine), selezionare GitHub.
  - Nella casella Informazione sull'origine, inserisci le informazioni necessarie per accedere all'origine nel formato seguente:

```
{
 "owner": "owner_name",
 "repository": "repository_name",
 "getOptions": "branch:branch_name",
 "path": "path_to_document",
 "tokenInfo": "{{ssm-secure:SecureString_parameter_name}}"
}
```

L'esempio seguente esegue il download in una directory di script denominata complex-script.

```
{
 "owner": "TestUser1",
 "repository": "SSTestDocsRepo",
 "getOptions": "branch:myBranch",
 "path": "scripts/python/complex-script",
 "tokenInfo": "{{ssm-secure:myAccessTokenParam}}"
}
```

#### Note

"branch" è richiesto solo se gli script sono memorizzati in un ramo diverso da master.

Per utilizzare la versione degli script che si trovano in un particolare commit nel repository, usa commitID con getOptions invece di branch. Ad esempio:

```
"getOptions": "commitID:bbc1ddb94...b76d3bEXAMPLE",
```

- In Riga di comando, inserisci i parametri per l'esecuzione di script. Ecco un esempio.

```
mainFile.py argument-1 argument-2
```

Questo esempio esegue `mainFile.py`, che può a sua volta eseguire altri script nella directory `complex-script`.

- (Facoltativo) In Directory di lavoro, inserisci il nome di una directory dell'istanza su cui si desidera scaricare ed eseguire lo script.
  - (Facoltativo) In Timeout di esecuzione, specifica il numero di secondi che il sistema dovrà attendere prima di interrompere l'esecuzione del comando di script.
6. Nella sezione Destinazioni, identifica i nodi in cui si desidera eseguire questa operazione specificando i tag, selezionando manualmente le istanze, i dispositivi edge o indicando un gruppo di risorse.

#### Tip

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

#### 7. In Altri parametri:

- In Commento, digita le informazioni su questo comando.
- In Timeout (secondi), specifica il numero di secondi che il sistema dovrà attendere prima di generare un errore per l'intera esecuzione del comando.

#### 8. Per Controllo velocità:

- In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

#### Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti



come target, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.
9. (Facoltativo) Nella sezione Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Scrivi l'output del comando in un bucket S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

#### Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

10. Se vuoi che vengano inviate notifiche sullo stato dell'esecuzione del comando, nella sezione Notifiche SNS selezionare la casella di controllo Abilita notifiche SNS.

Per ulteriori informazioni sulla configurazione delle notifiche Amazon SNS per Run Command, consulta [Monitoraggio delle modifiche di stato di Systems Manager utilizzando le notifiche Amazon SNS](#).

11. Scegli Esegui.

Esegui uno script Python usando GitHub il AWS CLI

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Il comando seguente consente di scaricare ed eseguire uno script da GitHub.

```
aws ssm send-command --document-name "AWS-RunRemoteScript" --instance-ids "instance-IDs" --parameters '{"sourceType":["GitHub"],"sourceInfo":["{\\"owner\\":\\"owner_name\\", \\"repository\\":\\"repository_name\\", \\"path\\":\\"path_to_script_or_directory\"}"],"commandLine":["commands_to_run"]}'
```

Ecco un esempio.

```
aws ssm send-command --document-name "AWS-RunRemoteScript" --instance-ids "i-02573cafcfEXAMPLE" --parameters '{"sourceType":["GitHub"],"sourceInfo":["{\\"owner\\":\\"TestUser1\\", \\"repository\\":\\"GitHubTestPublic\\", \\"path\\":\\"scripts/python/complex-script\\"}"],"commandLine":["mainFile.py argument-1 argument-2 "]}'
```

Questo esempio prevede il download di una directory di script denominata `complex-script`. La voce `commandLine` esegue `mainFile.py`, che può a sua volta eseguire altri script nella directory `complex-script`.

## Utilizzo Chef InSpec profili con Systems Manager Compliance

AWS Systems Manager si integra con [Chef InSpec](#). Chef InSpec è un framework di test open source che consente di creare profili leggibili dall'uomo da archiviare in GitHub Amazon Simple Storage Service (Amazon S3). È quindi possibile utilizzare Systems Manager per eseguire analisi della conformità e visualizzare nodi conformi e non conformi. Un profilo è un requisito di sicurezza, conformità o policy dell'ambiente di elaborazione. Ad esempio, è possibile creare profili che eseguano i seguenti controlli, quando si esegue la scansione dei nodi con Conformità, uno strumento di AWS Systems Manager:

- Controllo dell'apertura o della chiusura di porte specifiche.
- Controllo dell'esecuzione di determinate applicazioni.
- Controllo dell'avvenuta installazione di specifici pacchetti.
- Controllo delle chiavi del Registro di sistema Windows per proprietà specifiche.

Puoi creare InSpec profili solo per le istanze Amazon Elastic Compute Cloud (Amazon EC2) gestite con Systems Manager. On-premises i server o le macchine virtuali (VM) non sono supportati. Il seguente profilo Chef InSpec di esempio controlla se la porta 22 sia aperta.

```
control 'Scan Port' do
 impact 10.0
 title 'Server: Configure the service port'
 desc 'Always specify which port the SSH server should listen to.
 Prevent unexpected settings.'
 describe sshd_config do
 its('Port') { should eq('22') }
 end
end
```

InSpec include una raccolta di risorse che consentono di scrivere rapidamente controlli e verifiche. InSpec utilizza il [InSpec Domain-specific linguaggio \(DSL\)](#) per scrivere questi controlli in Ruby. Puoi anche utilizzare i profili creati da una vasta comunità di InSpec utenti. Ad esempio, il [progetto DevSec chef-os-hardening GitHub](#) include dozzine di profili per aiutarti a proteggere i tuoi nodi. È possibile creare e memorizzare i profili in GitHub o Amazon S3.

## Come funziona

Ecco come funziona il processo di utilizzo dei profili con conformità: InSpec

1. Identifica InSpec i profili predefiniti che desideri utilizzare o creane di tuoi. Per iniziare, ci si può avvalere dei [profili predefiniti](#) disponibili su GitHub. Per informazioni su come creare i tuoi InSpec profili, vedi [Chef Chef InSpec Profiles](#).
2. I profili possono essere memorizzati in un archivio GitHub pubblico o privato oppure in un bucket S3.
3. Esegui la conformità con InSpec i tuoi profili utilizzando il documento Systems Manager (documento SSM). AWS-RunInspecChecks È possibile iniziare una scansione di conformità utilizzando Run Command, per le scansioni su richiesta, oppure è possibile pianificare scansioni di conformità regolari utilizzando State Manager uno strumento in. AWS Systems Manager
4. Per identificare i nodi non conformi ci si può avvalere dell'API di conformità o della console di conformità .

### Note

Osservare le seguenti informazioni.

- Chef utilizza un client sui nodi per elaborare il profilo. Non è necessario installare il client. Quando Systems Manager esegue il documento SSM AWS-RunInspecChecks, il sistema

verifica che il client sia installato. Se non lo fosse, Systems Manager installa il client Chef durante la scansione, poi, al termine della stessa, lo disinstalla.

- L'esecuzione del documento SSM AWS-RunInspecChecks, come descritto in questo argomento, assegna una voce di conformità di tipo Custom: Inspec a ogni nodo di destinazione. Per assegnare questo tipo di conformità, il documento richiama l'[PutComplianceItems](#) operazione API.

## Esecuzione di una scansione InSpec della conformità

Questa sezione include informazioni su come eseguire una scansione della InSpec conformità utilizzando la console Systems Manager e AWS Command Line Interface (AWS CLI). La procedura della console illustra come configurare State Manager per eseguire la scansione. La AWS CLI procedura mostra come Run Command configurare l'esecuzione della scansione.

Esecuzione di una scansione di InSpec conformità con State Manager (console)

Per eseguire una scansione InSpec della conformità con State Manager utilizzando AWS Systems Manager console

1. Aprire la AWS Systems Manager console all'indirizzo <https://console.aws.amazon.com/systems-manager/>.
2. Nel pannello di navigazione, scegli State Manager.
3. Selezionare Create association (Crea associazione).
4. Immettere un nome nella sezione Provide association details (Fornisci dettagli associazione).
5. Nell'elenco Command document (Documento comando) scegliere **AWS-RunInspecChecks**.
6. Nell'elenco Document version (Versione del documento), scegliere Latest at runtime (Ultima versione al tempo di esecuzione).
7. Nella sezione Parametri, dall'elenco Tipo di origine, scegli GitHub o S3.

Se lo desideri GitHub, inserisci il percorso di un InSpec profilo in un GitHub archivio pubblico o privato nel campo Informazioni sulla fonte. Ecco un esempio di percorso verso un profilo pubblico fornito dal team di Systems Manager dalla seguente posizione: <https://github.com/awslabs/amazon-ssm/tree/master/Compliance/InSpec/PortCheck>.

```
{"owner":"awslabs","repository":"amazon-ssm","path":"Compliance/InSpec/PortCheck","getOptions":"branch:master"}
```

Se scegli S3, inserisci un URL valido per un InSpec profilo in un bucket S3 nel campo Source Info.

Per ulteriori informazioni sull'integrazione di Systems Manager con GitHub e Amazon S3, consulta [Esecuzione di script da GitHub](#).

8. Nella sezione Destinazioni, identifica i nodi in cui si desidera eseguire questa operazione specificando i tag, selezionando manualmente le istanze, i dispositivi edge o indicando un gruppo di risorse.

 Tip

Se un nodo gestito che ti aspetti di vedere non è presente nell'elenco, consulta [Risoluzione dei problemi relativi alla disponibilità dei nodi gestiti](#) per suggerimenti sulla risoluzione dei problemi.

9. Nella sezione Specify schedule (Specifica pianificazione), è possibile programmare su base periodica l'esecuzione della scansione di conformità avvalendosi delle opzioni specifiche del generatore di pianificazione.
10. In Controllo velocità:
  - In Simultaneità, specifica un numero o una percentuale di nodi gestiti su cui eseguire contemporaneamente il comando.

 Note

Se hai selezionato le destinazioni specificando i tag applicati ai nodi gestiti o specificando i gruppi di AWS risorse e non sei sicuro del numero di nodi gestiti presi di mira, limita il numero di destinazioni che possono eseguire il documento contemporaneamente specificando una percentuale.

- 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. Se, ad esempio, si specificano tre errori, Systems Manager interrompe l'invio del comando quando riceve il quarto errore. Anche i nodi gestiti che stanno ancora elaborando il comando potrebbero inviare errori.
11. (Facoltativo) Nella sezione Opzioni di output, per salvare l'output del comando in un file, seleziona la casella Scrivi l'output del comando in un bucket S3. Digita i nomi del bucket e del prefisso (cartella) nelle caselle.

 Note

Le autorizzazioni S3 che danno la possibilità di scrivere dati in un bucket S3 sono quelle del profilo dell'istanza (per istanze EC2) o del ruolo di servizio IAM (in macchine attivate da sistemi ibridi) assegnate all'istanza, non quelle dell'utente IAM che esegue questo processo. Per ulteriori informazioni, consulta le pagine [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#) oppure [Creazione di un ruolo di servizio IAM per un ambiente ibrido](#). Inoltre, se il bucket S3 specificato si trova su un Account AWS diverso, assicurarsi che il profilo dell'istanza o il ruolo di servizio IAM associato al nodo gestito disponga delle autorizzazioni necessarie per scrivere su quel bucket.

12. Scegli Crea associazione. Il sistema crea l'associazione ed esegue automaticamente la scansione di conformità.
13. Attendere per alcuni minuti il completamento della scansione, poi selezionare Compliance (Conformità) nel riquadro di navigazione.
14. Nelle istanze gestite corrispondenti, individua i nodi in cui si trova la colonna Tipo di conformità. Custom:Inspec
15. Scegliere un ID nodo per visualizzare i dettagli degli stati non conformi.

### Esecuzione di una scansione InSpec della conformità con Run Command (AWS CLI)

1. Installa e configura AWS Command Line Interface (AWS CLI), se non l'hai già fatto.

Per informazioni, consulta la pagina [Installazione o aggiornamento della versione più recente di AWS CLI](#).

2. Esegui uno dei seguenti comandi per eseguire un InSpec profilo da Amazon S3 GitHub o da Amazon S3.

Il comando accetta i parametri seguenti:

- sourceType: GitHub o Amazon S3
- SourceInfo: URL della cartella del InSpec profilo in GitHub o in un bucket S3. La cartella deve contenere il InSpec file base (\*.yml) e tutti i controlli correlati (\*.rb).

#### GitHub

```
aws ssm send-command --document-name "AWS-RunInspecChecks" --targets
' [{"Key": "tag:tag_name", "Values": ["tag_value"]}]' --parameters '{"sourceType":
["GitHub"], "sourceInfo": [{"\owner\": "\owner_name\ ", \repository\ ":
\repository_name\ ", \path\ ": \Inspec.yml_file"}]}'
```

Ecco un esempio.

```
aws ssm send-command --document-name "AWS-RunInspecChecks" --targets
' [{"Key": "tag:testEnvironment", "Values": ["webServers"]}]' --parameters
' {"sourceType": ["GitHub"], "getOptions": "branch:master", "sourceInfo": [{"\owner\ ":
\awslabs\ ", \repository\ ": \amazon-ssm\ ", \path\ ": \Compliance/Inspec/PortCheck
\"}]}'
```

## Amazon S3

```
aws ssm send-command --document-name "AWS-RunInspecChecks" --targets
' [{"Key": "tag:tag_name", "Values": ["tag_value"]}]' --parameters '{"sourceType":
["S3"], "sourceInfo": [{"\path\ ": \https://s3.aws-api-domain/amzn-s3-demo-
bucket/Inspec.yml_file"}]}'
```

Ecco un esempio.

```
aws ssm send-command --document-name "AWS-RunInspecChecks" --targets
' [{"Key": "tag:testEnvironment", "Values": ["webServers"]}]' --
parameters '{"sourceType": ["S3"], "sourceInfo": [{"\path\ ": \https://s3.aws-api-
domain/amzn-s3-demo-bucket/Inspec/PortCheck.yml"}]}'
```

3. Con il comando seguente è possibile visualizzare un riepilogo della scansione di conformità.

```
aws ssm list-resource-compliance-summaries --filters
Key=ComplianceType,Values=Custom:Inspec
```

4. Eseguire il seguente comando per visualizzare i dettagli di un nodo non conforme.

```
aws ssm list-compliance-items --resource-ids node_ID --resource-type
ManagedInstance --filters Key=DocumentName,Values=AWS-RunInspecChecks
```

## Integrazione con ServiceNow

ServiceNow fornisce un sistema di gestione dei servizi basato sul cloud per creare e gestire flussi di lavoro a livello di organizzazione, ad esempio per servizi IT, sistemi di ticketing e supporto. Il AWS Service Management Connector si integra ServiceNow con Systems Manager per fornire, gestire e gestire AWS le risorse daServiceNow. È possibile utilizzare AWS Service Management Connector per l'integrazione ServiceNow con AutomationChange Manager, Incident Manager e OpsCenter tutti gli strumenti inclusi. AWS Systems Manager

Utilizzando ServiceNow, è possibile eseguire le seguenti attività:

- Esegui i playbook di automazione da Systems Manager.
- Visualizza, aggiorna e risolvi gli incidenti da Systems Manager OpsItems.
- Visualizza e gestisci gli elementi operativi, come gli incidenti, tramite Systems Manager OpsCenter.
- Visualizza ed esegui le richieste di modifica di Systems Manager da un elenco selezionato di modelli di modifica pre-approvati.
- Gestisci e risolvi gli incidenti che coinvolgono applicazioni AWS ospitate mediante l'integrazione con Incident Manager.

### Note

Per informazioni su come eseguire l'integrazione conServiceNow, vedere [Configurazione delle integrazioni dei AWS servizi](#) nella Guida per l'amministratore di AWS Service Management Connector.



# AWS Systems Manager riferimento

Le informazioni e gli argomenti seguenti possono aiutarti a migliorare l'implementazione di soluzioni AWS Systems Manager .

## Principale

In AWS Identity and Access Management (IAM), puoi concedere o negare a un servizio l'accesso alle risorse utilizzando l'elemento della policy Principal. Il valore dell'elemento di Policy principale per Systems Manager è `ssm.amazonaws.com`.

## Supportato Regioni AWS ed endpoint

Consulta [Endpoint del servizio Systems Manager](#) nella Riferimenti generali di Amazon Web Services.

## Service Quotas

Consulta [Service Quotas di Systems Manager](#) nella Riferimenti generali di Amazon Web Services.

## Documentazione di riferimento API

Consulta [Documentazione di riferimento API di AWS Systems Manager](#).

## AWS CLI Riferimento al comando

Vedi la [AWS Systems Manager sezione del AWS CLI Command Reference](#).

## AWS Strumenti per PowerShell Riferimento ai cmdlet

Vedere la [AWS Systems Manager sezione del AWS Strumenti per PowerShell Cmdlet Reference](#).

## Repository SSM Agent su GitHub

Vedere [aws/amazon-ssm-agent](#).

## Fai una domanda

Problemi di Systems Manager in [AWS Re:post](#)

## AWS Blog di notizie

## [Strumenti di gestione](#)

## Altri argomenti di riferimento

- [L'utilizzo di questo servizio con un AWS SDK](#)

- [Riferimento: bucket Amazon S3 per operazioni di applicazione di patch](#)
- [Riferimento: modelli e tipi di EventBridge eventi Amazon per Systems Manager](#)
- [Riferimento: espressioni Cron e della frequenza per Systems Manager](#)
- [Referenza: ec2messages, ssmmessages e altre operazioni API](#)
- [Riferimento: formati di stringhe di data e ora per Systems Manager](#)

## L'utilizzo di questo servizio con un AWS SDK

AWS I kit di sviluppo software (SDK) sono disponibili per molti linguaggi di programmazione diffusi. Ogni SDK fornisce un'API, esempi di codice e documentazione che facilitano agli sviluppatori la creazione di applicazioni nel loro linguaggio preferito.

Documentazione sugli SDK	Esempi di codice
<a href="#">AWS SDK per C++</a>	<a href="#">AWS SDK per C++ esempi di codice</a>
<a href="#">AWS CLI</a>	<a href="#">AWS CLI esempi di codice</a>
<a href="#">AWS SDK per Go</a>	<a href="#">AWS SDK per Go esempi di codice</a>
<a href="#">AWS SDK per Java</a>	<a href="#">AWS SDK per Java esempi di codice</a>
<a href="#">AWS SDK per JavaScript</a>	<a href="#">AWS SDK per JavaScript esempi di codice</a>
<a href="#">AWS SDK per Kotlin</a>	<a href="#">AWS SDK per Kotlin esempi di codice</a>
<a href="#">AWS SDK per .NET</a>	<a href="#">AWS SDK per .NET esempi di codice</a>
<a href="#">AWS SDK per PHP</a>	<a href="#">AWS SDK per PHP esempi di codice</a>
<a href="#">AWS Strumenti per PowerShell</a>	<a href="#">AWS Strumenti per PowerShell esempi di codice</a>
<a href="#">AWS SDK per Python v4</a>	<a href="#">AWS Esempi di codice SDK per Python v4</a>
<a href="#">AWS SDK per Python (Boto3)</a>	<a href="#">AWS SDK per Python (Boto3) esempi di codice</a>
<a href="#">AWS SDK per Ruby</a>	<a href="#">AWS SDK per Ruby esempi di codice</a>

Documentazione sugli SDK	Esempi di codice
<a href="#">AWS SDK per Rust</a>	<a href="#">AWS SDK per Rust esempi di codice</a>
<a href="#">AWS SDK per SAP ABAP</a>	<a href="#">AWS SDK per SAP ABAP esempi di codice</a>
<a href="#">AWS SDK per Swift</a>	<a href="#">AWS SDK per Swift esempi di codice</a>

#### Esempio di disponibilità

Non riesci a trovare quello che ti serve? Richiedi un esempio di codice utilizzando il link Fornisci un feedback nella parte inferiore di questa pagina.

## Riferimento: bucket Amazon S3 per operazioni di applicazione di patch

Nel corso dell'esecuzione di varie operazioni di Patch Manager patching, AWS Systems Manager Agent (SSM Agent) accede a determinati bucket Amazon Simple Storage Service (Amazon S3) di proprietà e gestiti da Amazon Web Services (AWS). Questi bucket S3 sono accessibili pubblicamente e, per impostazione predefinita, l'SSM Agent si connette con essi usando chiamate HTTP.

Tuttavia, se utilizzi un endpoint cloud privato virtuale (VPC) nelle operazioni di Systems Manager, devi fornire un'autorizzazione esplicita in un profilo dell'istanza Amazon Elastic Compute Cloud (Amazon EC2) per Systems Manager o in un ruolo di servizio per le macchine non EC2 in un ambiente [ibrido e multicloud](#). In caso contrario, le risorse non accedono a questi bucket pubblici.

Questo argomento di riferimento elenca i bucket relativi alle patch per ogni Regione AWS supportata.

Per informazioni sulla specificazione di questi bucket S3 nei profili dell'istanza EC2, consulta [Agente SSM comunicazioni con AWS bucket S3 gestiti](#).

Per ulteriori informazioni sull'utilizzo degli endpoint VPC con Systems Manager, consulta [Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager](#).

### Argomenti

- [Bucket contenenti documenti SSM Command per le operazioni di patching \(Linux e Windows Server\)](#)

- [Bucket contenenti documenti SSM Command per le operazioni di patching \(macOS\)](#)
- [Secchi contenenti AWS istantanee della baseline delle patch gestite](#)

## Bucket contenenti documenti SSM Command per le operazioni di patching (Linux e Windows Server)

I bucket con formato `aws-patch-manager-region-unique-suffix` contengono i seguenti documenti utilizzati da Patch Manager per le operazioni di applicazione di patch sui sistemi operativi di Linux e Windows Server:

- AWS-RunPatchBaseline
- AWS-RunPatchBaselineAssociation
- AWS-RunPatchBaselineWithHooks
- AWS-InstanceRebootWithHooks
- AWS-PatchAsgInstance
- AWS-PatchInstanceWithRollback

Nome della Regione	Codice regione	<b>aws-patch-manager-<i>region-suffix</i></b> bucket
Stati Uniti orientali (Ohio)	us-east-2	aws-patch-manager-us-east-2-552881074
Stati Uniti orientali (Virginia settentrionale)	us-east-1	aws-patch-manager-us-east-1-1970c647d
Stati Uniti occidentali (California settentrionale)	us-west-1	aws-patch-manager-us-west-1-8badb4304
Stati Uniti occidentali (Oregon)	us-west-2	aws-patch-manager-us-west-2-34d7f99f8
Africa (Città del Capo)	af-south-1	aws-patch-manager-af-south-1-bdd5f65a9

Nome della Regione	Codice regione	<b>aws-patch-manager- <i>region-suffix</i></b> bucket
Asia Pacific (Hong Kong)	ap-east-1	aws-patch-patch-manager-ap-east-1-632356271
Asia Pacifico (Hyderabad)	ap-south-2	aws-patch-manager-ap-south-2-32f4b4128
Asia Pacifico (Giacarta)	ap-southeast-3	aws-patch-manager-ap-southeast-3-aa48fc462
Asia Pacifico (Melbourne)	ap-southeast-4	aws-patch-manager-ap-southeast-4-01e2c40d3
Asia Pacifico (Mumbai)	ap-south-1	aws-patch-manager-ap-south-1-cb7c62ff9
Asia Pacifico (Osaka)	ap-northeast-3	aws-patch-patch-manager-ap-northeast-3-67373598a
Asia Pacifico (Seoul)	ap-northeast-2	aws-patch-manager-ap-northeast-2-10467995c
Asia Pacifico (Singapore)	ap-southeast-1	aws-patch-manager-ap-southeast-1-7fd9fd9ef7
Asia Pacifico (Sydney)	ap-southeast-2	aws-patch-manager-ap-southeast-2-17283a275
Asia Pacifico (Tokyo)	ap-northeast-1	aws-patch-manager-ap-northeast-1-4849fa78f
Canada (Centrale)	ca-central-1	aws-patch-patch-manager-ca-central-1-3148e69e3
Canada occidentale (Calgary)	ca-west-1	aws-patch-manager-it-west-1-9e3a4b2f9

Nome della Regione	Codice regione	<b>aws-patch-manager- <i>region-suffix</i></b> bucket
Europa (Francoforte)	eu-central-1	aws-patch-patch-manager-eu-central-1-9163fdaaf
Europa (Irlanda)	eu-west-1	aws-patch-patch-manager-eu-west-1-5522fb710
Europa (Londra)	eu-west-2	aws-patch-patch-manager-eu-west-2-902a2bc74
Europa (Milan)	eu-south-1	aws-patch-patch-manager-eu-south-1-c52f3f594
Europa (Parigi)	eu-west-3	aws-patch-patch-manager-eu-west-3-29bf85721
Europa (Spagna)	eu-south-2	aws-patch-manager-eu-south-2-a4cf248b1
Europa (Stoccolma)	eu-north-1	aws-patch-patch-manager-eu-north-1-795879e9b
Europa (Zurigo)	eu-central-2	aws-patch-manager-eu-central-2-184ce43c8
Israele (Tel Aviv)	il-central-1	aws-patch-manager-il-central-1-e221cb57b
Medio Oriente (Bahrein)	me-south-1	aws-patch-patch-manager-me-south-1-a53fc9dce
Medio Oriente (Emirati Arabi Uniti)	me-central-1	aws-patch-manager-me-central-1-2932f2f80
Sud America (San Paolo)	sa-east-1	aws-patch-manager-it-east-1-ddf4b6a09

Nome della Regione	Codice regione	<b>aws-patch-manager-<i>region-suffix</i></b> bucket
Asia Pacifico (Taipei)	ap-east-2	aws-patch-manager-ap-east-2-5a64b2916
Asia Pacifico (Malesia)	ap-southeast-5	aws-patch-manager-ap-southeast-5-dcb42f3e3
Asia Pacifico (Nuova Zelanda)	ap-southeast-6	aws-patch-manager-ap-southeast-6-df0d3a7f2
Asia Pacifico (Thailandia)	ap-southeast-7	aws-patch-manager-ap-southeast-7-c707c017a
Messico (Centrale)	mx-central-1	aws-patch-manager-mx-central-1-396b275ad

## Bucket contenenti documenti SSM Command per le operazioni di patching (macOS)

I bucket con formato `aws-patchmanager-macos-region-unique-suffix` contengono i seguenti documenti utilizzati da Patch Manager per le operazioni di applicazione di patch sul sistema operativo macOS:

- `AWS-RunPatchBaseline`
- `AWS-RunPatchBaselineAssociation`
- `AWS-RunPatchBaselineWithHooks`
- `AWS-InstanceRebootWithHooks`
- `AWS-PatchAsgInstance`
- `AWS-PatchInstanceWithRollback`

Nome della Regione	Codice regione	<b>aws-patchmanager-macos-<i>region-suffix</i></b> bucket
Stati Uniti orientali (Ohio)	us-east-2	aws-patchmanager-macos-us-east-2-552881074
Stati Uniti orientali (Virginia settentrionale)	us-east-1	aws-patchmanager-macos-us-east-1-1970c647d
Stati Uniti occidentali (California settentrionale)	us-west-1	aws-patchmanager-macos-us-west-1-8badb4304
Stati Uniti occidentali (Oregon)	us-west-2	aws-patchmanager-macos-us-west-2-34d7f99f8
Africa (Città del Capo)	af-south-1	aws-patchmanager-macos-af-south-1-bdd5f65a9
Asia Pacific (Hong Kong)	ap-east-1	aws-patchmanager-macos-ap-east-1-632356271
Asia Pacifico (Hyderabad)	ap-south-2	aws-patchmanager-macos-ap-south-2-32f4b4128
Asia Pacifico (Giacarta)	ap-southeast-3	aws-patchmanager-macos-ap-southeast-3-aa48fc462
Asia Pacifico (Melbourne)	ap-southeast-4	aws-patchmanager-macos-ap-southeast-4-01e2c40d3
Asia Pacifico (Mumbai)	ap-south-1	aws-patchmanager-macos-ap-south-1-cb7c62ff9
Asia Pacifico (Osaka-Locale)	ap-northeast-3	aws-patchmanager-macos-ap-northeast-3-67373598a
Asia Pacific (Seoul)	ap-northeast-2	aws-patchmanager-macos-ap-northeast-2-10467995c



Nome della Regione	Codice regione	<b>aws-patchmanager-macos-<i>region-suffix</i></b> bucket
Asia Pacifico (Singapore)	ap-southeast-1	aws-patchmanager-macos-ap-southeast-1-7fd9fd9ef7
Asia Pacifico (Sydney)	ap-southeast-2	aws-patchmanager-macos-ap-southeast-2-17283a275
Asia Pacifico (Tokyo)	ap-northeast-1	aws-patchmanager-macos-ap-northeast-1-4849fa78f
Canada (Centrale)	ca-central-1	aws-patchmanager-macos-ca-central-1-3148e69e3
Canada occidentale (Calgary)	ca-west-1	aws-patchmanager-macos-en-west-1-9e3a4b2f9
Europa (Francoforte)	eu-central-1	aws-patchmanager-macos-eu-central-1-9163fddaaf
Europa (Irlanda)	eu-west-1	aws-patchmanager-macos-eu-west-1-5522fb710
Europa (London)	eu-west-2	aws-patchmanager-macos-eu-west-2-902a2bc74
Europa (Milan)	eu-south-1	aws-patchmanager-macos-eu-south-1-c52f3f594
Europa (Parigi)	eu-west-3	aws-patchmanager-macos-eu-west-3-29bf85721
Europa (Spagna)	eu-south-2	aws-patchmanager-macos-eu-south-2-a4cf248b1
Europa (Stoccolma)	eu-north-1	aws-patchmanager-macos-eu-north-1-795879e9b

Nome della Regione	Codice regione	<b>aws-patchmanager-macos-<i>region</i>-suffix</b> bucket
Europa (Zurigo)	eu-central-2	aws-patchmanager-macos-eu-central-2-184ce43c8
Israele (Tel Aviv)	il-central-1	aws-patchmanager-macos-il-central-1-e221cb57b
Medio Oriente (Bahrein)	me-south-1	aws-patchmanager-macos-me-south-1-a53fc9dce
Medio Oriente (Emirati Arabi Uniti)	me-central-1	aws-patchmanager-macos-me-central-1-2932f2f80
Sud America (San Paolo)	sa-east-1	aws-patchmanager-macos-sa-east-1-ddf4b6a09
Asia Pacifico (Taipei)	ap-east-2	aws-patchmanager-macos-ap-east-2-5a64b2916
Asia Pacifico (Malesia)	ap-southeast-5	aws-patchmanager-macos-ap-southeast-5-dcb42f3e3
Asia Pacifico (Nuova Zelanda)	ap-southeast-6	aws-patchmanager-macos-ap-southeast-6-df0d3a7f2
Asia Pacifico (Thailandia)	ap-southeast-7	aws-patchmanager-macos-ap-southeast-7-c707c017a
Messico (Centrale)	mx-central-1	aws-patchmanager-macos-mx-central-1-396b275ad

## Secchi contenenti AWS istantanee della baseline delle patch gestite

Bucket con il formato `patch-baseline-snapshot-region` o `patch-baseline-snapshot-region-unique-suffix` contengono istantanee della baseline delle patch AWS

gestite. È necessario accedere a questo bucket S3 quando si utilizza uno dei seguenti documenti SSM:

- AWS-RunPatchBaseline
- AWS-RunPatchBaselineAssociation
- AWS-RunPatchBaselineWithHooks
- AWS-ApplyPatchBaseline (un documento SSM legacy)

Nome della Regione	Codice regione	<b>patch-baseline-snapshot-*</b> bucket
Stati Uniti orientali (Ohio)	us-east-2	patch-baseline-snapshot-us-east-2
Stati Uniti orientali (Virginia settentrionale)	us-east-1	patch-baseline-snapshot-us-east-1
Stati Uniti occidentali (California settentrionale)	us-west-1	patch-baseline-snapshot-us-west-1
Stati Uniti occidentali (Oregon)	us-west-2	patch-baseline-snapshot-us-west-2
Africa (Città del Capo)	af-south-1	patch-baseline-snapshot-af-south-1-tbxdb5b9
Asia Pacific (Hong Kong)	ap-east-1	patch-baseline-snapshot-ap-east-1
Asia Pacifico (Hyderabad)	ap-south-2	patch-baseline-snapshot-ap-south-2-50209442
Asia Pacifico (Giacarta)	ap-southeast-3	patch-baseline-snapshot-ap-southeast-3-be0a3174
Asia Pacifico (Melbourne)	ap-southeast-4	patch-baseline-snapshot-ap-southeast-4-dc6f76ce

Nome della Regione	Codice regione	<b>patch-baseline-snapshot-*</b> bucket
Asia Pacifico (Mumbai)	ap-south-1	patch-baseline-snapshot-ap-south-1
Asia Pacifico (Osaka-Locale)	ap-northeast-3	patch-baseline-snapshot-ap-northeast-3
Asia Pacific (Seoul)	ap-northeast-2	patch-baseline-snapshot-ap-northeast-2
Asia Pacifico (Singapore)	ap-southeast-1	patch-baseline-snapshot-ap-southeast-1
Asia Pacifico (Sydney)	ap-southeast-2	patch-baseline-snapshot-ap-southeast-2
Asia Pacifico (Tokyo)	ap-northeast-1	patch-baseline-snapshot-ap-northeast-1
Canada (Centrale)	ca-central-1	patch-baseline-snapshot-ca-central-1
Canada occidentale (Calgary)	ca-west-1	patch-baseline-snapshot-ca-west-1
Europa (Francoforte)	eu-central-1	patch-baseline-snapshot-eu-central-1
Europa (Irlanda)	eu-west-1	patch-baseline-snapshot-eu-west-1
Europe (London)	eu-west-2	patch-baseline-snapshot-eu-west-2
Europe (Milan)	eu-south-1	patch-baseline-snapshot-eu-south-1

Nome della Regione	Codice regione	<b>patch-baseline-snapshot-*</b> bucket
Europa (Parigi)	eu-west-3	patch-baseline-snapshot-eu-west-3
Europa (Spagna)	eu-south-2	patch-baseline-snapshot-eu-south-2-df2c9d70
Europa (Stoccolma)	eu-north-1	patch-baseline-snapshot-eu-north-1
Europa (Zurigo)	eu-central-2	patch-baseline-snapshot-eu-central-2
Israele (Tel Aviv)	il-central-1	patch-baseline-snapshot-il-central-1
Medio Oriente (Bahrein)	me-south-1	patch-baseline-snapshot-me-south-1-uduvl7q8
Medio Oriente (Emirati Arabi Uniti)	me-central-1	patch-baseline-snapshot-me-central-1
Sud America (San Paolo)	sa-east-1	patch-baseline-snapshot-sa-east-1
Asia Pacifico (Taipei)	ap-east-2	patch-baseline-snapshot-ap-east-2-8947749e
Asia Pacifico (Malesia)	ap-southeast-5	patch-baseline-snapshot-ap-southeast-5
Asia Pacifico (Nuova Zelanda)	ap-southeast-6	patch-baseline-snapshot-ap-southeast-6-62f446f2
Asia Pacifico (Thailandia)	ap-southeast-7	patch-baseline-snapshot-ap-southeast-7-1699f14f

Nome della Regione	Codice regione	<b>patch-baseline-snapshot-*</b> bucket
Messico (Centrale)	mx-central-1	patch-baseline-snapshot-mx-central-1-ed0da79c

## Riferimento: modelli e tipi di EventBridge eventi Amazon per Systems Manager

### Note

Amazon EventBridge è il modo preferito per gestire i tuoi eventi. CloudWatch Events e EventBridge 2 sono lo stesso servizio e la stessa API di base, ma EventBridge offrono più funzionalità. Le modifiche apportate in una delle due console CloudWatch o EventBridge si riflettono in ciascuna console. Per ulteriori informazioni, consulta la [Amazon EventBridge User Guide](#).

Con Amazon EventBridge, puoi creare regole che corrispondono agli eventi in arrivo e indirizzarli verso le destinazioni per l'elaborazione.

Un evento indica una modifica in un ambiente nelle proprie applicazioni, applicazioni software as a service (SaaS) o un Servizio AWS. Gli eventi vengono prodotti nel miglior modo possibile. Dopo aver rilevato un tipo di evento specificato in una regola, lo EventBridge indirizza a una destinazione specificata per l'elaborazione. Gli obiettivi possono includere istanze di Amazon Elastic Compute Cloud (Amazon EC2), AWS Lambda funzioni, flussi Amazon Kinesis, attività di Amazon Elastic Container Service (Amazon ECS), macchine a stati, argomenti Amazon Simple Notification Service (Amazon SNS), AWS Step Functions Amazon Simple Queue Service (Amazon SQS) QS) code, obiettivi integrati e molto altro.

Per informazioni sulla creazione di regole, consulta i seguenti argomenti: EventBridge

- [Monitoraggio degli eventi di Systems Manager con Amazon EventBridge](#)
- [Esempi di EventBridge eventi Amazon per Systems Manager](#)
- [Come iniziare a usare Amazon EventBridge](#) nella Amazon EventBridge User Guide

Il resto di questo argomento descrive i tipi di eventi Systems Manager che è possibile includere nelle EventBridge regole.

## Tipo di evento: automazione

Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
Notifica di esecuzione di EC2 Automation Status-change	<p>Modifica dello stato generale di un flusso di lavoro di automazione. È possibile aggiungere e una o più delle seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"><li>• Approvato</li><li>• Annullato</li><li>• Non riuscito</li><li>• PendingApproval</li><li>• PendingChangeCalendarOverride</li><li>• Rifiutato</li><li>• Pianificato</li><li>• Completato</li><li>• TimedOut</li></ul>
Notifica della fase di automazione EC2 Status-change	<p>Modifica dello stato di un passaggio specifico di un flusso di lavoro di automazione. È possibile aggiungere una o più delle seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"><li>• Annullato</li><li>• Non riuscito</li><li>• Completato</li><li>• TimedOut</li></ul>

## Tipo di evento: Change Calendar

Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
Modifica dello stato del calendario	<p>Lo stato di un Change Calendar cambia. È possibile aggiungere una o entrambe le seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"><li>• APERTO</li><li>• CHIUSO</li></ul> <p>Le modifiche di stato per i calendari condivisi da altri Account AWS non sono supportate.</p>

## Tipo di evento: Change Manager

### Change Managermodifica della disponibilità

AWS Systems ManagerChange Managernon sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarloChange Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems ManagerChange Managerla pagina Modifica della disponibilità](#).

Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
Aggiornamento dello stato della richiesta di modifica	<p>Lo stato di una richiesta di modifica di Change Manager. Puoi utilizzare gli stati seguenti in una regola di evento:</p> <ul style="list-style-type: none"><li>• Approvato</li><li>• Rifiutato</li></ul>



Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
	<ul style="list-style-type: none"><li>• InProgress</li></ul>

## Tipo di evento: conformità di configurazione

Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
Modifica dello stato di conformità della configurazione	<p>Lo stato di nodo gestito cambia sia per conformità delle associazioni o per conformità delle patch. È possibile aggiungere una o più delle seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"><li>• conforme</li><li>• non_conforme</li></ul>

## Tipo di evento: Inventario

Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
Modifica dello stato della risorsa inventario	<p>L'eliminazione dell'inventario personalizzato e una <a href="#">PutInventory</a> chiamata che utilizza una vecchia versione dello schema. È possibile aggiungere una o più delle seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"><li>• Evento eliminato del tipo di inventario personalizzato su un nodo specifico. EventBridge invia un evento per nodo per personalizzazione InventoryType.</li></ul>

Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
	<ul style="list-style-type: none"> <li>Evento eliminato per tipo di inventario personalizzato su tutti i nodi.</li> <li>PutInventory chiamata con un evento della vecchia versione dello schema. EventBridge geinvia questo evento quando la versione dello schema è inferiore allo schema corrente. Questo evento si applica a tutti i tipi di inventario.</li> </ul> <p>Per ulteriori informazioni, consulta <a href="#">Utilizzo EventBridge per monitorare gli eventi dell'inventario</a>.</p>

## Tipo di evento: finestra di manutenzione

Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
Status-change Notifica della finestra di manutenzione	<p>Lo stato generale di uno o più target della finestra di manutenzione cambia. È possibile aggiungere una o più delle seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"> <li>DISABILITATO</li> <li>ABILITATO</li> </ul>
Notifica di registrazione del target della finestra di manutenzione	<p>Lo stato di uno o più target della finestra di manutenzione cambia. È possibile aggiungere e una o più delle seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"> <li>REGISTRAZIONE ANNULLATA</li> <li>REGISTRATO</li> </ul>

Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
	<ul style="list-style-type: none"><li>• AGGIORNATO</li></ul>
State-change Notifica di esecuzione della finestra di manutenzione	<p>Lo stato generale di una finestra di manutenzi one cambia durante l'esecuzione. È possibile aggiungere una o più delle seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"><li>• ANNULLATO</li><li>• IN CORSO DI ANNULLAMENTO</li><li>• NON RIUSCITO</li><li>• IN_PROGRESS</li><li>• IN ATTESA</li><li>• SKIPPED_OVERLAPPING</li><li>• RIUSCITO</li><li>• TIMED_OUT</li></ul>
Notifica di esecuzione delle attività nella finestra di manutenzione State-change	<p>Lo stato di un processo in una finestra di manutenzione cambia durante l'esecuzione. È possibile aggiungere una o più delle seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"><li>• ANNULLATO</li><li>• IN CORSO DI ANNULLAMENTO</li><li>• NON RIUSCITO</li><li>• IN_PROGRESS</li><li>• RIUSCITO</li><li>• TIMED_OUT</li></ul>

Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
Notifica di chiamata di Task Target della finestra di manutenzione State-change	<p>Lo stato di un processo della finestra di manutenzione su una destinazione specifica cambia.</p> <p>Questa notifica è completamente supportata solo per le attività Run Command. Per questo tipo di processo, è possibile aggiungere una o più delle seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"><li>• ANNULLATO</li><li>• IN CORSO DI ANNULLAMENTO</li><li>• NON RIUSCITO</li><li>• IN_PROGRESS</li><li>• RIUSCITO</li><li>• TIMED_OUT</li></ul> <p>Per Automation e AWS Step Functions Tasks AWS Lambda, EventBridge riporta solo gli stati e. IN_PROGRESS COMPLETE COMPLETEviene segnalato se l'operazione ha esito positivo o meno.</p>
Notifica della registrazione del processo della finestra di manutenzione	<p>Lo stato di uno o più processi della finestra di manutenzione cambia. È possibile aggiungere una o più delle seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"><li>• REGISTRAZIONE ANNULLATA</li><li>• REGISTRATO</li><li>• AGGIORNATO</li></ul>

## Tipo di evento: OpsCenter

Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
Creazione di OpsItem	<p>Si verifica quando viene creato un OpsItem. È possibile aggiungere regole per uno dei seguenti tipi di OpsItem:</p> <ul style="list-style-type: none"><li>• /aws/issue</li><li>• /aws/task</li><li>• /aws/insight</li><li>• /aws/actionitem</li></ul>
Aggiornamento di OpsItem	<p>Si verifica quando viene creato un OpsItem. È possibile aggiungere regole per uno dei seguenti tipi di OpsItem:</p> <ul style="list-style-type: none"><li>• /aws/issue</li><li>• /aws/task</li><li>• /aws/insight</li><li>• /aws/actionitem</li></ul>

## Tipo di evento: Parameter Store

Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
Modifica Archivio parametri	<p>Lo stato di un parametro cambia. È possibile aggiungere una o più delle seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"><li>• Crea</li><li>• Aggiorna</li><li>• Elimina</li></ul>

Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
	<ul style="list-style-type: none"> <li>LabelParameterVersion</li> </ul> <p>Per ulteriori informazioni, consulta <a href="#">Configurazione delle EventBridge regole per i parametri e delle politiche relative ai parametri</a>.</p>
Operazione della policy su Archivio parametri	<p>Viene soddisfatta una condizione di una modifica dei parametri avanzati della policy. È possibile aggiungere una o più delle seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"> <li>Scadenza</li> <li>ExpirationNotification</li> <li>NoChangeNotification</li> </ul> <p>Per ulteriori informazioni, consulta <a href="#">Configurazione delle EventBridge regole per i parametri e delle politiche relative ai parametri</a>.</p>

## Tipo di evento: Run Command

Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
Notifica di Status-change invocazione dei comandi EC2	<p>Lo stato di un comando inviato a una singola istanza gestita cambia. È possibile aggiungere una o più delle seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"> <li>Completato</li> <li>InProgress</li> <li>TimedOut</li> </ul>

Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
	<ul style="list-style-type: none"> <li>• Annullato</li> <li>• Non riuscito</li> </ul>
Notifica dei comandi EC2 Status-change	<p>Lo stato generale di un comando cambia. È possibile aggiungere una o più delle seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"> <li>• Completato</li> <li>• InProgress</li> <li>• TimedOut</li> <li>• Annullato</li> <li>• Non riuscito</li> </ul>

## Tipo di evento: State Manager

Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
EC2 State Manager Modifica dello stato dell'associazione	<p>Lo stato generale di un'associazione cambia man mano che viene applicata. È possibile aggiungere una o più delle seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"> <li>• Non riuscito</li> <li>• Pending (In attesa)</li> <li>• Completato</li> </ul>
EC2 State Manager Modifica dello stato dell'associazione dell'istanza	<p>Lo stato di una singola istanza gestita a cui è destinata un'associazione cambia. È possibile aggiungere una o più delle seguenti modifiche di stato a una regola di evento:</p> <ul style="list-style-type: none"> <li>• Non riuscito</li> </ul>

Nome tipo di evento	Descrizione degli eventi che è possibile aggiungere a una regola
	<ul style="list-style-type: none"><li>• Pending (In attesa)</li><li>• Completato</li></ul>

## Riferimento: espressioni Cron e della frequenza per Systems Manager

Quando si crea un'associazione o una finestra di manutenzione in AWS Systems Manager, si specifica una pianificazione per l'esecuzione della finestra o dell'associazione. Una pianificazione può essere specificata come elemento basato sul tempo, denominato espressione Cron, oppure come elemento basato sulla frequenza, denominato espressione della frequenza.

### Informazioni generali sulle espressioni Cron e della frequenza

Le seguenti informazioni si applicano alle espressioni Cron e della frequenza sia per le finestre di manutenzione che per le associazioni.

#### Single-run pianificazioni

Quando crei un'associazione o una finestra di manutenzione è possibile anche specificare un timestamp in formato UTC (Coordinated Universal Time) in modo che venga eseguita all'ora specificata. Ad esempio: "at(2020-07-07T15:55:00)"

#### Offset di pianificazione

Le associazioni e le finestre di manutenzione supportano anche gli offset di pianificazione solo per le espressioni cron. Un offset di pianificazione è il numero di giorni di attesa dopo la data e l'ora specificate da un'espressione CRON per l'avvio dell'esecuzione della finestra di manutenzione.

#### Maintenance window example

Nel comando riportato di seguito, l'espressione Cron pianifica l'esecuzione di una finestra di manutenzione il terzo martedì di ogni mese alle 23:30. Tuttavia, poiché l'offset di pianificazione è 2, la finestra di manutenzione non sarà eseguita fino alle 23:30 di due giorni dopo.

```
aws ssm create-maintenance-window \
```



```
--name "My-Cron-Offset-Maintenance-Window" \
--allow-unassociated-targets \
--schedule "cron(30 23 ? * TUE#3 *)" \
--duration 4 \
--cutoff 1 \
--schedule-offset 2
```

## Association example

Nel comando seguente, l'espressione Cron pianifica l'esecuzione di un'associazione il secondo giovedì di ogni mese. Tuttavia, poiché l'offset di pianificazione è 3, l'associazione non sarà attiva fino alla domenica successiva, tre giorni dopo.

```
aws ssm create-association \
 --name "AWS-UpdateSSMAgent" \
 --targets "Key=instanceids,Values=i-0cb2b964d3e14fd9f" \
 --schedule-expression "cron(0 0 ? * THU#2 *)" \
 --schedule-offset 3
 --apply-only-at-cron-interval
```

### Note

Per utilizzare un offset con un'associazione, è necessario specificare l'opzione `--apply-only-at-cron-interval`. Questa opzione indica al sistema di non eseguire un'associazione immediatamente dopo averla creata.

Se crei una finestra di manutenzione o associazione con un'espressione Cron che ha come destinazione un giorno già passato nel periodo corrente, ma aggiungi una data di offset di pianificazione che ricade in futuro, la finestra di manutenzione o associazione non viene eseguita nel periodo. Verrà eseguita nel periodo successivo. Ad esempio, se specifichi un'espressione Cron che avrebbe eseguito una finestra di manutenzione ieri e aggiungi un offset di pianificazione di due giorni, la finestra di manutenzione non verrà eseguita domani.

## Campi obbligatori

Le espressioni Cron per la manutenzione hanno sei campi obbligatori. Le espressioni cron per le associazioni ne hanno cinque. (State Manager attualmente non supporta la specifica di mesi nelle espressioni cron per le associazioni.) Un campo aggiuntivo, Seconds, (il primo in un'espressione cron), è facoltativo. I campi sono separati da uno spazio.

## Esempi di espressioni Cron

Minuti	Ore	Giorno del mese	Mese	Giorno della settimana	Anno	Significato
0	10	*	*	?	*	Esegui ogni giorno alle 10:00 (UTC)
15	12	*	*	?	*	Esegui ogni giorno alle 12.15 (UTC)
0	18	?	*	MON-FRI	*	Funziona alle 18:00 (UTC) dal lunedì al venerdì (solo nei periodi di manutenzione)
0	8	1	*	?	*	Esegui ogni primo giorno del mese alle 8:00 (UTC)

**Note**

Day-of-week gli intervalli (ad esempio MON-FRI) e gli elenchi di giorni separati da virgole (ad esempio MON, TUE, WED) sono supportati solo per le finestre di manutenzione. Per le associazioni, è necessario specificare un solo giorno (ad esempio MON) o utilizzarlo \* per tutti i giorni.

**Valori supportati**

La tabella seguente mostra i valori supportati per le voci Cron richieste.

Valori supportati per le espressioni Cron

Campo	Valori	Caratteri jolly
Minuti	0-59	, - * /
Ore	0-23	, - * /
Day-of-month	1-31	, - * ? / L W
Mese (solo finestre di manutenzione)	1-12 o JAN-DEC	, - * /
Day-of-week	1-7 o SUN-SAT	, - * ? / L #
Anno	1970-2199	, - * /

**Note**

Non è possibile specificare un valore nei campi giorno-del-mese) e giorno-della-settimana nella stessa espressione Cron. Se specifichi un valore in uno dei campi, usa un carattere ? (punto interrogativo) nell'altro campo.

**Caratteri jolly per le espressioni cron**

La tabella che segue mostra i valori jolly supportati dalle espressioni Cron.

**Note**

Systems Manager non supporta le espressioni cron che generano velocità superiori a 5 minuti per le finestre di manutenzione. Per State Manager le associazioni, è necessario utilizzare un intervallo di pianificazione di almeno 30 minuti. Per ulteriori informazioni sulle limitazioni alla pianificazione delle associazioni, vedere. [Espressioni Cron e della frequenza per le associazioni](#) Il supporto per specificare entrambi i valori per giorno-della-settimana e giorno-del-mese non è ancora completo. Devi utilizzare il punto interrogativo (?) in uno di questi campi.

## Caratteri jolly supportati per le espressioni Cron

Carattere jolly	Description
,	Il carattere jolly , (virgola) include valori aggiuntivi. Nel campo Month (Mese), JAN,FEB,MAR (GEN,FEB,MAR) include gennaio, febbraio e marzo.
-	Il carattere jolly - (trattino) specifica gli intervalli. Nel campo Day (Giorno), 1-15 include i giorni dall'1 al 15 del mese specificato.
*	Il carattere jolly * (asterisco) include tutti i valori nel campo. Nel campo Hours (Ore), * include ogni ora.
/	Il carattere jolly / (barra) specifica gli incrementi. Nel campo Minuti, è possibile immettere 1/10 per specificare ogni decimo minuto, a partire dal primo minuto dell'ora. Quindi 1/10 specifica il primo, l'11°, il 21° e il 31° minuto e così via.
?	Il carattere jolly ? (punto interrogativo) specifica uno dei valori. Nel Day-of-month

Carattere jolly	Description
	campo puoi inserire 7 e se non ti interessasse che giorno della settimana era il 7, potresti inserire? nel Day-of-week campo.
L	Il L carattere jolly nei Day-of-week campi Day-of-month o specifica l'ultimo giorno del mese o della settimana.
W	Il carattere W jolly nel Day-of-month campo specifica un giorno della settimana. Nel Day-of-month campo, 3W specifica il giorno più vicino al terzo giorno della settimana del mese.
#	Il carattere jolly # nel campo giorno-della-settimana seguito da un numero compreso tra uno e cinque specifica un dato giorno del mese. 5#3 specifica il terzo venerdì del mese.

## Espressioni della frequenza

Le espressioni della frequenza hanno i due seguenti campi obbligatori. I campi sono separati da spazi.

Campi obbligatori per le espressioni della frequenza

Campo	Valori
Valore	numero positivo, ad esempio 1 o 15
Unità	minute minutes hour hours

Campo	Valori
	day
	days

Se il valore è uguale a 1, l'unità deve essere singolare. Analogamente, per valori maggiori di 1, l'unità deve essere plurale. Ad esempio, `rate(1 hours)` e `rate(5 hour)` non sono validi, mentre lo sono `rate(1 hour)` e `rate(5 hours)`.

### Argomenti

- [Espressioni Cron e della frequenza per le associazioni](#)
- [Espressioni Cron e della frequenza per le finestre di manutenzione](#)

## Espressioni Cron e della frequenza per le associazioni

Questa sezione include esempi di espressioni Cron e della frequenza per le associazioni State Manager. Prima di creare una di tali espressioni, devi conoscere le seguenti informazioni:

### Important

Per State Manager le associazioni, è necessario utilizzare un intervallo di pianificazione di almeno 30 minuti. Non è possibile utilizzare espressioni cron o rate che generano intervalli inferiori a 30 minuti. Ad esempio, non puoi usare `cron(0/5 * * * ? *)` (ogni 5 minuti) o `rate(15 minutes)`. Il minimo di 5 minuti descritto nella sezione sulle espressioni cron generali si applica solo alle finestre di manutenzione, non alle associazioni.

- Le associazioni supportano le seguenti espressioni cron: Ogni 1/2, 1, 2, 4, 8 o 12 ore; ogni giorno, ogni settimana o ogni giorno e ora della settimana specificati; un giorno specifico in una settimana specifica del mese o l'ultimo x giorno del mese a un'ora specifica.
- Le associazioni supportano le seguenti espressioni della frequenza: intervalli di 30 minuti o maggiori e meno di 31 giorni.
- Se specifichi il campo Seconds facoltativo, il relativo valore può essere 0 (zero). Ad esempio: `cron(0 */30 * * * ? *)`

- Per un'associazione che raccoglie i metadati per l'inventario , ti consigliamo di utilizzare un'espressione tariffaria.
- State Manager attualmente non supporta la specifica di mesi nelle espressioni cron per le associazioni.

Le associazioni supportano espressioni cron che includono un giorno della settimana e il segno numerico (#) per designare il n giorno di un mese per gestire un'associazione. Ecco un esempio che esegue un programma cron il terzo martedì di ogni mese alle 23:30 UTC:

```
cron(30 23 ? * TUE#3 *)
```

Ecco un esempio che viene eseguito il secondo giovedì di ogni mese a mezzanotte UTC:

```
cron(0 0 ? * THU#2 *)
```

Le associazioni supportano anche il segno (L) per indicare l'ultimo X giorno del mese. Ecco un esempio che esegue un programma cron l'ultimo martedì di ogni mese a mezzanotte UTC:

```
cron(0 0 ? * 3L *)
```

Per controllare ulteriormente l'esecuzione di un'associazione, ad esempio se si desidera eseguire un'associazione due giorni dopo la patch di martedì, è possibile specificare un offset. Un record offset definisce quanti giorni attendere dopo il giorno programmato per eseguire un'associazione. Ad esempio, se hai specificato un programma cron di `cron(0 0 ? * THU#2 *)`, è possibile specificare il numero 3 nel campo Offset di pianificazione per eseguire l'associazione ogni domenica dopo il secondo giovedì del mese.

Per utilizzare gli offset, è necessario o scegliere l'opzione **Applica associazione solo al prossimo intervallo Cron** specificato nella console o è necessario specificare l'uso del parametro `--apply-only-at-cron-interval` dalla riga di comando. Questa opzione dice a State Manager di non eseguire un'associazione immediatamente dopo la creazione.

La tabella seguente presenta esempi di espressioni cron per le associazioni.

#### Esempi di espressioni Cron per le associazioni

Esempio	Informazioni
<code>cron(0/30 * * * ? *)</code>	Ogni 30 minuti
<code>cron(0 0/1 * * * ? *)</code>	Ogni ora

Esempio	Informazioni
<code>cron(0 0/2 * * ? *)</code>	Ogni 2 ore
<code>cron(0 0/4 * * ? *)</code>	Ogni 4 ore
<code>cron(0 0/8 * * ? *)</code>	Ogni 8 ore
<code>cron(0 0/12 * * ? *)</code>	Ogni 12 ore
<code>cron(15 13 ? * * *)</code>	Ogni giorno alle 13.15
<code>cron(15 13 ? * MON *)</code>	Ogni lunedì alle 13.15
<code>cron(30 23 ? * TUE#3 *)</code>	Il terzo martedì di ogni mese alle 23:30

Di seguito sono elencati alcuni esempi di espressioni Rate per le associazioni.

#### Esempi di espressioni Rate per le associazioni

Esempio	Informazioni
<code>rate(30 minutes)</code>	Ogni 30 minuti
<code>rate(1 hour)</code>	Ogni ora
<code>rate(5 hours)</code>	Ogni 5 ore
<code>rate(15 days)</code>	Ogni 15 giorni

#### AWS CLI esempi di associazioni

Per creare State Manager associazioni utilizzando il AWS CLI, includi il `--schedule-expression` parametro con un'espressione cron o rate. Gli esempi seguenti utilizzano il comando AWS CLI su una macchina Linux locale.

#### Note

Per impostazione predefinita, quando si crea una nuova associazione, il sistema viene eseguito immediatamente dopo la creazione e quindi in base alla pianificazione specificata.



Specifica `--apply-only-at-cron-interval` in modo che l'associazione non venga eseguita immediatamente dopo la creazione. Questo parametro non è supportato per le espressioni della frequenza.

```
aws ssm create-association \
 --association-name "My-Cron-Association" \
 --schedule-expression "cron(0 2 ? * SUN *)" \
 --targets Key=tag:ServerRole,Values=WebServer \
 --name AWS-UpdateSSMAgent
```

```
aws ssm create-association \
 --association-name "My-Rate-Association" \
 --schedule-expression "rate(7 days)" \
 --targets Key=tag:ServerRole,Values=WebServer \
 --name AWS-UpdateSSMAgent
```

```
aws ssm create-association \
 --association-name "My-Rate-Association" \
 --schedule-expression "at(2020-07-07T15:55:00)" \
 --targets Key=tag:ServerRole,Values=WebServer \
 --name AWS-UpdateSSMAgent \
 --apply-only-at-cron-interval
```

## Espressioni Cron e della frequenza per le finestre di manutenzione

Questa sezione include esempi di espressioni Cron e della frequenza per le finestre di manutenzione.

A differenza delle associazioni State Manager, le finestre di manutenzione supportano tutte le espressioni Cron e della frequenza. Ciò include il supporto per i valori nel campo dei secondi.

Ad esempio, la seguente espressione Cron composta da 6 campi esegue una finestra di manutenzione ogni giorno alle 9:30.

```
cron(30 09 ? * * *)
```

Aggiungendo un valore al campo Seconds, la seguente espressione Cron composta da 7 campi esegue una finestra di manutenzione ogni giorno alle 9:30:24.

```
cron(24 30 09 ? * * *)
```

La tabella seguente fornisce ulteriori esempi di espressioni Cron composte da 6 campi per le finestre di manutenzione.

#### Esempi di espressioni Cron per finestre di manutenzione

Esempio	Informazioni
<code>cron(0 2 ? * THU#3 *)</code>	Il terzo giovedì di ogni mese alle 02.00
<code>cron(15 10 ? * * *)</code>	Ogni giorno alle 10.15
<code>cron (15) 10? * MON-FRI *)</code>	Ogni lunedì, martedì, mercoledì, giovedì e venerdì alle 10.15
<code>cron(0 2 L * ? *)</code>	L'ultimo giorno di ogni mese alle 02.00
<code>cron(15 10 ? * 6L *)</code>	L'ultimo venerdì di ogni mese alle 10.15

La tabella seguente fornisce esempi di espressioni Rate per le finestre di manutenzione.

#### Esempi di espressioni Rate per le finestre di manutenzione

Esempio	Informazioni
<code>rate(30 minutes)</code>	Ogni 30 minuti
<code>rate(1 hour)</code>	Ogni ora
<code>rate(5 hours)</code>	Ogni 5 ore
<code>rate(25 days)</code>	Ogni 25 giorni

#### AWS CLI esempi di finestre di manutenzione

Per creare finestre di manutenzione utilizzando il AWS CLI, includi il `--schedule` parametro con un'espressione cron o rate o un timestamp. Gli esempi seguenti utilizzano il comando AWS CLI su una macchina Linux locale.

```
aws ssm create-maintenance-window \
 --name "My-Cron-Maintenance-Window" \
 --allow-unassociated-targets \
 --schedule "cron(0 16 ? * TUE *)" \
 --schedule-timezone "America/Los_Angeles" \
 --start-date 2021-01-01T00:00:00-08:00 \
 --end-date 2021-06-30T00:00:00-08:00 \
 --duration 4 \
 --cutoff 1
```

```
aws ssm create-maintenance-window \
 --name "My-Rate-Maintenance-Window" \
 --allow-unassociated-targets \
 --schedule "rate(7 days)" \
 --duration 4 \
 --schedule-timezone "America/Los_Angeles" \
 --cutoff 1
```

```
aws ssm create-maintenance-window \
 --name "My-TimeStamp-Maintenance-Window" \
 --allow-unassociated-targets \
 --schedule "at(2021-07-07T13:15:30)" \
 --duration 4 \
 --schedule-timezone "America/Los_Angeles" \
 --cutoff 1
```

Ulteriori informazioni

[Espressione CRON](#) sul sito di Wikipedia

## Referenza: ec2messages, ssmmessages e altre operazioni API

Quando si monitorano le operazioni API, è possibile vedere le chiamate alle seguenti operazioni:

- `ec2messages:AcknowledgeMessage`
- `ec2messages>DeleteMessage`
- `ec2messages:FailMessage`
- `ec2messages:GetEndpoint`
- `ec2messages:GetMessages`

- `ec2messages:SendReply`
- `ssmmessages:CreateControlChannel`
- `ssmmessages:CreateDataChannel`
- `ssmmessages:OpenControlChannel`
- `ssmmessages:OpenDataChannel`
- `ssm:DescribeDocumentParameters`
- `ssm:DescribeInstanceProperties`
- `ssm:GetCalendar`
- `ssm:GetManifest`
- `ssm:ListInstanceAssociations`
- `ssm:PutCalendar`
- `ssm:PutConfigurePackageResult`
- `ssm:RegisterManagedInstance`
- `ssm:RequestManagedInstanceRoleToken`
- `ssm:UpdateInstanceAssociationStatus`
- `ssm:UpdateInstanceInformation`
- `ssm:UpdateManagedInstancePublicKey`

Si tratta di operazioni speciali utilizzate da AWS Systems Manager, come descritto nel resto di questo argomento.

## Agent-related Operazioni API (endpoint **ssmmessages** ed **ec2messages**)

### Operazioni API ssmmessages

Systems Manager utilizza l'endpoint `ssmmessages` per i seguenti tipi di operazioni API:

- Operazioni dall'agente Systems Manager (SSM Agent) al servizio Systems Manager nel cloud.
- Operazioni da SSM Agent e nel cloud. Session Manager Questo endpoint è necessario per creare ed eliminare i canali di sessione con il Session Manager servizio nel cloud.

Se la connettività è consentita, SSM Agent riceve Command i documenti tramite Amazon Message Gateway Service. Se la connettività non è consentita, SSM Agent riceve i documenti di Command

tramite Amazon Message Delivery Service. Per ulteriori informazioni, consulta [Operazioni, risorse e chiavi di condizione per Amazon Message Gateway Service](#).

#### Note

Se l'`ssmmessages:OpenControlChannel` autorizzazione viene rimossa dalle policy allegate al profilo dell'istanza IAM o al ruolo del servizio IAM, SSM Agent sul nodo gestito perde la connettività al servizio Systems Manager nel cloud. Tuttavia, l'interruzione di una connessione può richiedere fino a 1 ora dopo la rimozione dell'autorizzazione. Si tratta dello stesso comportamento di quando il ruolo di istanza IAM o il ruolo del servizio IAM viene eliminato.

L'`ssmmessages:OpenControlChannel` autorizzazione è inclusa nella policy gestita [AmazonSSMManagedInstanceCore](#), utilizzata nelle istruzioni per [creare un profilo di istanza IAM per le istanze EC2](#) e per [creare un ruolo](#) di servizio IAM per le istanze non EC2.

- Operazioni da Run Command.

## Operazioni API `ec2messages`

Le operazioni API `ec2messages:*` vengono effettuate per l'endpoint Amazon Message Delivery Service. Systems Manager utilizza questo endpoint per effettuare operazioni API da Systems Manager Agent (SSM Agent) al servizio Systems Manager nel cloud.

#### Important

Le operazioni API `ec2messages:*` sono supportate solo nelle Regioni AWS avviate prima del 2024. Nelle regioni avviate dal 2024 in poi, sono supportate solo le operazioni API `ssmmessages:*`.

## Priorità delle connessioni all'endpoint

A partire dalla versione 3.3.40.0 dell'SSM Agent, Systems Manager ha iniziato a utilizzare endpoint `ssmmessages:*` (Amazon Message Gateway Service) ogni volta che era disponibile, al posto dell'endpoint `ec2messages:*` (Amazon Message Delivery Service).

Se fornisci l'accesso alle `ssmmessages:*` tue politiche di autorizzazione AWS Identity and Access Management (IAM), SSM Agent si connette all'endpoint. `ssmmessages:*` Ciò vale anche se il

profilo dell'istanza IAM è configurato per consentire entrambi gli endpoint. Ciò include le policy per i [profili dell'istanza](#) e i [ruoli di servizio IAM](#) creati, nonché per i profili dell'istanza IAM creati dalla [Configurazione di gestione host di Quick Setup](#) e dalla [Configurazione di gestione host predefinita](#).

Se hai fornito le autorizzazioni per entrambi gli endpoint e monitora le operazioni API utilizzando, ad esempio, CloudWatch Metrics, non vedi chiamate a `ec2messages : *`

Per il Regioni AWS lancio prima del 2024: al momento puoi rimuovere in sicurezza le `ec2messages : *` autorizzazioni dalle tue policy.

### Failover della connessione all'endpoint

Il seguente comportamento di failover si applica solo ai Regioni AWS lanci prima del 2024.

Se il profilo dell'istanza IAM fornisce `ec2messages : *` le autorizzazioni solo all'avvio dell'agente, si SSM Agent connette all'endpoint. `ec2messages : *`

Se il profilo dell'istanza IAM fornisce entrambe `ssmmessages : *` le `ec2messages : *` autorizzazioni all'avvio dell'agente, ma successivamente le rimuovi `ssmmessages : *`, SSM Agent passa all'endpoint. `ec2messages : *`

Per le regioni avviate dal 2024 in poi, è supportato solo l'endpoint `ssmmessages : *`.

Per ulteriori informazioni sugli endpoint `ssmmessages` e `ec2messages : *`, consulta gli argomenti seguenti nella Referenza sull'autorizzazione del servizio AWS .

- [Operazioni, risorse e chiavi di condizione per Amazon Message Gateway Service](#) (`ssmmessages`).
- [Operazioni, risorse e chiavi di condizione per Amazon Message Delivery Service](#) (`ec2messages : *`)

## **ssm: \* operazioni API relative all'istanza dello spazio dei nomi**

### DescribeDocumentParameters

Systems Manager esegue questa operazione API per il rendering di nodi specifici nella console di Amazon EC2. I risultati delle operazioni `DescribeDocumentParameters` sono visualizzati nel nodo Documenti.

## DescribeInstanceProperties

Systems Manager esegue questa operazione API per il rendering di nodi specifici nella console di Amazon EC2. I risultati delle operazioni DescribeInstanceProperties sono visualizzati nel nodo Fleet Manager.

## GetCalendar

Systems Manager esegue questa operazione API per eseguire il rendering dei documenti di tipo Change Calendar nella console Change Calendar.

## GetManifest

SSM Agent esegue questa operazione API per determinare i requisiti di sistema per l'installazione o l'aggiornamento di una versione specificata di un pacchetto [AWS Systems Manager Distributor](#). Si tratta di un'operazione API obsoleta e non disponibile se lanciata dopo il 2017. Regioni AWS

## ListInstanceAssociations

SSM Agent: avvia questa operazione API per vedere se è disponibile una nuova associazione State Manager. Questa operazione API è necessaria per il funzionamento di State Manager.

## PutCalendar

Systems Manager esegue questa operazione API per aggiornare i documenti di tipo Change Calendar nella console Change Calendar.

## PutConfigurePackageResult

SSM Agent esegue questa operazione API per pubblicare le metriche relative agli errori di installazione e alla latenza per i pacchetti pubblici del distributore sull'account del proprietario del pacchetto.

## RegisterManagedInstance

SSM Agent esegue questa operazione API per i seguenti scenari:

- Per registrare un server on-premises o macchina virtuale (VM) con Systems Manager come istanza gestita utilizzando un codice di attivazione e un ID.
- Per registrare le credenziali. AWS IoT Greengrass Version 2

Questa operazione viene chiamata anche dalle istanze Amazon EC2 che eseguono SSM Agent nella versione 3.1.x o successiva.

## RequestManagedInstanceRoleToken

SSM Agent esegue questa operazione API per recuperare le credenziali temporanee per accedere al nodo gestito.

## UpdateInstanceAssociationStatus

SSM Agent: esegue questa operazione API per aggiornare un'associazione. Questa operazione API è necessaria per il funzionamento di State Manager.

## UpdateInstanceInformation

SSM Agent chiama il servizio Systems Manager in cloud ogni cinque minuti per fornire le informazioni di heartbeat. Questa chiamata è necessaria per mantenere l'heartbeat con l'agente in modo che il servizio sappia che l'agente funziona correttamente.

## UpdateManagedInstancePublicKey

SSM Agent esegue questa operazione API per fornire la chiave pubblica dopo aver ruotato la coppia di chiavi sul nodo gestito. La chiave pubblica viene utilizzata per autenticare le richieste, firmate con la chiave privata, col fine di ottenere credenziali temporanee da Systems Manager.

## ssm:\* namespace per altre operazioni API

### ExecuteApi

Gli amministratori delegati di Systems Manager che gestiscono gli OpsItems in OpsCenter richiedono l'accesso a questa operazione API in modo da visualizzare i dettagli su OpsItems tramite diversi Account AWS. In particolare, questa API consente a un amministratore delegato di visualizzare i seguenti OpsItem dettagli in Console di gestione AWS: OpsItem descrizione, tag, CloudFormation modello, AWS Config modifiche, CloudWatch registri, allarmi ed eventi. AWS CloudTrail Per ulteriori informazioni su come utilizzare gli OpsItems negli account, consulta [\(Facoltativo\) Configurazione manuale OpsCenter per gestire centralmente OpsItems tra gli account](#). Per ulteriori informazioni sui dettagli delle risorse correlate per gli OpsItems, consulta [Aggiungere risorse correlate a un OpsItem](#).

## Riferimento: formati di stringhe di data e ora per Systems Manager

AWS Systems Manager Le operazioni API accettano filtri per limitare il numero di risultati restituiti da una richiesta. Alcune di queste operazioni API accettano filtri che richiedono una stringa formattata



per rappresentare una data e un'ora specifiche. Ad esempio, l'operazione API `DescribeSessions` accetta le chiavi `InvokedAfter` e `InvokedBefore` come alcuni dei valori validi per un oggetto `SessionFilter`. Un altro esempio è l'operazione API `DescribeAutomationExecutions`, che accetta le chiavi `StartTimeBefore` e `StartTimeAfter` come alcuni dei valori validi per un oggetto `AutomationExecutionFilter`. I valori forniti per queste chiavi durante il filtraggio delle richieste devono corrispondere allo standard ISO 8601. Per informazioni su ISO 8601, consulta [ISO 8601](#).

Queste stringhe di data e ora formattate non sono limitate ai filtri. Esistono anche operazioni API che richiedono una stringa formattata ISO 8601 per rappresentare una data e un'ora specifiche quando si fornisce un valore per un parametro di richiesta. Ad esempio, il parametro di richiesta `AtTime` per l'operazione `GetCalendarState`. Queste stringhe sono difficili da creare. Utilizzare gli esempi in questo argomento per creare stringhe di data e ora formattate da utilizzare con le operazioni API di Systems Manager.

## Formattazione di stringhe di data e ora per Systems Manager

Di seguito è riportato un esempio di una stringa di data e ora formattata secondo lo standard ISO 8601.

```
2024-05-08T15:16:43Z
```

Rappresenta l'8 maggio 2024 alle 15:16 del Tempo Coordinato Universale (UTC). La parte della data del calendario della stringa è rappresentata da un anno a quattro cifre, un mese a due cifre e un giorno a due cifre separati da trattini. Questo può essere rappresentato nel seguente formato.

```
YYYY-MM-DD
```

La parte temporale della stringa inizia con la lettera "T" come delimitatore, quindi è rappresentata da un'ora a due cifre, un minuto a due cifre e un secondo a due cifre separati da due punti. Questo può essere rappresentato nel seguente formato.

```
hh:mm:ss
```

La parte temporale della stringa termina con la lettera "Z", che indica lo standard UTC.

## Creazione di stringhe di data e ora personalizzate per Systems Manager

È possibile creare stringhe di data e ora personalizzate dal computer locale utilizzando lo strumento da riga di comando preferito. La sintassi utilizzata per creare una stringa di data e ora formattata secondo lo standard ISO 8601 varia a seconda del sistema operativo del computer locale. I seguenti sono esempi di come è possibile utilizzare i coreutils date di GNU su Linux o PowerShell su Windows per creare una stringa di data e ora in formato ISO 8601.

### coreutils

```
date '+%Y-%m-%dT%H:%M:%SZ'
```

### PowerShell

```
(Get-Date).ToString("yyyy-MM-ddTH:mm:ssZ")
```

Quando si utilizzano le operazioni API di Systems Manager, potrebbe essere necessario creare stringhe di data e ora cronologiche a scopo di reporting o risoluzione dei problemi. Di seguito sono riportati alcuni esempi di come è possibile creare e utilizzare stringhe di data e ora storiche personalizzate in formato ISO 8601 per e (). AWS Strumenti per PowerShell AWS Command Line Interface AWS CLI

### AWS CLI

- Recuperare l'ultima settimana di cronologia dei comandi per un documento SSM.

```
lastWeekStamp=$(date '+%Y-%m-%dT%H:%M:%SZ' -d '7 days ago')

docFilter='{"key":"DocumentName","value":"AWS-RunPatchBaseline"}'
timeFilter='{"key":"InvokedAfter","value":"\"$lastWeekStamp\""}'

commandFilters=[$docFilter,$timeFilter]

aws ssm list-commands \
 --filters $commandFilters
```

- Recuperare l'ultima settimana di cronologia di esecuzione dell'automazione.

```
lastWeekStamp=$(date '+%Y-%m-%dT%H:%M:%SZ' -d '7 days ago')
```

```
aws ssm describe-automation-executions \
 --filters Key=StartTimeAfter,Values=$lastWeekStamp
```

- Recuperare l'ultimo mese di cronologia delle sessioni.

```
lastWeekStamp=$(date '+%Y-%m-%dT%H:%M:%SZ' -d '30 days ago')

aws ssm describe-sessions \
 --state History \
 --filters key=InvokedAfter,value=$lastWeekStamp
```

## AWS Strumenti per PowerShell

- Recuperare l'ultima settimana di cronologia dei comandi per un documento SSM.

```
$lastWeekStamp = (Get-Date).AddDays(-7).ToString("yyyy-MM-ddTH:mm:ssZ")

$docFilter = @{
 Key="DocumentName"
 Value="AWS-InstallWindowsUpdates"
}
$timeFilter = @{
 Key="InvokedAfter"
 Value=$lastWeekStamp
}

$commandFilters = $docFilter,$timeFilter

Get-SSMCommand `
 -Filters $commandFilters
```

- Recuperare l'ultima settimana di cronologia di esecuzione dell'automazione.

```
$lastWeekStamp = (Get-Date).AddDays(-7).ToString("yyyy-MM-ddTH:mm:ssZ")

Get-SSMAutomationExecutionList `
 -Filters @{Key="StartTimeAfter";Values=$lastWeekStamp}
```

- Recuperare l'ultimo mese di cronologia delle sessioni.

```
$lastWeekStamp = (Get-Date).AddDays(-30).ToString("yyyy-MM-ddTH:mm:ssZ")
```

```
Get-SSMSession `
 -State History `
 -Filters @{Key="InvokedAfter";Value=$lastWeekStamp}
```

# Casi d'uso e best practice

Questo argomento elenca i casi d'uso più comuni e le best practice per AWS Systems Manager gli strumenti. Se disponibili, questa sezione include anche i collegamenti ai post sul blog e alla documentazione tecnica relativa.

Per informazioni sulla pulizia delle risorse, vedere [Eliminazione di risorse e artefatti di Systems Manager](#).

## Note

Il titolo di ogni sezione qui è un collegamento attivo alla corrispondente sezione nella documentazione tecnica.

## [Automazione](#)

- Creazione di runbook self-service per l'infrastruttura come runbook di Automazione.
- Usa Automation per semplificare la creazione Amazon Machine Images (AMIs) da Marketplace AWS o personalizzata AMIs, utilizzando documenti pubblici di Systems Manager (documenti SSM) o creando i tuoi flussi di lavoro.
- [Creazione e mantenimento di AMIs](#) utilizzando AWS-UpdateLinuxAmi e i runbook di Automazione AWS-UpdateWindowsAmi oppure attraverso l'utilizzo di documenti di automazione personalizzati appositamente creati.

## [Conformità](#)

- Come best practice di sicurezza, ti consigliamo di aggiornare il ruolo AWS Identity and Access Management (IAM) utilizzato dai nodi gestiti per limitare la capacità del nodo di utilizzare l'[PutComplianceItems](#) operazione API. Questa operazione API registra un tipo di conformità e altri dettagli relativi a questa su una risorsa designata, come un'istanza Amazon EC2 o un nodo gestito. Per ulteriori informazioni, consulta [Configurazione delle autorizzazioni per la conformità](#).

## [Inventory](#)

- Usa Inventory with AWS Config per verificare le configurazioni delle tue applicazioni nel tempo.

## [Intervallo di manutenzione](#)

- Definizione di una pianificazione per eseguire operazioni potenzialmente problematiche sui propri nodi, ad esempio l'applicazione di patch al sistema operativo (OS), gli aggiornamenti o le installazioni di software.
- Per informazioni sulle differenze tra State Manager e Maintenance Windows, strumenti di AWS Systems Manager, consulta [Scelta tra State Manager and Intervallo di manutenzione](#).

## [Parameter Store](#)

- Utilizzo di Parameter Store per gestire in modo centralizzato le impostazioni di configurazione globale.
- [Come AWS Systems Manager Parameter Store utilizza AWS KMS](#).
- [AWS Secrets Manager Segreti di riferimento Parameter Store ricavati dai parametri](#).

## [Patch Manager](#)

- Patch Manager Utilizzatelo per implementare patch su larga scala e aumentare la visibilità della conformità della flotta in tutti i nodi.
- [Integra Patch Manager con AWS Security Hub CSPM](#) per ricevere avvisi quando i nodi del tuo parco istanze non sono conformi e per monitorare lo stato di applicazione delle patch dei tuoi parchi istanze dal punto di vista della sicurezza. L'utilizzo di Security Hub CSPM è a pagamento. Per ulteriori informazioni, consulta [Prezzi](#).
- Utilizza un solo metodo alla volta per analizzare i nodi gestiti e verificare la conformità delle patch per [evitare di sovrascrivere involontariamente i dati di conformità](#).

## [Run Command](#)

- [Gestione su larga scala di istanze senza accesso SSH utilizzando Run Command di EC2](#).
- Controlla tutte le chiamate API effettuate da o per conto dell'Run Command utilizzo. AWS CloudTrail
- Quando si invia un comando utilizzando Run Command, non includere informazioni riservate formattate come testo normale, ad esempio password, dati di configurazione o altri segreti. Tutte le attività dell'API di Systems Manager nel tuo account vengono registrate in un bucket S3 per i log. AWS CloudTrail Ciò significa che qualsiasi utente con accesso a quel bucket S3 può visualizzare

i valori in testo normale di quei segreti. Per questo motivo, si consiglia vivamente di creare e utilizzare parametri SecureString per crittografare i dati sensibili utilizzati nelle operazioni di Systems Manager.

Per ulteriori informazioni, consulta [Gestire l'accesso a Parameter Store parametri che utilizzano le politiche IAM](#).

#### Note

Per impostazione predefinita, i file di log inviati CloudTrail al tuo bucket sono crittografati dalla crittografia [lato server di Amazon con chiavi di crittografia Amazon \(\)](#). [S3-managed SSE-S3](#) Per fornire un livello di sicurezza direttamente gestibile, puoi invece utilizzare la crittografia [lato server con AWS KMS—managed keys \(\)](#) per i tuoi file di registro. [SSE-KMS](#) CloudTrail

Per ulteriori informazioni, [consulta Crittografia dei file di CloudTrail registro con chiavi AWS KMS gestite \(SSE-KMS\) nella Guida per l'utente](#). AWS CloudTrail

- [Utilizzo delle funzionalità di controllo delle destinazioni e della velocità di Run Command per eseguire un comando staged](#).
- [Utilizza autorizzazioni di accesso granulari per Run Command \(e tutti gli strumenti di Systems Manager\) utilizzando le policy \(IAM\)](#). AWS Identity and Access Management

## [Session Manager](#)

- [Attività di log delle sessioni nell' Account AWS tramite AWS CloudTrail](#).
- [Registra i dati delle tue sessioni Account AWS utilizzando Amazon CloudWatch Logs o Amazon S3](#).
- [Controllo dell'accesso utente della sessione alle istanze](#).
- [Limitare l'accesso ai comandi in una sessione \(console\)](#).
- [Disattivare o attivare le autorizzazioni amministrative dell'account ssm-user](#).

## [State Manager](#)

- [Aggiornamento SSM Agent almeno una volta al mese utilizzando il documento AWS-UpdateSSMAgent preconfigurato](#).

- (Windows) Carica il modulo PowerShell o DSC su Amazon Simple Storage Service (Amazon S3) e utilizzalo. `AWS-InstallPowerShellModule`
- Utilizzo dei tag per creare gruppi di applicazioni per i propri nodi. Indirizzamento delle istanze tramite l'utilizzo del parametro `Targets` invece dell'indicazione degli ID di nodo specifici.
- [Risoluzione automatica dei risultati generati da Amazon Inspector utilizzando Systems Manager.](#)
- [Utilizzo di un repository di configurazione centralizzato per tutti i documenti e condivisione dei documenti all'interno dell'organizzazione.](#)
- Per ulteriori informazioni sulla differenza tra State Manager e Maintenance Windows, consulta [Scelta tra State Manager and Intervallo di manutenzione.](#)

### Nodi gestiti

- Systems Manager richiede riferimenti temporali precisi per eseguire le operazioni. Se la data e l'ora del nodo non sono impostate correttamente, tali informazioni potrebbero non corrispondere alla data di firma delle richieste API. Ciò potrebbe portare a errori o funzionalità incomplete. Ad esempio, nodi con le impostazioni di tempo errate non saranno inclusi nell'elenco dei nodi gestiti.

Per informazioni sull'impostazione del tempo sui nodi, consulta [Impostazione dell'orario di un'istanza in Amazon EC2.](#)

- Nei nodi gestiti da Linux, [verifica la firma di SSM Agent.](#)

### Ulteriori informazioni

- [Le migliori pratiche di sicurezza per Systems Manager](#)

## Eliminazione di risorse e artefatti di Systems Manager

Ti consigliamo di eliminare le risorse e gli artefatti di Systems Manager che non ti servono più. La tabella seguente elenca ogni strumento o artefatto di Systems Manager con un collegamento a ulteriori informazioni sull'eliminazione di tali risorse.

Capacità o artefatto	Informazioni
Application Manager	Non è possibile eliminare un'applicazione in Application Manager. Tuttavia, puoi rimuovere un'applicazione dal servizio eliminando i <a href="#">tag</a> ,



Capacità o artefatto	Informazioni
	i gruppi <a href="#">di</a> risorse o gli <a href="#">AWS CloudFormation stack</a> sottostanti.
Automazione	Se si creano AWS risorse utilizzando Systems Manager Automation, è necessario eliminare manualmente tali risorse utilizzando il corrispondente. Console di gestione AWS Se è stato creato un runbook personalizzato, è possibile eliminare il documento SSM sottostante. Per ulteriori informazioni, consulta <a href="#">Eliminazione di documenti SSM personalizzati</a> .
Change Calendar	È possibile eliminare un change calendar e un evento del change calendar. Per ulteriori informazioni, consulta <a href="#">Eliminazione di un calendario delle modifiche</a> e <a href="#">Eliminazione di un Modifica calendario evento</a> .
Change Manager	È possibile eliminare un modello di modifica. Per ulteriori informazioni, consulta <a href="#">Eliminazione di modelli di modifica</a> .
Conformità	Systems Manager Compliance visualizza automaticamente i dati di conformità riguardanti Patch Manager e le associazioni State Manager. Non è possibile eliminare questi dati. Se hai configurato una sincronizzazione dei dati delle risorse per centralizzare i dati di conformità in un bucket S3, è possibile eliminare la sincronizzazione. Per ulteriori informazioni, consulta <a href="#">Eliminazione di una sincronizzazione dei dati delle risorse per Compliance</a> .
Distributor	È possibile eliminare i pacchetti in Distributor. Per ulteriori informazioni, consulta <a href="#">Eliminare un Distributor package</a> .

Capacità o artefatto	Informazioni
Explorer	<p>È possibile disconnettersi dalle fonti da cui viene effettuata la Explorer raccolta OpsData. Per ulteriori informazioni, consulta <a href="#">Modifica delle origini dei dati in Systems Manager Explorer</a>.</p> <p>Puoi anche eliminare la sincronizzazione dei dati di una risorsa utilizzata Explorer per aggregare OpsData e OpsItems da più account Regioni AWS and a un singolo bucket Amazon Simple Storage Service (Amazon S3). Per ulteriori informazioni, consulta <a href="#">Cancellazione della Sincronizzazione dei dati delle risorse di Systems Manager Explorer</a>. Per informazioni sull'eliminazione di un bucket S3, consulta la pagina <a href="#">Eliminazione di un bucket</a> nella Guida per gli sviluppatori di Amazon Simple Email Service.</p>
Fleet Manager	<p>Non è possibile eliminare un nodo gestito utilizzando Fleet Manager. Devi usare Amazon Elastic Compute Cloud (Amazon EC2). Per ulteriori informazioni, consulta <a href="#">Termina la tua istanza (Linux)</a> e <a href="#">Termina la tua istanza (Windows)</a>.</p>

Capacità o artefatto	Informazioni
Inventory	<p>È possibile interrompere la raccolta dei dati di Inventario eliminando le associazioni State Manager che definiscono la pianificazione e le risorse da cui raccogliere i metadati. Per ulteriori informazioni, consulta <a href="#">Interruzione della raccolta dati ed eliminazione dei dati di inventario</a>.</p> <p>Se non desideri più utilizzare AWS Systems Manager Inventory per visualizzare i metadati sulle tue AWS risorse, ti consigliamo anche di eliminare le sincronizzazioni dei dati delle risorse utilizzate per la raccolta dei dati di inventario. Per ulteriori informazioni, consulta <a href="#">Eliminazione di un Resource Data Sync di Inventory</a>.</p>
Maintenance Windows	<p>È possibile eliminare una finestra di manutenzione, la destinazione di una finestra di manutenzione e l'attività di una finestra di manutenzione. Per ulteriori informazioni, consulta <a href="#">Aggiorna o elimina le risorse della finestra di manutenzione utilizzando la console</a>.</p>
OpsCenter	<p>Puoi eliminare una persona OpsItem chiamando l'operazione <a href="#">Delete OpsItem</a> API utilizzando o l' AWS Command Line Interface SDK. AWS Non è possibile eliminare un OpsItem nella Console di gestione AWS. Per ulteriori informazioni, consulta <a href="#">Elimina OpsItems</a>.</p>
Parameter Store	<p>È possibile eliminare un parametro che hai creato. Per ulteriori informazioni, consulta <a href="#">Eliminazione dei parametri da Parameter Store</a>.</p>

Capacità o artefatto	Informazioni
Patch Manager	È possibile eliminare una baseline delle patch personalizzata. Per ulteriori informazioni, consulta <a href="#">Aggiornamento o eliminazione di una baseline delle patch personalizzata</a> .
Configurazione rapida	È possibile eliminare le associazioni create dalla funzione Configurazione rapida. Le associazioni vengono memorizzate ed elaborate da State Manager. Per ulteriori informazioni, consulta <a href="#">Eliminazione di associazioni</a> .
Run Command	Al termine dell'elaborazione di un comando, le informazioni su di esso vengono memorizzate nella scheda Cronologia del comando. Non è possibile eliminare informazioni dalla scheda Cronologia del comando.
Automazione	Al termine dell'elaborazione di un'automazione, le relative informazioni vengono memorizzate nella scheda Esecuzioni. Non è possibile eliminare informazioni dalla scheda Esecuzioni.
Service-linked ruolo	Systems Manager crea automaticamente ruoli collegati al servizio <a href="#">per alcuni strumenti</a> . È possibile eliminare questi ruoli. Per ulteriori informazioni, consulta <a href="#">Eliminazione del ruolo collegato al servizio per AWSServiceRoleForAmazonSSM Systems Manager</a> .
Session Manager	Session Manager non conserva i dati sulle risorse dopo aver terminato una sessione. Per terminare una sessione, consulta <a href="#">Terminare una sessione</a> .

Capacità o artefatto	Informazioni
SSM Agent	<p>È possibile disinstallare manualmente SSM Agent dai nodi. Per ulteriori informazioni, consulta i seguenti argomenti.</p> <ul style="list-style-type: none"> <li>Linux: <a href="#">Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per Linux</a></li> <li>macOS: <a href="#">Installazione e disinstallazione manuale di SSM Agent su istanze EC2 per macOS</a></li> <li>Windows Server: Apri il pannello di controllo e quindi scegli <b>Add/remove</b> i programmi.</li> </ul>
State Manager	<p>È possibile eliminare un'associazione. Per ulteriori informazioni, consulta <a href="#">Eliminazione di associazioni</a>.</p>
Servizio documenti di Systems Manager	<p>Non puoi eliminare i runbook forniti da AWS o Supporto AWS, ma puoi eliminare i runbook personalizzati. Per ulteriori informazioni, consulta <a href="#">Eliminazione di documenti SSM personalizzati</a>.</p>

## Scelta tra State Manager and Intervallo di manutenzione

State Manager e Maintenance Windows, entrambi gli strumenti AWS Systems Manager, possono eseguire alcuni tipi di aggiornamenti simili sui nodi gestiti. La scelta dipende dalla necessità di automatizzare la conformità del sistema o di eseguire attività ad alta priorità e sensibili al tempo durante i periodi specificati.

### State Manager and Intervallo di manutenzione: Casi d'uso principali

State Manager imposta e mantiene la configurazione dello stato mirata per i nodi e AWS le risorse gestiti all'interno del tuo Account AWS. È possibile definire combinazioni di configurazioni e destinazioni come oggetti di associazione. Usalo State Manager se desideri mantenere uno stato

coerente in tutti i nodi gestiti, utilizzare Amazon EC2 Auto Scaling per generare nuovi nodi o avere rigidi requisiti di reporting di conformità.

I principali casi d'uso per State Manager sono i seguenti:

- **Scenari Auto Scaling:** State Manager è in grado di monitorare tutti i nuovi nodi avviati all'interno di un account manualmente o tramite i gruppi Auto Scaling. Se nell'account sono presenti associazioni destinate al nuovo nodo (tramite tag o tutti i nodi), tale associazione viene applicata automaticamente al nuovo nodo.
- **Report di conformità:** State Manager può favorire la creazione di report sulla conformità degli stati desiderati per le risorse nell'account.
- **Supporto di tutti i nodi:** State Manager può indirizzare tutti i nodi all'interno di un determinato account.

Una Finestra di manutenzione esegue una o più operazioni sulle risorse AWS all'interno di una determinata finestra temporale. È possibile definire una singola finestra di manutenzione con orari di inizio e fine. È possibile specificare più processi da eseguire all'interno di questa finestra di manutenzione. Usalo Maintenance Windows se le tue priorità includono l'applicazione di patch ai nodi gestiti, l'esecuzione di più tipi di attività durante un periodo di aggiornamento o il controllo del momento in cui vengono eseguiti gli aggiornamenti.

I principali casi d'uso per Maintenance Windows sono i seguenti:

- **Esecuzione di più documenti:** le finestre di manutenzione possono eseguire più processi. Ogni processo può utilizzare un tipo di documento diverso. Di conseguenza, è possibile creare flussi di lavoro complessi utilizzando processi diversi all'interno di un'unica finestra di manutenzione.
- **Applicazione di patch:** una finestra di manutenzione può fornire il supporto per l'applicazione di patch per tutti i nodi gestiti di una singola regione contrassegnati con un tag o un gruppo di risorse specifico. L'applicazione delle patch in genere comporta la rimozione dei nodi da un sistema di bilanciamento del carico, l'applicazione di patch e il ripristino della produzione dei nodi. È possibile eseguire questa operazione eseguendo una serie di attività all'interno di una finestra temporale dedicata alle patch.

#### Note

Utilizzando una finestra di manutenzione, l'operazione di applicazione di patch è limitata a una singola regione in un unico account. Utilizzando una policy di patch creata in Quick Setup, uno strumento di Systems Manager, è possibile invece configurare l'applicazione

di patch per alcuni o tutti gli account e le regioni di un'organizzazione creata in AWS Organizations. Per ulteriori informazioni, consulta [Configurazioni delle policy sulle patch in Configurazione rapida](#).

- Operazioni finestra: le finestre di manutenzione possono fare in modo che uno o più insiemi di operazioni avviino entro una finestra temporale specifica. Le finestre di manutenzione non inizieranno al di fuori di quella finestra. Le operazioni già avviate continuano fino al termine, anche se terminano al di fuori della finestra temporale.

La tabella seguente confronta le principali funzionalità di State Manager e Maintenance Windows.

Funzionalità	State Manager	Maintenance Windows
CloudFormation integration	AWS CloudFormation i modelli supportano State Manager le associazioni.	CloudFormation i modelli supportano le finestre di manutenzione, le destinazioni delle finestre e le attività delle finestre.
Conformità	Ogni State Manager associato segnala la conformità rispetto allo stato richiesto della risorsa target. È possibile utilizzare il pannello di controllo di Compliance per aggregare e visualizzare la conformità segnalata.	Non applicabile.
Integrazione di Configuration Management	State Manager supporta soluzioni di stato mirate esterne come Microsoft PowerShell Desired State Configuration (DSC), Ansible playbook e Chef ricette. È possibile utilizzare le associazioni State Manager per verificarle e il funzionamento delle	Non applicabile.

Funzionalità	State Manager	Maintenance Windows
	soluzioni di gestione della configurazione e applicare le relative modifiche alla configurazione alle istanze quando sei pronto.	
Documenti	Le configurazioni di State Manager possono essere definite come documenti di Policy (per la raccolta delle informazioni sull'inventario), runbook Automation, per risorse AWS come i bucket Amazon Simple Storage Service (Amazon S3) o i documenti di Systems Manager Command (documenti SSM) per nodi gestiti.	Le configurazioni di Maintenance Windows possono essere definite come documenti di automazione (operazioni in più fasi con flussi di lavoro di approvazione facoltativi) o documenti SSM (stato richiesto per i nodi gestiti).
Monitoraggio	State Manager monitora le modifiche nella configurazione, associazione o stato di un nodo (ad esempio, nuovi nodi in arrivo online). Quando State Manager rileva queste modifiche, l'associazione data viene riapplicata ai nodi originariamente destinati a tale associazione.	Non applicabile.



Funzionalità	State Manager	Maintenance Windows
Priorità dei processi	Non applicabile.	<p>È possibile assegnare una priorità ai processi all'interno di una finestra di manutenzione. Tutte i processi con la stessa priorità vengono eseguiti in parallelo. I processi con priorità inferiori vengono eseguiti dopo che le attività con priorità più elevate raggiungono uno stato finale. Non c'è modo di eseguire i processi in modo condizionale. Dopo che un processo con priorità superiore raggiunge lo stato finale, viene eseguito il processo con priorità successiva, indipendentemente dallo stato del processo precedente.</p>

Funzionalità	State Manager	Maintenance Windows
Controlli di sicurezza	<p>State Manager supporta due controlli di sicurezza durante l'implementazione di configurazioni in un parco istanze di grandi dimensioni. È possibile utilizzare la concorrenza massima per definire quanti nodi o risorse concorrenti devono applicare la configurazione. È possibile definire un tasso di errore massimo che può essere utilizzato per mettere in pausa State Manager se si verifica un certo numero o percentuale di errori nel parco istanze.</p>	<p>Le finestre di manutenzione supportano due controlli di sicurezza quando si implementano configurazioni in un parco istanze macchine di grandi dimensioni. È possibile utilizzare la concorrenza massima per definire quanti nodi o risorse concorrenti devono applicare la configurazione. È possibile definire un tasso di errore massimo che può essere utilizzato per sospendere le operazioni in una finestra di manutenzione se si verificano un certo numero o percentuale di errori nel parco istanze.</p>

Funzionalità	State Manager	Maintenance Windows
Pianificazione	<p>È possibile eseguire le associazioni State Manager su richiesta, a un particolare intervallo cron, a una determinata velocità, o dopo che sono state create. Ciò è utile se vuoi mantenere lo stato richiesto delle risorse in modo coerente e tempestivo.</p> <div data-bbox="592 682 1031 1717"> <p> <b>Important</b></p> <p>Le espressioni cron per le associazioni State Manager non supportano il campo dei mesi, come 03 o MAR per il mese di marzo. Se hai bisogno di aggiornamenti di configurazione mensili o trimestrali, una finestra di manutenzione può soddisfare al meglio le esigenze dell'utente. Per ulteriori informazioni, consulta <a href="#">Riferimento: espressioni Cron e della frequenza per Systems Manager</a>.</p> </div>	<p>Le finestre di manutenzione supportano diverse opzioni di pianificazione, tra cui espressioni at (ad esempio, "at(2021-07-07T13:15:30)" ), Cron e della frequenza, Cron con offset e ora di inizio e fine per quando le finestre di manutenzione dovrebbero essere eseguite e tempi di cutoff per specificare quando interrompere la programmazione entro una determinata finestra temporale.</p>

Funzionalità	State Manager	Maintenance Windows
Definizione del target	Le associazioni State Manager possono scegliere come target uno o più nodi utilizzando l'ID istanza, il tag o il gruppo di risorse. State Manager può indirizzare tutti i nodi gestiti all'interno di un determinato account.	Le finestre di manutenzione possono indirizzare uno o più nodi utilizzando ID nodo, tag o gruppi di risorse.
Processo all'interno delle finestre di manutenzione	Non applicabile.	<p>Le finestre di manutenzione possono supportare una o più processi in cui ogni processo è destinato a un runbook Automation specifico o un'azione del documento Command. Tutte i processi all'interno di una finestra di manutenzione vengono eseguite in parallelo, a meno che non siano impostate priorità diverse per processi diversi.</p> <p>Le finestre di manutenzione supportano l'esecuzione di quattro tipi di processi:</p> <ul style="list-style-type: none"> <li>• Comandi AWS Systems Manager Run Command</li> <li>• AWS Systems Manager Flussi di lavoro di automazione</li> <li>• AWS Lambda funzioni</li> <li>• AWS Step Functions compiti</li> </ul>

# Informazioni correlate

Le seguenti risorse correlate possono rivelarsi utili durante l'utilizzo di questo servizio.

## Prezzi

Alcuni strumenti di Systems Manager sono a pagamento. Per ulteriori informazioni, consulta [Prezzi di AWS Systems Manager](#).

## AWS Systems Manager libreria di documentazione

[AWS Systems Manager Documentazione](#): accedi a tutta la documentazione utente per Systems Manager AWS AppConfig, incluso Incident Manager e AWS Systems Manager per SAP.

## AWS re:Post

[AWS re:Post](#)— servizio AWS gestito di domande e risposte (Q & A) che offre risposte raccolte in crowdsourcing e esaminate da esperti alle vostre domande tecniche.

## AWS & Blog e podcast

Leggi i post del blog relativi a Systems Manager nella [Categoria strumenti di gestione AWS](#) e altri post con il tag [#Systems Manager](#).

## Service Quotas

Rivedi [Service Quotas di Systems Manager](#) nella Riferimenti generali di Amazon Web Services. Salvo dove diversamente specificato, ogni quota si applica a una singola regione in un Account AWS.

## Guida di riferimento per l'autorizzazione del servizio per Systems Manager

Nel AWS Service Authorization Reference, visualizza le informazioni sulle [azioni, le risorse e le chiavi di contesto delle condizioni](#) che puoi utilizzare nelle policy AWS Identity and Access Management (IAM) per Systems Manager.

## AWS Systems Manager Contratto sul livello di servizio

Il [AWS Systems Manager Service Level Agreement](#) (SLA) è una politica che disciplina l'uso di Systems Manager e si applica separatamente a ciascun Account AWS utente di Systems Manager.

## Ambito generale AWS risorse

Le seguenti risorse generali possono aiutarti a lavorare con AWS.

- [Corsi e workshop](#): collegamenti a corsi specialistici e basati sui ruoli, oltre a laboratori di autoapprendimento per affinare le tue abilità e acquisire esperienza pratica. AWS
- [AWS Developer Center](#): esplora i tutorial, scarica gli strumenti e scopri gli eventi per sviluppatori. AWS
- [AWS Strumenti per sviluppatori](#): collegamenti a strumenti per sviluppatori, SDK, toolkit IDE e strumenti da riga di comando per lo sviluppo e la gestione di applicazioni. AWS
- [Centro risorse introduttive](#): scopri come configurare la tua Account AWS, entrare a far parte della AWS community e lanciare la tua prima applicazione.
- [Hands-On Tutorial](#): segui i tutorial dettagliati per avviare la tua prima applicazione su. AWS
- [AWS Whitepaper](#): collegamenti a un elenco completo di AWS white paper tecnici, che trattano argomenti come architettura, sicurezza ed economia e scritti da Solutions Architects o altri esperti tecnici. AWS
- [Supporto AWS Center](#): l'hub per la creazione e la gestione dei tuoi casi. Supporto AWS Include anche collegamenti ad altre risorse utili, come forum, domande frequenti tecniche, stato di salute del servizio e AWS Trusted Advisor.
- [Supporto](#)— La pagina web principale per informazioni su Supporto un canale di supporto individuale e a risposta rapida per aiutarti a creare ed eseguire applicazioni nel cloud.
- [Contattaci](#): un punto di contatto centrale per richieste relative a fatturazione, account, eventi, uso illecito e altre questioni relative ad AWS .
- [AWS Termini del sito](#): informazioni dettagliate sul nostro copyright e marchio, sull'account, sulla licenza e sull'accesso al sito dell'utente e su altri argomenti.

# Cronologia dei documenti

La tabella seguente descrive le modifiche importanti alla documentazione rispetto all'ultima versione di AWS Systems Manager. Per ricevere notifiche sugli aggiornamenti di questa documentazione, è possibile [iscriversi a un feed RSS](#).

Modifica	Descrizione	Data
<a href="#">Linee guida IAM aggiornate per limitare l'accesso ai parametri Parameter Store</a>	<p>Ha spiegato come Parameter Store autorizza ogni operazione e di recupero dei parametri, in modo da poter scrivere policy IAM che limitino l'accesso ai parametri e ai percorsi dei parametri come previsto. Per ulteriori informazioni, consulta i seguenti argomenti:</p> <ul style="list-style-type: none"><li>• <a href="#">In che modo Parameter Store autorizza il recupero dei parametri</a></li><li>• <a href="#">Limitazione dell'accesso a parametri e percorsi specifici</a></li><li>• <a href="#">Limitazione della decrittografia dei valori dei parametri SecureString</a></li></ul>	21 settembre 2026
<a href="#">AWS Parameters and Secrets Lambda Extension supporta la fase INIT</a>	<p>L'estensione Lambda AWS Parameters and Secrets ora può essere richiamata durante la INIT fase di una funzione Lambda, oltre che durante la fase. INVOKE. La documentazione non indica più che le chiamate sono limitate alla INVOKE fase. Per ulteriori</p>	21 settembre 2026

informazioni, consulta [Utilizzo dei parametri Parameter Store nelle funzioni](#) Lambda.

[AWS Parametri e segreti aggiornati Lambda Extension ARN](#)

Sono stati aggiornati gli ARN per l'estensione Lambda AWS Parameters and Secrets alle ultime versioni disponibili per tutte le versioni supportate. Regioni AWS Per ulteriori informazioni, consulta [Utilizzo dei parametri di Parameter Store nelle funzioni Lambda](#).

21 agosto 2026

[AWS Systems ManagerApplication Managermodifica della disponibilità](#)

AWS Systems ManagerApplication Managernon è più aperto a nuovi clienti. Per funzionalità simili a AWS Systems ManagerApplication Manager, esplora le alternative [qui](#).

30 luglio 2026



[AWS Parameters and Secrets  
Lambda Extension aggiunge il  
supporto per SnapStart e per  
le istanze gestite da Lambda](#)

L'estensione Lambda AWS Parameters and Secrets ora funziona con Lambda e Lambda SnapStart Managed Instances. Per recuperare e il token di sessione per l'X-Aws-Parameters-Secrets-Token intestazione in modo affidabile in tutte le modalità di inizializzazione, utilizza la catena di provider di credenziali di un SDK anziché la variabile di ambiente. AWS\_SESSION\_TOKEN

Per ulteriori informazioni, consulta [Utilizzo dei parametri Parameter Store nelle funzioni Lambda.](#)

28 luglio 2026

[AWS Parametri e segreti  
aggiornati Lambda Extension  
ARN](#)

Sono stati aggiornati gli ARN per l'estensione Lambda AWS Parameters and Secrets alle ultime versioni disponibili per tutte le versioni supportate. Regioni AWS

Per ulteriori informazioni, consulta [Utilizzo dei parametri di Parameter Store nelle funzioni Lambda.](#)

21 luglio 2026

[L'automazione ora utilizza l'identità di esecuzione per il monitoraggio CloudWatch degli allarmi](#)

Systems Manager Automation ora utilizza l'identità di esecuzione del runbook per il monitoraggio degli CloudWatch allarmi. Non utilizza più il ruolo collegato al servizio SSM per questa operazione. Assicurati che la tua identità di esecuzione disponga delle autorizzazioni richieste. Per ulteriori informazioni, consulta [Configurazione del monitoraggio degli CloudWatch allarmi per l'automazione.](#)

8 luglio 2026

[Advanced-instances livello rimosso](#)

Il livello di istanze avanzate è stato rimosso. Non esiste più un limite di 1.000 istanze per i nodi gestiti ibridi e non è più necessario abilitare un livello a pagamento da utilizzare su macchine non EC2. Session Manager Run Command utilizza invece i prezzi Session Manager pay-as-you-go se utilizzati su nodi gestiti ibridi. Per ulteriori informazioni sui prezzi, consulta [Prezzi di AWS Systems Manager.](#)

1 luglio 2026

[AWS Systems ManagerApplication Managermodifica della disponibilità](#)

AWS Systems ManagerApplication Managernon sarà più aperto a nuovi clienti a partire dal 30 luglio 2026. Per utilizzare il servizio, iscriviti prima del 30 luglio 2026. Per funzionalità simili a AWS Systems ManagerApplication Manager, scopri di più [qui](#).

30 giugno 2026

[AWS Parametri e segreti aggiornati Lambda Extension ARN](#)

Sono stati aggiornati gli ARN per l'estensione Lambda AWS Parameters and Secrets alle ultime versioni disponibili per tutte le versioni supportate. Regioni AWS Per ulteriori informazioni, consulta [Utilizzo dei parametri di Parameter Store nelle funzioni Lambda](#).

19 giugno 2026

### [Policy gestite e aggiornate AWSQuickSetupManagedInstanceProfileExecutionPolicy](#)

Systems Manager ha aggiornato la policy gestita AWSQuickSetupManagedInstanceProfileExecutionPolicy per supportare la Quick Setup PatchPolicy migrazione dalle policy CloudFormation in linea alle policy gestite. L'aggiornamento aggiunge funzionalità di esecuzione automatizzata, tra cui il rilevamento delle istanze, gli aggiornamenti dei ruoli, l'etichettatura dei ruoli e PassRole le autorizzazioni estese a Systems Manager. Per informazioni, consulta [Aggiornamenti di Systems Manager alle policy AWS gestite.](#)

3 giugno 2026

### [Nuova politica gestita AWSQuickSetupPatchPolicyTagManagementExecutionPolicy](#)

Systems Manager ha rilasciato una nuova policy gestita AWSQuickSetupPatchPolicyTagManagementExecutionPolicy per consentire alle configurazioni delle policy di Quick Setup patch di tenere traccia delle istanze gestite tramite l'etichettatura automatica e la raccolta dell'inventario. Per informazioni, vedere [Aggiornamenti di Systems Manager alle AWS policy gestite.](#)

3 giugno 2026

[Nuova politica gestita  
AWSQuickSetupPatch  
PolicyLambdaExecutionPolicy](#)

Systems Manager ha rilasciato o una nuova policy gestita AWSQuickSetupPatch PolicyLambdaExecutionPolicy che concede le autorizzazioni per gestire le associazioni di State Manager per le operazioni di pulizia automatiche quando le configurazioni di Quick Setup vengono eliminate . Per informazioni, vedere Aggiornamenti di [Systems Manager alle politiche gestite.](#) [AWS](#)

3 giugno 2026

[AWS Parametri e segreti  
aggiornati Lambda Extension  
ARN](#)

Sono stati aggiornati gli ARN per l'estensione Lambda AWS Parameters and Secrets alle ultime versioni disponibili per tutte le versioni supportate. Regioni AWS Per ulteriori informazioni, consulta [Utilizzo dei parametri di Parameter Store nelle funzioni Lambda.](#)

14 maggio 2026

[AWS Parametri e segreti  
aggiornati Lambda Extension  
ARN](#)

Sono stati aggiornati gli ARN per l'estensione Lambda AWS Parameters and Secrets alle ultime versioni disponibili per tutte le versioni supportate. Regioni AWS Per ulteriori informazioni, consulta [Utilizzo dei parametri Parameter Store nelle funzioni](#) Lambda.

6 maggio 2026

## [Policy gestite e aggiornate AmazonSSMAutomationRole](#)

Systems Manager ha aggiornato la policy gestita AmazonSSMAutomationRole per aggiungere le `cloudformation:UntagResource` autorizzazioni `cloudformation:TagResource` e. Queste autorizzazioni consentono ai runbook di Automation che creano CloudFormation stack di aggiungere e rimuovere tag dalle risorse. Per informazioni, consulta [Aggiornamenti di Systems Manager alle AWS policy gestite.](#)

20 marzo 2026

## [Nuova sezione per il recupero programmatico degli ARN Lambda Extension più recenti](#)

L'ultimo Amazon Resource Name (ARN) per l'estensione Lambda viene pubblicato come parametro pubblico in Systems Manager Parameter Store per ciascuna architettura supportata. Puoi recuperare e l'ARN più recente a livello di codice utilizzando AWS CLI o CloudFormation per assicurarti che l'applicazione faccia sempre riferimento alla versione dell'estensione più recente senza aggiornamenti manuali. Per ulteriori informazioni, consulta [AWS Parameters and Secrets Lambda Extension ARNs.](#)

10 marzo 2026

[Policy gestite e aggiornate AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy](#)

Systems Manager ha aggiornato la policy gestita AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy per aggiungere ulteriori autorizzazioni EC2 e SSM per funzionalità di diagnosi avanzate. Per informazioni, vedere Aggiornamenti di [Systems Manager alle AWS politiche gestite.](#)

19 dicembre 2025

[Policy gestite e aggiornate AWSQuickSetupDeploymentRolePolicy](#)

Systems Manager ha aggiornato la policy gestita AWSQuickSetupDeploymentRolePolicy per aggiungere il supporto per due documenti SSM aggiuntivi: AWSQuickSetupType-ConfigureDevOpsGuru e AWSQuickSetupType-DeployConformancePack. Queste aggiunte consentono di Quick Setup implementare le configurazioni DevOps Guru e i pacchetti di conformità tramite la policy. Per informazioni, vedere Aggiornamenti di [Systems Manager alle policy gestite.](#) [AWS](#)

15 dicembre 2025

### [AWS Systems ManagerCh ange Managernon è più aperto a nuovi clienti.](#)

AWS Systems ManagerCh  
ange Managernon è più aperto  
a nuovi clienti. I clienti esistenti  
possono continuare a utilizzar  
e il servizio normalmente. Per  
ulteriori informazioni, consulta  
[AWS Systems ManagerCh  
ange Manager la modifica  
della disponibilità.](#)

7 novembre 2025

### [Nuove versioni dell'estensione Lambda AWS Parameters and Secrets](#)

Nuove versioni dell'[estensione  
Lambda di segreti e parametri  
AWS](#) sono ora disponibi  
li per tutte le Regioni e le  
architetture precedentemente  
supportate. Inoltre, ARM64  
è stato aggiunto il supporto  
per l'Mac with Apple siliconar  
chitettura per la regione Asia  
Pacifico (Nuova Zelanda) (ap-  
southeast-6).

22 ottobre 2025

### [Supporto aggiornato per Python e runtime PowerShell](#)

Abbiamo aggiornato gli elenchi  
e gli esempi «supportati»  
con i runtime ora supportat  
i ufficialmente da Systems  
Manager, che includono  
Python 3.10, Python 3.11 e  
7.4 (dotnet8). PowerShell Le  
versioni precedenti non sono  
più supportate.

16 ottobre 2025



### [Patch Manager supporto per ambienti IPv6](#)

Patch Manager ora fornisce il supporto per gli ambienti IPv6 (Internet Protocol version 6). Per informazioni, consulta [Migliorare la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager](#) e Applicando [patch a un server in un ambiente solo IPv6](#).

15 ottobre 2025

### [AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025.](#)

AWS Systems Manager Change Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzarlo Change Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta [AWS Systems Manager Change Manager la modifica della disponibilità](#).

7 ottobre 2025

### [Nuove versioni dell'estensione Lambda AWS Parameters and Secrets](#)

Nuove versioni dell'[estensione Lambda di segreti e parametri AWS](#) sono ora disponibili per tutte le Regioni e le architetture precedentemente supportate. Inoltre, è stato aggiunto il supporto per la Regione Asia Pacifico (Nuova Zelanda) (ap-southeast-6), solo per le architetture `x86_64` e `x86`.

30 settembre 2025

[Policy gestite e aggiornate  
AWSSystemsManagerJ  
ustInTimeAccessTokenPolicy](#)

Systems Manager ha aggiornato la policy gestita `AWSSystemsManagerJustInTimeAccessTokenPolicy` per fornire le autorizzazioni dei canali di dati per la gestione delle sessioni. Per informazioni, vedere [Aggiornamenti di Systems Manager alle politiche AWS gestite](#).

25 settembre 2025

[Politica gestita aggiornata: AWSQuickSetupStart  
StopInstancesExecutionPolicy](#)

Systems Manager ha aggiornato la politica gestita `AWSQuickSetupStartStopInstancesExecutionPolicy` per perfezionare le autorizzazioni per la configurazione dello Quick Setup scheduler. La policy ora fornisce autorizzazioni più specifiche per l'avvio e l'arresto delle istanze Amazon EC2, l'accesso ai calendari delle modifiche e l'esecuzione di documenti di automazione con condizioni di sicurezza avanzate. Per informazioni, consulta gli aggiornamenti di [Systems Manager alle policy gestite. AWS](#)

12 settembre 2025

[Politica gestita aggiornata: AWSQuickSetupStartSSMAssociationsExecutionPolicy](#)

12 settembre 2025

Systems Manager ha aggiornato la policy gestita `AWSQuickSetupStartSSMAssociationsExecutionPolicy` per modificare il documento di automazione da `AWSQuickSetupType-StartSSMAssociations` a `AWSQuickSetupType-Scheduler-ChangeCalendarState`. Questo aggiornamento modifica lo scopo della politica, dall'avvio delle associazioni SSM alla gestione delle modifiche degli stati del calendario per le operazioni pianificate. Per informazioni, vedere [Aggiornamenti di Systems Manager alle policy AWS gestite](#).

Tre politiche gestite aggiornate

Systems Manager ha aggiornato tre politiche gestite per consentire Quick Setup di avviare le esecuzioni di automazione su risorse aggiuntive di Systems Manager: `AWSQuickSetupSSMLifecycleManagementExecutionPolicy`, `AWSQuickSetupPatchPolicyPermissionsBoundary`, e `AWSQuickSetupManagedInstanceProfileExecutionPolicy`. Per informazioni, vedere Aggiornamenti [di Systems Manager alle politiche AWS gestite](#).

12 settembre 2025

Politica gestita aggiornata: `AmazonSSMAutomationRole`

Systems Manager ha aggiornato la policy `AmazonSSMAutomationRole` gestita per aggiungere l'autorizzazione `ssmmessages:OpenDataChannel`. Questa autorizzazione consente ai runbook di Automazione di stabilire canali di comunicazione per le operazioni basate sulla sessione. Per informazioni, vedere Aggiornamenti [di Systems Manager alle politiche AWS gestite](#).

11 settembre 2025

[Nuovo argomento: Comprendere l'ibernazione dell'SSM Agent](#)

Questo nuovo argomento spiega che l'ibernazione è una modalità operativa che si verifica quando l'agente non riesce a mantenere una comunicazione corretta con il servizio di Systems Manager. Durante l'ibernazione, l'agente riduce la frequenza di comunicazione ed entra in uno stato di stand-by. Per informazioni dettagliate sull'ibernazione dell'agente, consulta [Comprendere l'ibernazione dell'SSM Agent](#).

2 settembre 2025

[Politica gestita aggiornata: AWSSystemsManagerJ ustInTimeAccessServicePolicy](#)

Systems Manager ha aggiornato la policy gestita `AWSSystemsManagerJ ustInTimeAccessServicePolicy` per aggiungere le autorizzazioni di etichetta di esecuzione dell'automazione, consentendo ai clienti di ridurre le autorizzazioni degli operatori a tag specifici. Per informazioni, vedere Aggiornamenti [di Systems Manager alle politiche AWS gestite](#).

25 agosto 2025

[Descrizioni aggiornate per le schede sui dettagli dei nodi \(console unificata\)](#)

Abbiamo aggiornato le descrizioni dei contenuti nelle schede della pagina dei dettagli del nodo nella console unificata (schede: Tag, Inventario, Associazione, Patch, Conformità della configurazione). Per ulteriori informazioni, consulta [Cos'è la console unificata?](#).

20 agosto 2025

[Nuovo argomento sulle best practice di sicurezza per l'installazione dell'SSM Agent](#)

Il nuovo argomento [sulle best practice di installazione di SSM Agent](#) spiega l'importanza di utilizzare il metodo corretto per installare l'agente in base al tipo di macchina, all'istanza EC2 o alla macchina attivata in modo ibrido.

18 agosto 2025

[Nuove funzionalità di Automazione basate su console](#)

## AWS Systems Manager

14 agosto 2025

L'automazione ha introdotto nuove funzionalità di esecuzione e avanzate con riprova automatica per le operazioni limitate e la possibilità di rieseguire le esecuzioni di automazione. La funzione di ripetere il tentativo di limitazione (della larghezza di banda della rete) automatica garantisce un'esecuzione affidabile dell'automazione su larga scala tramite la ripetizione automatica delle chiamate API che riscontra i limiti di limitazione (della larghezza di banda della rete), con limiti di tempo configurabili fino a 3.600 secondi. (Tutte le operazioni di Automazione tranne la ripetizione del tentativo di limitazione (della larghezza di banda della rete) automatico di [aws:executeScript](#). Inoltre, ora puoi rieseguire facilmente le esecuzioni di automazione completate con parametri identici o modificati, semplificando le operazioni ripetute e riducendo il sovraccarico operativo senza ricreare manualmente le configurazioni. Per ulteriori informazioni, consulta i seguenti argomenti:

- [Configurazione dei tentativi automatici per le operazioni di limitazione \(della larghezza di banda della rete\)](#)
- [Nuove esecuzioni delle esecuzioni di automazione](#)
- [Esecuzione di automazioni in più account e Regioni AWS](#)

### [Aggiornamenti per la policy AWSQuickSetupDeploymentRolePolicy gestita](#)

Systems Manager ha aggiornato la policy AWSQuickSetupDeploymentRolePolicy gestita per concedere autorizzazioni relative all'associazione a runbook di AWSQuickSetupType-\*. Automazione aggiuntivi e per consentire a Quick Setup di collegare e scollegare policy IAM aggiuntive. Inoltre, abbiamo aggiornato la documentazione per la AWSQuickSetupDeploymentRolePolicy per fornire descrizioni più dettagliate delle autorizzazioni concesse per le operazioni di gestione della configurazione di Quick Setup. Per informazioni, vedere [Aggiornamenti di Systems Manager alle politiche AWS gestite](#).

12 agosto 2025



[Nuovo argomento: Perimetri dei dati in AWS Systems Manager](#)

È possibile configurare le politiche perimetrali dei dati per le risorse di AWS proprietà del servizio a cui accede Systems Manager. [Il perimetro dei dati in AWS Systems Manager](#) descrive lo scopo del bucket ssm-document-categories- *region* S3 gestito da Systems Manager. Questo bucket contiene metadati sulle categorie di documenti che aiutano a organizzare e classificare i documenti SSM nella console.

12 agosto 2025

[Nuova politica gestita per lo scheduler: Quick Setup AWSQuickSetupStartStopInstancesExecutionPolicy](#)

Systems Manager ha rilasciato o una nuova policy gestita, AWSQuickSetupStartStopInstancesExecutionPolicy , che fornisce le autorizzazioni per la Quick Setup per avviare e arrestare le istanze Amazon EC2 in base a una pianificazione. Per informazioni, vedere Aggiornamenti [di Systems Manager alle politiche AWS](#) gestite.

12 agosto 2025

[Nuova politica AWS gestita per Quick Setup: AWSQuickSetupStartSSMAssociationsExecutionPolicy](#)

Systems Manager ha rilasciato una nuova policy AWSQuickSetupStartSSMAssociationsExecutionPolicy gestita che consente a Quick Setup di eseguire il runbook di Automazione. Per informazioni, vedere Aggiornamenti [di Systems Manager alle politiche AWS gestite](#). 12 agosto 2025

[Nuove linee guida per la risoluzione dei problemi di dipendenza del blocco dei pacchetti zypper sui nodi gestiti SLES](#)

Aggiunta una guida completa alla risoluzione dei problemi per risolvere gli errori di dipendenza dal blocco del pacchetto zypper che si verificano durante le operazioni Patch Manager Install sui nodi gestiti di SUSE Linux Enterprise Server. La nuova sezione [Problema: errori di dipendenza dal blocco dei pacchetti Zypper sui nodi gestiti di SLES](#) fornisce informazioni dettagliate sull'identificazione, la diagnosi e la risoluzione dei conflitti di blocco dei pacchetti che impediscono la corretta installazione delle patch. 28 luglio 2025

[Linee guida avanzate per la risoluzione dei problemi relativi alle associazioni di inventario ignorate](#)

È stata aggiornata la sezione relativa alla risoluzione dei problemi [ignorati](#) per fornire una guida completa sulla gestione prioritaria delle associazioni di inventario. La documentazione avanzata ora include informazioni dettagliate sulle associazioni di inventario di Quick Setup, sugli scenari di targeting espliciti e sulle procedure di risoluzione dettagliate per la gestione delle associazioni di inventario in conflitto.

24 luglio 2025

I miglioramenti includono:

- Spiegazione dell'ordine di priorità delle associazioni di inventario (Quick Setup, associazioni esplicite e globali)
- Scenari comuni con esempi specifici e risultati attesi
- Passaggi di risoluzione dettagliati per rimuovere le configurazioni di Quick Setup, quando si utilizzano associazioni di inventario personalizzate
- Note importanti sul comportamento di raccolta dei dati e sulla precedenza delle associazioni

[Politica gestita aggiornata: AWS-SSM-RemediationAutomation-ExecutionRolePolicy](#)

16 luglio 2025

Systems Manager ha aggiornato la policy gestita AWS-SSM-RemediationAutomation-ExecutionRolePolicy per migliorare il livello di sicurezza dell'StartAutomationExecution API ssm: richiedendo le autorizzazioni per i tipi di risorse «documento» e «esecuzione automatica». Questo aggiornamento è stato apportato per migliorare il livello di sicurezza dell'StartAutomationExecution API ssm: richiedendo le autorizzazioni per i tipi di risorse «documento» e «esecuzione automatica», fornendo autorizzazioni più complete e dettagliate per l'esecuzione dell'automazione delle riparazioni. Per informazioni, [consulta Aggiornamenti di Systems Manager alle policy gestite. AWS](#)

[Politica gestita aggiornata: AWS-SSM-RemediationAutomation-AdministrationRolePolicy](#)

Systems Manager ha aggiornato la policy gestita AWS-SSM-RemediationAutomation-AdministrationRolePolicy per supportare il miglioramento delle autorizzazioni API per le operazioni di automazione delle riparazioni. La policy aggiornata migliora le autorizzazioni per l'esecuzione delle attività definite nei documenti di Automazione, con controlli di sicurezza e modelli di accesso alle risorse migliorati per i flussi di lavoro di riparazione. Per informazioni, vedere Aggiornamenti [di Systems Manager alle politiche AWS gestite](#).

16 luglio 2025

[Politica gestita aggiornata: AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy](#)

Systems Manager ha aggiornato la policy AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy gestita per fornire autorizzazioni più dettagliate e accurate per l'esecuzione automatizzata della diagnosi. La policy aggiornata include descrizioni migliorate per l'accesso alle risorse di Amazon EC2 e Amazon VPC, autorizzazioni di automazione SSM più specifiche e descrizioni delle autorizzazioni migliorate AWS KMS e IAM con adeguate restrizioni sulle risorse. Per informazioni, consulta gli aggiornamenti di [Systems Manager alle policy gestite. AWS](#)

16 luglio 2025

[Politica gestita aggiornata: AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy](#)

Systems Manager ha aggiornato la policy AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy gestita per includere autorizzazioni e condizioni di sicurezza più specifiche per le operazioni di automazione della diagnosi. La policy aggiornata fornisce controlli di sicurezza avanzati per l'utilizzo delle AWS KMS chiavi, l'accesso ai bucket Amazon S3 e i presupposti di ruolo, con condizioni basate sulle risorse e restrizioni a livello di account più rigorose. Per informazioni, consulta la sezione Aggiornamenti di Systems Manager alle policy gestite. [AWS](#)

16 luglio 2025

[È stata aggiunta la documentazione per le policy AmazonSSMAutomationRole gestite](#)

Systems Manager ha aggiornato la documentazione per la policy AmazonSSMAutomationRole gestita esistente. Per informazioni, vedere Aggiornamenti [di Systems Manager alle politiche AWS gestite](#).

15 luglio 2025

## [Sicurezza avanzata per i documenti SSM con interpolazione delle variabili di ambiente](#)

14 luglio 2025

AWS Systems Manager I documenti di comando ora supportano l'interpolazione delle variabili di ambiente durante l'elaborazione dei parametri. Questa funzionalità, disponibile nella versione 2.2 dello schema e nella versione SSM Agent 3.3.2746.0 o successiva, aiuta a prevenire gli attacchi di iniezione di comandi trattando i valori dei parametri come stringhe letterali invece di comandi potenzialmente eseguibili. Se impostato su ENV\_VAR, l'agente crea una variabile di ambiente denominata nel formato SSM\_*parameter-name* che contiene il valore del parametro.

Per ulteriori informazioni, consulta i seguenti argomenti:

- [Componenti del documento](#)
- [Esempi di gestione sicura dei parametri](#)
- [Elementi di dati e parametri](#)
- [Documentazione di riferimento del plugin per i documenti di comando](#)



## [Explorersincronizzazione dei dati delle risorse disponibile in quattro modalità opt-in Regioni AWS](#)

Per impostazione predefinita, Explorer le sincronizzazioni dei dati delle risorse tra account/cross regioni non supportano l'aggregazione dei dati nelle regioni con consenso esplicito. È stato aggiunto il supporto per le seguenti Regioni con consenso esplicito il 30 giugno 2025.

- Europa (Milano)
- Africa (Città del Capo)
- Medio Oriente (Bahrein)
- Asia Pacifico (Hong Kong)

Tieni presente che non puoi utilizzare un account amministratore delegato per creare una sincronizzazione dei dati delle risorse nelle Regioni che hanno aderito. È necessario utilizzare un account di gestione. AWS Organizations Per ulteriori informazioni, consulta [Informazioni sulle sincronizzazioni dei dati delle risorse di più account e Regioni](#).

30 giugno 2025

### [Nuove versioni dell'estensione Lambda AWS Parameters and Secrets](#)

Nuove versioni delle [estensioni Lambda di segreti e parametri AWS](#) sono ora disponibili. È stato inoltre aggiunto il supporto per la Regione Asia Pacifico (Taipei) (ap-east-2).

26 giugno 2025

### [Nuovo argomento: Change Calendar integrazione con Amazon EventBridge](#)

L'argomento [Change Calendar integrazione con Amazon EventBridge](#) fornisce informazioni su questa integrazione nelle seguenti categorie:

25 giugno 2025

- Tempistica degli eventi e affidabilità
- Modifiche agli eventi e considerazioni sulla tempistica
- Eventi adiacenti e sovrapposti
- Best practice

### [Aggiornamento del supporto di runtime per l'operazione di Automazione 'aws:executeScript'](#)

Il Runtime parametro nell'azione di automazione [AWS:ExecuteScript](#) ora supporta gli script PowerShell 7.4 (. dotnet8

24 giugno 2025

[SSM Agent e Patch Manager ora supportano RHEL 10 e Ubuntu Server 25.04](#)

23 giugno 2025

Ora puoi gestire le macchine Red Hat Enterprise Linux 10 e Ubuntu Server 25.04 con Systems Manager, inclusa l'applicazione di patch ai nodi gestiti tramite Patch Manager. Per gli elenchi completi delle versioni e sistemi operativi supportati, consulta quanto segue:

- [Sistemi operativi supportati per Systems Manager](#)
- [Sistemi operativi supportati per Patch Manager](#)

## [Aggiornamenti agli argomenti relativi all'accesso ai nodi just-in-time](#)

17 giugno 2025

Abbiamo apportato i seguenti aggiornamenti al contenuto del capitolo sull'accesso ai [Just-in-time nodi tramite Systems Manager](#):

- Chiarimenti sul supporto di autenticazione per l'accesso ai nodi just-in-time. Per informazioni, consulta [Configurazione dell'accesso just-in-time con Systems Manager](#)
- È stato chiarito il requisito di etichettare le AWS KMS chiavi utilizzate per la Session Manager crittografia e la registrazione RDP nell'accesso just-in-time al nodo con la chiave SystemsManagerJustInTimeNodeAccessManaged del tag e il valore del tag. true Per informazioni, consulta [Aggiornare le preferenze della sessione di accesso al nodo just-in-time](#) e [Configurazione della crittografia dei bucket S3 per le registrazioni RDP](#).
- [Notifiche di configurazione aggiornate per le richieste di accesso just-in-time](#) con dettagli di configurazione aggiuntivi.

### [Registrazione RDP migliorata per l'accesso ai nodi just-in-time](#)

AWS Systems Manager  
L'accesso ai nodi just-in-time fornisce ora informazioni aggiuntive sulle configurazioni di registrazione RDP. Quando si utilizza AWS KMS la crittografia sui bucket S3 in cui sono archiviate le registrazioni, è necessario fornire l'accesso alla chiave KMS utilizzata per la crittografia del bucket all'entità del servizio. `ssm-guiconnect` Questa versione introduce anche un nuovo stato di registrazione, `ProcessingError`, che indica errori intermedi durante l'elaborazione video che potrebbero essere dovuti a errori di dipendenza dal servizio o ad autorizzazioni mancanti. Per ulteriori informazioni, consulta [Registrazione di connessioni RDP](#).

13 giugno 2025

### [Informazioni aggiornate sulla selezione e l'installazione delle patch in Patch Manager](#)

Sono state aggiunte informazioni per spiegare come Patch Manager gestisce i pacchetti obsoleti durante la selezione e l'installazione delle patch. Per ulteriori informazioni, consulta [Come vengono selezionate le patch di sicurezza](#) e [Come vengono installate le patch](#).

12 giugno 2025

### [Politica gestita aggiornata per Quick Setup: AWSQuickSetupDeploymentRolePolicy](#)

Systems Manager ha aggiornato la policy gestita `AWSQuickSetupDeploymentRolePolicy` in modo che Quick Setup possa creare associazioni utilizzando questa policy gestita invece delle policy in linea. Per informazioni, vedere Aggiornamenti [di Systems Manager alle politiche AWS gestite](#).

10 giugno 2025

### [Introduzione estesa a Patch Manager](#)

Per una migliore presentazione di Patch Manager ai potenziali clienti e utenti, abbiamo aggiunto le seguenti tre sezioni al capitolo su Patch Manager:

21 maggio 2025

- [Quali sono i vantaggi di Patch Manager per la mia organizzazione?](#)
- [A chi è consigliato l'uso di Patch Manager?](#)
- [Quali sono le funzionalità principali di Patch Manager?](#)

[Politica gestita aggiornata per Quick Setup: AWSQuickSetupSSMDeploymentRolePolicy](#)

Systems Manager ha aggiornato la policy gestita `AWSQuickSetupSSMDeploymentRolePolicy` per fornire le autorizzazioni per etichettare i ruoli IAM e le risorse Lambda create per la console unificata. Per informazioni, vedere [Aggiornamenti di Systems Manager alle politiche AWS gestite](#).

07 maggio 2025

[Opzioni di configurazione della funzionalità per la console unificata](#)

Systems Manager ora offre opzioni di configurazione delle funzionalità durante la configurazione della console unificata. Queste configurazioni di funzionalità consentono di scegliere se configurare la configurazione DHMC (Default Host Management Configuration), la raccolta dei metadati dell'inventario e gli aggiornamenti dell'SSM Agent automatici. Per ulteriori informazioni, consulta [Configurazione della console unificata di Systems Manager per un'organizzazione](#) e [Configurazione della console unificata di Systems Manager per un singolo account e una singola Regione](#).

07 maggio 2025

[Politica gestita aggiornata per Quick Setup: AWS Systems Manager JustInTimeNodeAccessRolePropagationPolicy](#)

Systems Manager ha aggiornato la policy gestita `AWSManagedJustInTimeNodeAccessRolePropagationPolicy` per fornire le autorizzazioni per contrassegnare una risorsa condivisa AWS Resource Access Manager per l'accesso immediato ai nodi. Per informazioni, vedere Aggiornamenti di [Systems Manager alle AWS politiche gestite](#).

29 aprile 2025

[Politica gestita aggiornata per Quick Setup: AWS QuickSetupManageJITNAResourcesExecutionPolicy](#)

Systems Manager ha aggiornato la policy gestita `AWSQuickSetupManageJITNAResourcesExecutionPolicy` per fornire le autorizzazioni per etichettare i ruoli IAM creati per l'accesso ai nodi just-in-time. Per informazioni, vedere Aggiornamenti [di Systems Manager alle politiche AWS gestite](#).

29 aprile 2025



## [Systems Manager introduce l'accesso ai nodi just-in-time](#)

AWS Systems Manager ora supporta un metodo di accesso just-in-time per la connessione ai nodi gestiti. Questo nuovo metodo di connessione ai nodi gestiti aiuta a migliorare la sicurezza dei nodi fornendo un accesso temporaneo e limitato ai nodi solo quando necessari o, eliminando la necessità di autorizzazioni di lunga durata. Inoltre, Systems Manager fornisce la registrazione delle sessioni RDP ai Windows Server nodi per aiutarvi a soddisfare i requisiti di conformità, eseguire l'analisi delle cause principali e altro ancora. Per ulteriori informazioni, vedere Accesso ai [Just-in-time nodi tramite Systems Manager](#).

29 aprile 2025

## [Nuove policy gestite per l'accesso ai nodi just-in-time](#)

Systems Manager ha rilasciato o diverse nuove policy gestite per supportare l'accesso ai nodi just-in-time. Per informazioni, vedere Aggiornamenti [di Systems Manager alle policy AWS gestite](#).

29 aprile 2025

## [Nuove versioni dell'estensione Lambda AWS Parameters and Secrets](#)

Nuove versioni delle [estensioni Lambda di segreti e parametri AWS](#) sono ora disponibili.

23 aprile 2025

### [Nuovo argomento: "In cosa consiste la conformità in Patch Manager?"](#)

La conformità delle patch per i nodi gestiti del parco istanze non è definita da AWS né da altre terze parti. Il nuovo argomento [In cosa consiste la conformità in Patch Manager?](#) chiarisce che la conformità delle patch per un nodo gestito da Systems Manager significa che sul nodo sono state installate tutte le patch che soddisfano i criteri di approvazione specificati nella baseline delle patch associata. La conformità è definita dall'utente, nelle regole configurate in una baseline di patch o in una baseline di patch predefinita fornita da te scelta per le AWS operazioni di patching.

11 aprile 2025

### [Nuove versioni dell'estensione Lambda AWS Parameters and Secrets](#)

Nuove versioni dell'[estensione e Lambda di AWS Parameters and Secrets](#) sono ora disponibili. Inoltre, è stato aggiunto il supporto per l'estensione per le seguenti Regioni:

03 aprile 2025

- Asia Pacifico (Thailandia) (ap-southeast-2)
- Messico (centrale) (mx-central-1)

[Nuovo argomento: Configurazione delle autorizzazioni per la conformità](#)

Come best practice di sicurezza, ti consigliamo di aggiornare il ruolo AWS Identity and Access Management (IAM) utilizzato dai nodi gestiti per limitare la capacità del nodo di utilizzare l'azione [PutComplianceItems](#) API. Quest'operazione dell'API registra un tipo di conformità e altri dettagli di conformità su una risorsa designata, come un'istanza Amazon EC2 o un nodo gestito. Per ulteriori informazioni, consulta [Configurazione delle autorizzazioni per la Conformità](#).

11 marzo 2025

[Argomento aggiornato: Revisione degli approfondimenti sui nodi](#)

Nella [console unificata](#) per Systems Manager, la pagina Rivedi approfondimenti sui nodi riporta il numero di istanze EC2 gestite e non gestite nell'organizzazione o nell'account. Abbiamo chiarito che Systems Manager include un'istanza EC2 nel conteggio "Non gestita", quando si trova in uno stato Stopped. Per ulteriori informazioni, consulta [Cos'è un'istanza non gestita?](#).

25 febbraio 2025

[Argomento aggiornato:](#)  
[Verifica della firma dell'SSM Agent](#)

14 febbraio 2025

I pacchetti di installazione AWS Systems Manager Agent (SSM Agent) RPM e Debian per le istanze Linux sono firmati crittograficamente. È possibile utilizzare una chiave pubblica per verificare che il pacchetto dell'agente sia originale e non modificato. Se i file sono danneggiati o sono stati alterati, la verifica non va a buon fine. È possibile verificare la firma del pacchetto di installazione utilizzando RPM o GPG. L'argomento include una nuova chiave pubblica per l'SSM Agent. Per ulteriori informazioni, consulta [Verifica della firma dell'SSM Agent](#).

### [Nuovo argomento: Verifica della firma del plug-in Session Manager](#)

I pacchetti di installazione RPM e Debian del plug-in Session Manager per le istanze Linux sono firmati crittograficamente. È possibile utilizzare una chiave pubblica per verificare che il plug-in binario e il pacchetto siano originali e non modificati. Se i file sono in qualche modo danneggiati o alterati, la verifica non va a buon fine. È possibile verificare la firma del pacchetto di installazione utilizzando lo strumento GNU Privacy Guard (GPG). Per ulteriori informazioni, consulta [Verifica della firma del plug-in Session Manager](#).

13 febbraio 2025

### [Plug-in di Session Manager aggiornato](#)

Il plug-in di Session Manager è stato recentemente aggiornato con i seguenti miglioramenti: aggiornamento della versione Go alla 1.23 nel Dockerfile. È stata aggiornata la fase di configurazione della versione nel [README](#). Per ulteriori informazioni sul plug-in di Session Manager, consulta [Installazione del plug-in di Session Manager per la AWS CLI](#).

06 febbraio 2025

[Quote TPS pubblicate per le operazioni dell'API di Automazione](#)

Abbiamo pubblicato le quote di transazione al secondo (TPS), precedentemente note come limitate, per diverse azioni dell'API di Systems Manager. Automation-related Per informazioni, consulta [Service quotas di Systems Manager](#) nella Riferimenti generali di Amazon Web Services.

21 gennaio 2025

[Modifica della terminologia: le funzionalità di Systems Manager sono state rinominate "strumenti"](#)

Fino ad ora, le unità funzionali che compongono Systems Manager erano chiamate funzionalità, come la funzionalità di Automazione, la capacità di Parameter Store e così via. Queste unità funzionali sono ora denominate strumenti, come lo strumento di Automazione e quello di Parameter Store. Questa guida per l'utente è stata aggiornata in modo da includere le modifiche.

10 gennaio 2025

[Supporto di Patch Manager per le versioni macOS aggiuntive \(AMI di Amazon EC2\)](#)

Patch Manager ora supporta macOS le versioni 12.7, 13.6, 13.7 e 15.x. Per gli elenchi completi dei sistemi operativi e delle versioni supportati da Patch Manager, consulta [Sistemi operativi supportati per Patch Manager](#).

08 gennaio 2025

[Supporto per SSM Agent e Patch Manager per versioni aggiuntive: CentOS Stream, Ubuntu Server e Windows Server](#)

Patch Manager ora supporta CentOS Stream 9, Ubuntu Server 24.10 e Windows Server 2025. SSM Agent ora supporta Ubuntu Server 24.10 e 2025. Windows Server (Il supporto di Agent per CentOS Stream 9 è stato rilasciato in precedenza.) Per gli elenchi completi delle versioni e sistemi operativi supportati, consulta quanto segue:

22 novembre 2024

- [Sistemi operativi supportati per Systems Manager](#)
- [Sistemi operativi supportati per Patch Manager](#)

[Nuovo argomento: crittografia dei parametri AWS KMSPParameter Store SecureString](#)

Scopri come AWS Systems ManagerParameter Store AWS Key Management Service si utilizza la crittografia dei valori dei SecureString parametri Parameter Store nel seguente argomento:

22 novembre 2024

- [AWS KMS crittografia per i SecureString parametri in Parameter Store](#)

## [Policy gestite nuove e aggiornate per Systems Manager](#)

Per supportare le nuove funzionalità di Systems Manager, stiamo rilasciando diverse nuove policy gestite per supportare nuove configurazioni e operazioni di Systems Manager e aggiornando altre policy gestite. Per ulteriori informazioni, vedere Aggiornamenti [di Systems Manager alle politiche AWS gestite](#).

21 novembre 2024



## [Una nuova esperienza semplificata di gestione dei nodi per Systems Manager](#)

21 novembre 2024

AWS Systems Manager ha rilasciato una nuova esperienza di console unificata per la gestione dei nodi su larga scala tra account e regioni. Ora puoi vedere tutti i nodi gestiti e non gestiti delle tue organizzazioni Account AWS e regioni da un'unica posizione. È possibile anche identificare, diagnosticare e correggere i nodi non gestiti. Systems Manager è ora integrato anche con Amazon Q Developer (Amazon Q), che estende la tua capacità di vedere e controllare i tuoi nodi da qualsiasi punto Console di gestione AWS inserendo istruzioni in linguaggio naturale. Con questa versione, ora puoi anche consentire a AWS Organizations a un account amministratore delegato di gestire i nodi in tutta l'organizzazione da un punto di vista centrale. Per ulteriori informazioni, consulta i seguenti argomenti:

- [Che cos'è? AWS Systems Manager](#)
- [Configurazione AWS Systems Manager](#)
- [Completa le attività del nodo con AWS Systems Manager](#)

### [Correzione di bug del plug-in di Session Manager](#)

Il Session Manager plugin è stato recentemente aggiornato con la seguente correzione di bug: Modifica annullata che aggiungeva credenziali alle OpenDataChannel richieste.

20 novembre 2024

### [Miglioramenti del plug-in di Session Manager](#)

Questa versione è stata dichiarata obsoleta il 11/2024.

6 novembre 2024

Il plug-in di Session Manager è stato recentemente aggiornato con i seguenti miglioramenti.

- Credenziali aggiunte alle OpenDataChannel richieste.
- Sono stati aggiornati i pacchetti dipendenti testify e objx.

### [Supporto aggiuntivo alla versione del sistema operativo per macOS](#)

Systems Manager ora supporta la versione 15.x (Sequoia) del sistema operativo macOS (solo istanze EC2). Per un elenco di tutti i sistemi operativi e le versioni supportati, vedere [Sistemi operativi supportati per Systems Manager](#).

6 novembre 2024

### [Patch Manager: aggiornamenti ai formati dei nomi dei pacchetti supportati per gli elenchi Approvati e Rifiutati](#)

Per diversi sistemi operativi, abbiamo aggiornato e ampliato gli elenchi di formati per i nomi dei pacchetti che è possibile specificare negli elenchi delle Patch approvate e delle Patch rifiutate nelle baseline delle patch. Per informazioni, consulta [Formati del nome del pacchetto per Amazon Linux 1, Amazon Linux 2, Amazon Linux 2022, Amazon Linux 2023, CentOS, Oracle Linux, e Red Hat Enterprise Linux \(RHEL\)](#).

1° novembre 2024

### [Supporto aggiuntivo della versione operativa per Patch Manager](#)

Patch Manager ora supporta versioni aggiuntive di Oracle Linux (8.10 e 9.4) e Ubuntu Server (23.10 e 24.04). Per gli elenchi di tutte le versioni e sistemi operativi supportati, consultare i seguenti argomenti:

1° novembre 2024

- [Sistemi operativi supportati per Systems Manager](#)
- [Sistemi operativi supportati per Patch Manager](#)

[Supporto dell'SSM Agent per versioni aggiuntive: CentOS Stream, Oracle Linux, e Ubuntu Server](#)

SSM Agent ora supporta CentOS Stream 9, Oracle Linux 8.10 e 9.4 e Ubuntu Server 24.04 LTS, oltre alle versioni precedenti supportate. Per gli elenchi completi dei sistemi operativi e delle versioni supportati per Systems Manager, consultare [Sistemi operativi supportati per Systems Manager](#).

25 ottobre 2024

[Miglioramento del plug-in Session Manager](#)

È stato aggiunto il supporto per il passaggio della versione del plugin con le richieste. OpenDataChannel

10 ottobre 2024

[Novità: visualizza i dettagli sulle connessioni RDP effettuate utilizzando Fleet Manager](#)

Ora puoi visualizzare le informazioni sulle connessioni del protocollo Remote Desktop che sono state effettuate dagli utenti nel tuo Account AWS. Per informazioni, consulta [Visualizzazione delle informazioni sulle connessioni correnti e completate](#).

10 ottobre 2024

### [Patch Manager supporta ora la versione SLES 15.6](#)

È stato rilasciato il supporto per l'applicazione di patch per SUSE Linux Enterprise Server (SLES) 15.6. È ora possibile applicare patch alle macchine 15.6 di SLES utilizzando Patch Manager. Per un elenco di sistemi operativi e versioni supportate da Patch Manager, consulta [Sistemi operativi e regioni supportati per Patch Manager](#).

29 settembre 2024

## [Nuove versioni dell'estensione Lambda AWS Parameters and Secrets](#)

Nuove versioni delle [estensioni  
i Lambda di segreti e  
parametri AWS](#) sono ora

19 settembre 2024

disponibili. È stato introdotto il supporto per tutte le architetture per la Regione Asia Pacifico (Malesia) (ap-southeast-5). Inoltre, è stato aggiunto il supporto per l'estensione dell'architettura ARM64 e Mac with Apple silicon per le seguenti regioni:

- Asia Pacifico (Hyderabad) (ap-south-2)
- Asia Pacifico (Melbourne) (ap-southeast-4)
- Canada occidentale (Calgary) (ca-west-1)
- Europa (Zurigo) (eu-central-2)
- Europa (Spagna) (eu-south-2)
- Medio Oriente (EAU) (me-central-1)
- Cina (Pechino) cn-north-1
- Cina (Ningxia) cn-nordovest-1
- Israele (Tel Aviv) (il-central-1)
- AWS GovCloud (US-East) (us-gov-east-1)
- AWS GovCloud (US-West) (us-gov-ovest-1)

[Nuovo argomento: Configurazione delle autorizzazioni per le finestre di manutenzione utilizzando AWS CLI](#)

L'argomento [Configurazione delle autorizzazioni per le finestre di manutenzione utilizzando la AWS CLI](#) fornisce istruzioni per la creazione di un ruolo di servizio personalizzato (e delle relative policy) per l'esecuzione delle attività della finestra di manutenzione per conto di un utente.

19 agosto 2024

[SSM Agente Patch Manager supporto per versioni aggiuntive: AlmaLinux,, e Oracle LinuxRocky Linux](#)

SSM Agente Patch Manager ora supportano le versioni 8.10, 9.3 e 9.4 di and e la versione 9.3 di AlmaLinux Rocky LinuxOracle Linux, oltre alle versioni precedenti supportate. Per gli elenchi completi delle versioni e sistemi operativi supportati, consulta quanto segue:

14 agosto 2024

- [Sistemi operativi supportati per Systems Manager](#)
- [Sistemi operativi supportati per Patch Manager](#)

[Nuova condizione della policy IAM per il supporto Parameter Store: ssm:Policies](#)

Utilizzando `ssm:Policies`, una nuova condizione supportata per le policy IAM, è possibile impedire alle Entità di creare o aggiornare parametri che includono una policy parametrica. Per ulteriori informazioni, consulta i seguenti argomenti:

14 agosto 2024

- [ssm:Policies: impedisce la creazione o l'aggiornamento di parametri che utilizzano policy di parametro](#)
- [Chiavi di condizione per AWS Systems Manager](#) nel Riferimento per l'autorizzazione del servizio.

[Politica gestita aggiornata per: Quick Setup SSMQuickSetupRolePolicy](#)

Systems Manager ha aggiornato la policy gestita `SSMQuickSetupRolePolicy` per fornire l'accesso a set di CloudFormation stack aggiuntivi. Per informazioni, vedere Aggiornamenti [di Systems Manager alle policy AWS gestite](#).

13 agosto 2024



[Supporto per il provisioning  
e la gestione delle risorse di  
Systems Manager tramite  
Terraform](#)

Abbiamo aggiunto HashiCorp Terraform all'elenco delle integrazioni di terze parti supportate con Systems Manager. [Terraform](#) è uno strumento software open source di infrastructure as code (IaC) che fornisce un flusso di lavoro con interfaccia a riga di comando (CLI) per gestire vari servizi cloud. È possibile utilizzare Terraform per effettuare il provisioning e gestire diverse risorse e fonti di dati di Systems Manager di uso comune. Per informazioni su questa e altre integrazioni di terze parti con Systems Manager, vedere [Integrazione con altri prodotti e servizi](#).

1° agosto 2024

## [Nuova esperienza della console di Quick Setup e API](#)

Systems Manager Quick Setup ha rilasciato una nuova esperienza di console e API. Ora puoi interagire con questa API utilizzando la console, AWS CLI CloudFormation, e gli SDK. È possibile attivare la nuova console utilizzando la console Quick Setup. Per ulteriori informazioni sull'accesso alla nuova esperienza Quick Setup, consulta la [Guida introduttiva alla Configurazione rapida](#). Per maggiori dettagli sulle operazioni API disponibili tramite l'API Quick Setup, consulta la [Documentazione di riferimento API di Quick Setup](#).

1° agosto 2024

[Nuovo argomento: opzioni dell'elenco delle patch rifiutate nelle baseline delle patch personalizzate](#)

Per le operazioni di patch che utilizzano una baseline delle patch personalizzata in Patch Manager, abbiamo chiarito il comportamento quando a una patch aggiunta all'elenco delle Patch rifiutate viene assegnata l'azione Allow as dependency . Poiché Windows Server non supporta il concetto di dipendenze tra le patch, le patch ancora non installate su un nodo gestito vengono ignorate. Alle patch già installate sul nodo viene assegnato lo stato INSTALLED\_REJECTED

. Per ulteriori informazioni, consulta le [Opzioni dell'elenco delle patch rifiutate nelle baseline delle patch personalizzate](#) e [Valori di conformità delle patch per altri sistemi operativi](#).

23 luglio 2024

[Nuovo argomento: Configurazione dell'SSM Agent da utilizzare con il Federal Information Processing Standard \(FIPS\)](#)

Abbiamo fornito istruzioni per la configurazione dell'SSM Agent per l'uso con il Federal Information Processing Standard (FIPS). Per informazioni, consulta la pagina [Configurazione dell'SSM Agent da utilizzare con il Federal Information Processing Standard \(FIPS\)](#).

22 luglio 2024

[Aggiornamento: è stato chiarito il supporto per i simboli @ nei nomi utente di Fleet Manager](#)

Se un nome utente di IAM Identity Center contiene uno o più @ simboli, Fleet Manager RDP ignora il primo @ simbolo e tutti i caratteri che lo seguono, indipendentemente dal fatto che @ introduca la parte di dominio di un indirizzo email. Per ulteriori informazioni sui caratteri supportati per i nomi utente nelle connessioni Fleet Manager RDP, consulta [Autenticazione delle connessioni Desktop remoto](#).

21 luglio 2024

[Policy gestita aggiornata: AmazonSSMManagedEC2InstanceDefaultPolicy](#)

Systems Manager ha aggiornato la policy gestita AmazonSSMManagedEC2InstanceDefaultPolicy fornendo ID di dichiarazione in linea (SID) per chiarire lo scopo di ogni dichiarazione di policy. Per informazioni, vedere Aggiornamenti [di Systems Manager alle politiche AWS gestite](#).

18 luglio 2024

[Modifiche dei nomi ai bucket  
AWS gestiti per le operazioni  
di Patch Manager patching](#)

18 luglio 2024

AWS possiede e gestisce diversi bucket Amazon S3 a cui SSM Agent accede durante l'esecuzione di varie operazioni di patching. Patch Manager Questi bucket S3 sono accessibili pubblicamente e, per impostazione predefinita, l'SSM Agent si connette con essi usando chiamate HTTP. Tuttavia, se utilizzi un endpoint cloud privato virtuale (VPC) nelle operazioni di Systems Manager, è necessario fornire un'autorizzazione esplicita in un profilo dell'istanza Amazon EC2 per Systems Manager o in un ruolo di servizio per le macchine non EC2 in un ambiente ibrido e multicloud. In caso contrario, le risorse non accedono a questi bucket pubblici. Di solito, cambiamo i nomi di questi bucket. Ad esempio, per le operazioni di applicazione di patch, il bucket `aws-patchmanager-macos-us-east-2` viene sostituito da `aws-patchmanager-macos-us-east-2-552881074`, mentre il bucket `aws-ssm-us-east-2` viene sostituito da `aws-patch-manager-us-east-2-55288107`.

4 . Per ulteriori informazioni, consulta i seguenti argomenti:

- [SSM Agent comunicazioni con bucket AWS S3 gestiti](#)
- [Riferimento: bucket Amazon S3 per operazioni di applicazione di patch](#)

#### [Nuovo ruolo collegato al servizio Quick Setup](#)

Systems Manager ha rilasciato un nuovo ruolo collegato al servizio, `AWSServiceRoleForSSMQuickSetup` . Systems Manager utilizza questo ruolo per verificare lo stato di configurazione delle risorse impostate , Quick Setup per garantire un uso coerente dei parametri e delle risorse assegnate e per correggere le risorse quando viene rilevata una deriva. La policy gestita associata a questo ruolo è [SSMQuickSetupRolePolicy](#) . Per ulteriori informazioni, vedere Autorizzazioni dei ruoli [AWSServiceRoleForSSMQuickSetup collegati ai servizi per Systems Manager](#).

3 luglio 2024

[Nuove policy gestite per i tipi di configurazione di Quick Setup](#)

Systems Manager ha rilasciato o altre 12 nuove policy gestite per supportare vari tipi e processi di configurazione di Quick Setup. Per informazioni, vedere [Aggiornamenti di Systems Manager alle AWS politiche gestite.](#)

3 luglio 2024

[Supporto per RHEL 8.10 e 9.4](#)

Systems Manager e Patch Manager ora supportano le versioni Red Hat Enterprise Linux 8.10 e 9.4. Per ulteriori informazioni, vedere [Sistemi operativi e tipi di macchine supportati](#) e [Sistemi operativi supportati per Patch Manager.](#)

26 giugno 2024

[Patch Managersupporto per le versioni 8.8 e 8.9: AlmaLinux,, Oracle Linux e Rocky Linux](#)

Patch Managerora supporta le versioni 8.8 e 8.9 di AlmaLinux , e Oracle LinuxRocky Linux, oltre alle precedenti versioni 8.x. Per gli elenchi completi dei sistemi operativi e delle versioni supportati per Patch Manager, consulta [Sistemi operativi supportati per Patch Manager.](#)

17 giugno 2024

## [Nuovi parametri pubblici per le AMIs Amazon EC2 di macOS](#)

17 giugno 2024

I parametri pubblici sono stati rilasciati per supportare Amazon Machine Images per le istanze di Amazon Elastic Compute Cloud di macOS. Per ulteriori informazioni, consulta i seguenti argomenti.

- [Trovare parametri pubblici](#)
- [Chiamata dei parametri pubblici AMI per macOS](#)
- [Avvia un'istanza Mac](#) nella Guida per l'utente di Amazon EC2
- [Istanze Mac di Amazon EC2](#) nella Guida per l'utente di Amazon EC2
- [Utilizza AWS Systems Manager i parametri anziché AMI gli ID nei modelli di avvio nella Amazon EC2 Auto Scaling User Guide](#)



[Aggiornamento: disponibilità regionale del percorso dei parametri /aws/service/global-infrastructure](#)

Abbiamo chiarito a quali [regioni commerciali](#) è possibile richiedere il percorso del parametro pubblico `/aws/service/global-infrastructure`, e come eseguire una query per il percorso se si lavora in un'altra Regione AWS commerciale. Per informazioni, consulta [Chiamare i parametri pubblici per AWS servizi, regioni, endpoint, zone di disponibilità, zone locali e zone di lunghezza d'onda.](#)

12 giugno 2024

[Nuovo: capitolo sugli esempi di codice](#)

Un nuovo capitolo, [Code examples for Systems Manager using AWS SDKs](#), fornisce esempi in diversi linguaggi SDK su come lavorare con il servizio Systems Manager.

8 maggio 2024

### Modifiche al supporto degli ec2messages:\* endpoint

Per il Regioni AWS lancio nel 2024 o versioni successive, gli ec2messages:\* endpoint non sono supportati SSM Agent per l'invio di informazioni sullo stato e sull'esecuzione al servizio Systems Manager. Gli account di queste regioni necessitano l'utilizzo di ssmmessages:\* . Nelle regioni lanciate prima del 2024, sia ssmmessages:\* che ec2messages:\* sono ancora supportati, ma ora consigliamo di utilizzare solo gli endpoint ssmmessages:\* (Amazon Message Gateway Service). Al momento è possibile rimuovere in sicurezza le autorizzazioni ec2messages:\* dalle policy. Per ulteriori informazioni, vedere [Lavorare con SSM Agent](#) e operazioni [Agent-related API \(endpoint ssmmessages ed ec2messages\)](#).

3 maggio 2024

### Sono disponibili runtime aggiuntivi per l'esecuzione di script nei runbook Automation

L'azione aws:executeScript supporta ora i runtime Python 3.9, 3.10 e 3.11. Per ulteriori informazioni sull'utilizzo di quest'azione, consulta [aws:executeScript](#) .

23 aprile 2024

[Supporto per le versioni 8.8 e 8.9:, e AlmaLinux Oracle LinuxRocky Linux](#)

Systems Manager ora supporta le versioni 8.8 e 8.9 di AlmaLinux, e Oracle LinuxRocky Linux, oltre alle precedenti versioni 8.x. Per gli elenchi completi di tutti i sistemi operativi e le versioni supportati, vedere [Sistemi operativi supportati per Systems Manager](#).

22 aprile 2024

[Patch Manager: passa allo stato di applicazione di patch 'INSTALLED\\_PENDING\\_REBOOT'](#)

In precedenza, solo le patch installate da Patch Manager venivano contrassegnate come INSTALLED\_PENDING\_REBOOT. Le patch installate al di fuori di Patch Manager non hanno mai ricevuto questo stato. Ora, è possibile associare INSTALLED\_PENDING\_REBOOT a qualsiasi patch applicata a un nodo gestito dall'ultima volta che è stato riavviato. Ciò include le patch installate da Patch Manager con l'opzione NoReboot selezionata e le patch installate al di fuori di Patch Manager dopo il riavvio più recente del nodo. Per le descrizioni di tutti i valori dello stato di applicazione di patch di Patch Manager, vedi [Informazioni sui valori relativi allo stato di conformità delle patch](#).

16 aprile 2024

[Supporto per RHEL 8.9 e 9.3](#)

Systems Manager, incluso Patch Manager, ora supporta le versioni Red Hat Enterprise Linux (RHEL) 8.9 e 9.3, oltre alle precedenti versioni 8.x e 9.x.

26 marzo 2024

[Aggiornamento dell'argomento: politiche gestite per AWS Systems Manager](#)

L'argomento [Policy gestite da AWS per AWS Systems Manager](#) ha fornito informazioni sulle quattro policy gestite per Systems Manager che sono state introdotte o aggiornate dal 12 marzo 2021. Abbiamo aggiunto una sezione a questo argomento con informazioni sulle altre 12 policy gestite da utilizzare con Systems Manager che sono state create o aggiornate l'ultima volta prima di tale data. Per i dettagli, consulta [Policy gestite aggiuntive per Systems Manager](#).

1° marzo 2024

### [Parameter Store supporta ora la condivisione tra più account](#)

Ora puoi condividere i parametri avanzati in modo sicuro ed efficiente all'interno Account AWS o all'interno della tua AWS organizzazione configurando la condivisione delle risorse. La condivisione delle risorse consente di centralizzare la gestione della configurazione delle applicazioni e di ridurre il sovraccarico operativo derivante dalla condivisione dei parametri con ogni singolo account di proprietà. I parametri possono essere condivisi tra gli account utilizzando la Parameter Store console, la AWS RAM console o il AWS CLI Per ulteriori informazioni, consulta la sezione [Utilizzo dei parametri condivisi](#).

21 febbraio 2024

### [Miglioramento delle operazioni di automazione](#)

È ora possibile utilizzare le proprietà `onFailure` e `isCritical` con l'azione `aws:approve`. Per ulteriori informazioni sull'operazione `aws:approve`, consulta [aws:approve: sospendere un'automazione per l'approvazione manuale](#).

12 febbraio 2024

### [Supporto aggiuntivo della versione operativa per Patch Manager](#)

Aggiunta all'elenco delle [versioni del sistema operativo supportate per Patch Manager](#). È stato aggiunto anche supporto per i seguenti:

04 gennaio 2024

- Debian Server 11.x e 12.x
- macOS 14.x (Sonoma)
- SUSE Linux Enterprise Server (SLES) 15.5
- Ubuntu Server23.04

### [Configurazione degli aggiornamenti automatici di SSM Agent tramite la console Application Manager](#)

Ora è possibile utilizzare e la console Application Manager per automatizzare gli aggiornamenti di SSM Agent per le istanze delle applicazioni. Per ulteriori informazioni, consulta la pagina [Utilizzo delle istanze dell'applicazione](#).

21 dicembre 2023

### [Nuovo processo per la registrazione di macchine non Amazon EC2 in ambienti ibridi e multi-cloud](#)

Systems Manager ora fornisce la `ssm-setup-cli`, che consente di registrare macchine non Amazon Elastic Compute Cloud (Amazon EC2) in ambienti ibridi e multi-cloud. Per ulteriori informazioni, vedere [Come installare SSM Agent su nodi Linux ibridi](#) e [Come installare SSM Agent su nodi Windows ibridi](#).

20 dicembre 2023

### [Gestione dei volumi Amazon EBS tramite Fleet Manager](#)

Ora puoi utilizzare uno strumento in Fleet Manager AWS Systems Manager, per gestire i volumi di Amazon Elastic Block Store sulle tue istanze gestite. Ad esempio, è possibile inizializzare un volume EBS, formattare una partizione e montare il volume per renderlo disponibile all'uso. Per ulteriori informazioni, consulta la pagina [Gestione dei volumi EBS](#).

14 dicembre 2023

### [Miglioramento del plug-in Session Manager](#)

È stato aggiunto il supporto per il passaggio di una risposta [StartSession](#) API come variabile di ambiente a session-manager-plugin.

04 dicembre 2023

### [Nuova esperienza di progettazione visiva per i runbook Automation](#)

Ora è possibile creare e modificare i runbook utilizzando una nuova esperienza di progettazione visiva sviluppata da Systems Manager Automation. L'esperienza di progettazione visiva offre un'interfaccia drag-and-drop con poco codice che consente di creare e modificare i runbook più facilmente. Per ulteriori informazioni, consulta [Esperienza di progettazione visiva per i runbook Automation](#).

26 novembre 2023

[Nuove operazioni di Systems Manager Automation, elementi di dati e miglioramenti funzionali per i runbook](#)

17 novembre 2023

È ora possibile eseguire il ciclo con più operazioni in un runbook utilizzando l'azione `aws:loop`. Questa nuova azione supporta i cicli in stile `do while` e `for each`. Inoltre, utilizzando il nuovo elemento di dati variabili, è possibile definire, fare riferimento e aggiornare i valori in modo dinamico nel contesto di un runbook. Per aggiornare il valore di una variabile nel runbook, usa la nuova azione `aws:updateVariable`. Automation ha anche aggiunto il supporto per le conversioni dinamiche dei tipi di dati per gli output. Ciò significa che se il valore di un output non corrisponde al tipo di dati specificato, Automation prova a convertire il tipo di dati. Ad esempio, se il valore restituito è un `Integer`, ma il `Type` specificato è `String`, allora il valore dell'output finale sarà un valore `String`. Infine, Automation ora supporta le espressioni di filtro `JSONPath` per i selettori. Per ulteriori informazioni, consulta i seguenti argomenti:

- [aws:loop: itera le fasi in un processo di automazione](#)



- [aws:updateVariable:](#)  
[aggiorna un valore per una  
variabile del runbook](#)
- [Elementi e parametri di dati:](#)  
[elementi di dati Top-level](#)
- [Utilizzo degli output delle  
operazioni come input.](#)
- [Utilizzo della variabile  
JSONPath nei runbook.](#)

[Supporto per le Regioni  
aggiornato per le connessio  
ni Remote Desktop Protocol  
\(RDP\)](#)

[Il Desktop remoto di Fleet  
Manager](#), basato su Amazon  
DCV, offre una connettività  
sicura alle istanze Windows  
Server direttamente dalla  
console di Systems Manager.  
Le seguenti tre Regioni  
aggiuntive sono state abilitate  
per le connessioni di Desktop  
remoto Fleet Manager:

15 novembre 2023

- Africa (Città del Capo) (af-  
south-1)
- Asia Pacifico (Giacarta) (ap-  
southeast-3)
- Israele (Tel Aviv) (il-centr  
al-1)

[Patch Manager: supporto esteso della versione del sistema operativo per RHEL e macOS](#)

Patch Manager ora supporta le seguenti ulteriori versioni di sistema operativo:

23 ottobre 2023

- Red Hat Enterprise Linux: versione 8.8
- macOS: 11.5-11.7 (Big Sur)
- macOS: 12.0-12.6 (Monterey)
- macOS: 13.0-13.5 (Ventura)

[Nuova API OpsCenter: DeleteOpsItem](#)

OpsCenter ora offre l'API DeleteOpsItem per l'eliminazione di singoli OpsItems. Per ulteriori informazioni, consulta [DeleteOpsItem](#) nella documentazione di riferimento dell'API AWS Systems Manager .

20 ottobre 2023

[Nuovo tipo di configurazione Quick Setup: aggiornamenti SSM Agent per l'intera organizzazione](#)

Il nuovo tipo di configurazione Default Host Management Configuration consente a un amministratore dell'organizzazione, come definito in AWS Organizations, di richiedere il controllo e gli aggiornamenti automatici di SSM Agent tutte le istanze EC2 negli account e nelle regioni dell'organizzazione. Per ulteriori informazioni, consulta la pagina [Gestione host predefinita per un'organizzazione](#).

16 ottobre 2023

[Nuovo formato di titolo e descrizione OpsItems creato da CloudWatch Application Insights](#)

Il titolo e la descrizione di «OpsItems creato da CloudWatch Application Insights» cambieranno in un formato migliorato il 16 ottobre 2023. Per visualizzare il nuovo formato, consulta [Amazon CloudWatch Application Insights](#).

29 settembre 2023

## [Supporto per più risoluzioni di visualizzazione nelle connessioni Fleet Manager RDP](#)

22 settembre 2023

Quando ti connetti ai nodi gestiti da Windows Server utilizzando l'opzione Remote Desktop protocol (RDP) in Fleet Manager, ora è possibile scegliere la risoluzione dello schermo. In precedenza, tutte le connessioni utilizzavano una risoluzione fissa di 720P (1366 x 768). Ora è possibile scegliere tra le seguenti opzioni per ogni connessione:

- Adatta automaticamente (determina la risoluzione ottimale in base alle dimensioni dello schermo rilevate)
- 1920 x 1080
- 1400 x 900
- 1366 x 768
- 800 x 600

Per ulteriori informazioni, consulta [Connessione a un nodo gestito tramite desktop remoto](#).

[Nuovo argomento: ID casuali delle baseline delle patch nelle operazioni relative alle policy delle patch](#)

Abbiamo aggiunto contenuti per descrivere come le policy delle patch di Quick Setup utilizzano il parametro `BaselineOverride` nel documento `AWS-RunPatchBaseline` SSM Command per generare ID casuali per le baseline delle patch ogni volta che viene eseguita un'operazione relativa a queste. Per informazioni, consulta [ID casuali delle baseline delle patch nelle operazioni relative alle policy delle patch](#).

22 settembre 2023

[Un nuovo approfondimento operativo per la gestione di OpsItems](#)

OpsCenter ora include una panoramica operativa denominata `Risorse che generano di più OpsItems`. Una panoramica di questo tipo viene generata quando una AWS risorsa ne ha più di 10 aperte `OpsItems`. Usa questo approfondimento per individuare le risorse problematiche. Usa il runbook `AWS-BulkResolveOpsItems` dall'interno di un approfondimento per risolvere rapidamente gli `OpsItems` associati a una risorsa. Per ulteriori informazioni, consulta [Analisi degli approfondimenti operativi per ridurre gli OpsItems](#).

22 settembre 2023

### [Chiave pubblica GPG aggiornata](#)

È stata creata una nuova chiave pubblica per verificarla e la firma di SSM Agent. Per ulteriori informazioni, consulta [Verifica della firma di SSM Agent](#).

05 settembre 2023

### [È stato aggiunto il supporto per versioni aggiuntive di AlmaLinux, Oracle Linux, RHEL, e Rocky Linux](#)

Gli elenchi dei sistemi operativi supportati per [AWS Systems Manager](#) e [Patch Manager](#) sono stati aggiornati in modo da supportare le seguenti versioni aggiuntive del sistema operativo:

30 agosto 2023

- AlmaLinux: 9.2
- Oracle Linux: 8.7 e 9.2
- Red Hat Enterprise Linux (RHEL): 8.7, 9.1 e 9.2
- Rocky Linux: 8.6 e 8.7, 9.0 - 9.2

[OpsCenter ha aggiunto il supporto per la formattazione Markdown nel campo della descrizione dell'OpsItem.](#)

OpsCenter ora supporta la formattazione Markdown nel campo della descrizione dell'OpsItem. Sono supportati i seguenti tipi di formattazione Markdown:

18 agosto 2023

- Paragrafi
- Spaziatura tra le righe
- Linee orizzontali
- Intestazioni
- Formattazione del testo
- Link
- Elenchi

Per ulteriori informazioni, consulta [Usare Markdown nella Console](#) nella Guida introduttiva alla guida Console di gestione AWS introduttiva.

[Nuove versioni dell'estensione Lambda AWS Parameters and Secrets](#)

Sono ora disponibili nuove versioni dell'estensione AWS Parameters and Secrets Lambda. Inoltre, è stato aggiunto il supporto delle estensioni per le Regioni Asia Pacifico (Melbourne) (ap-south-east-4) e Israele (Tel Aviv) (il-central-1) (solo le architetture x86\_64 e x86). Per ulteriori informazioni, vedere [Utilizzo Parameter Store dei parametri nelle AWS Lambda funzioni.](#)

16 agosto 2023

[Aggiornamento: sono state aggiunte informazioni sulle autorizzazioni richieste per i bucket delle policy di patch relative a Quick Setup](#)

06 luglio 2023

Quando crei una policy di patch, Quick Setup crea un bucket Amazon S3 che contiene un file denominato `baseline_overrides.json`. Questo file memorizza le informazioni sulle baseline delle patch che hai specificato per la tua policy di patch. Quando configuri la policy di patch, hai la possibilità di selezionare la casella di controllo **Aggiungi le policy IAM richieste ai profili di istanza esistenti collegati alle istanze**. Se scegli di non selezionare questa opzione, devi fornire manualmente a determinate risorse le autorizzazioni per accedere a questo bucket, altrimenti le operazioni relative alle policy potrebbero non riuscire. Per ulteriori informazioni, consulta i seguenti argomenti:

- [Autorizzazioni per il bucket S3 con policy di patch](#)
- [Problema: errore "Invoke-PatchBaselineOperation : accesso negato" o errore «Impossibile scaricare il file da S3" per baseline\\_overrides.json](#)



[Utilizzare Quick Setup per configurare OpsCenter per la gestione di OpsItems su più account](#)

Quick Setup per OpsCenter consente di completare le seguenti attività per la gestione di OpsItems su più account:

19 giugno 2023

- Definizione dell'account di amministratore delegato
- Creazione di policy e ruoli obbligatori AWS Identity and Access Management (IAM)
- Specificare un' AWS Organizations organizzazione o un sottoinsieme di account membri, in cui un amministratore delegato può gestire tutti gli account OpsItems

Per ulteriori informazioni, consulta [\(Facoltativo\) Configurare OpsCenter per la gestione di OpsItems su più account utilizzando Quick Setup](#).

### [Aggiornare gli agenti di avvio di Amazon EC2 utilizzando Quick Setup](#)

Ora è possibile consentire a Systems Manager di verificar e ogni 30 giorni la presenza di una nuova versione dell'agente di avvio installato sull'istanza. Se è presente una nuova versione, Systems Manager aggiorna l'agente sull'istanza. Per ulteriori informazioni, consulta [Quick Setup Gestione Host](#).

19 giugno 2023

### [Patch Manager ora supporta Ubuntu Server 22.04 LTS](#)

Ora è possibile utilizzare Patch Manager per patchare i nodi Ubuntu Server 22.04 LTS. Come altre versioni supportate di Ubuntu Server, la versione 22.04 LTS, utilizza la patch di base gestita. AWS-`UbuntuDefaultPatchBaseline`

15 maggio 2023

### [Systems Manager ora supporta, tra cui AlmaLinux Patch Manager](#)

È ora possibile utilizzare Systems Manager per gestire i nodi AlmaLinux 8.3-8.7; 9.0-9.1. Molte delle regole che si applicano a RHEL 8 per l'applicazione delle patch si applicano anche a. AlmaLinux AlmaLinux utilizza il nuovoAWS-DefaultAlmaLinuxPatchBaseline . Per ulteriori informazioni, consulta i seguenti argomenti:

08 maggio 2023

- [Installazione manuale SSM Agent sulle AlmaLinux istanze](#)
- [Come vengono selezionate le patch di sicurezza](#)
- [Come vengono installate le patch](#)
- [Come funzionano le regole di base delle patch su AlmaLinux, RHEL, e. Rocky Linux](#)

### [Implementare l'agente EC2Launch v2 utilizzando Quick Setup](#)

Ora è possibile implementare l'agente EC2Launch v2 utilizzando Quick Setup. Per ulteriori informazioni, consulta la pagina [Implementazione di pacchetti Distributor con Quick Setup](#).

13 aprile 2023

## [Systems Manager ora supporta Amazon Linux 2023](#)

23 marzo 2023

Systems Manager ora supporta il nuovo tipo di istanza EC2 Amazon Linux 2023 (AL2023), incluso il supporto per le operazioni di Patch Manager. Molte delle regole per l'applicazione di patch che valgono per Amazon Linux 2 valgono anche per Amazon Linux 2023. (Patch Manager continua inoltre a supportare la versione di anteprima di Amazon Linux 2022). Per ulteriori informazioni, consulta i seguenti argomenti:

- [Come vengono selezionate le patch di sicurezza](#)
- [Come vengono installate le patch](#)
- [Funzionamento delle regole delle baseline delle patch su Amazon Linux 1, Amazon Linux 2, Amazon Linux 2022 e Amazon Linux 2023](#)

[Revisione della configurazione  
dei contenuti per le istanze  
Amazon EC2](#)

Abbiamo rivisto la configurazione dei contenuti per le istanze Amazon EC2. Ora ti consigliamo di utilizzare la configurazione di gestione host predefinita appena rilasciata per le autorizzazioni dell'istanza. Per ulteriori informazioni, consulta la pagina [Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager](#).

15 febbraio 2023

[Gestione automatica delle  
istanze con la configurazione  
di gestione host predefinita](#)

Ora è possibile gestire automaticamente le istanze Amazon EC2 in un'intera Regione AWS utilizzando Systems Manager. Per ulteriori informazioni, consulta la pagina [Configurazione di gestione host predefinita](#).

15 febbraio 2023

### [Aggiunta di documenti SSM ai preferiti](#)

Per aiutarti a trovare i documenti SSM usati di frequente, ora è possibile aggiungere documenti ai tuoi preferiti. Puoi aggiungere ai preferiti fino a 20 documenti per tipo di documento, per Account AWS e Regione AWS. È possibile scegliere , modificare e visualizzare i tuoi preferiti dalla console Documenti di Systems Manager. Per ulteriori informazioni, consulta la pagina [Aggiunta di documenti ai preferiti](#).

7 febbraio 2023

### [Implementazione dei controlli delle modifiche per Automazione utilizzando Change Calendar](#)

Integrando Automation con Change Calendar, ora puoi implementare i controlli delle modifiche a tutte le automazioni del tuo Account AWS. Per ulteriori informazioni, consulta la pagina [Implementazione dei controlli delle modifiche per Automazione](#).

24 gennaio 2023

## [Nuovo flusso di lavoro di approvazione di Change Manager](#)

Il flusso di lavoro di approvazione di Change Manager ora supporta le approvazioni per livello anziché per riga. In precedenza, ogni approvatore aggiunto a un livello di approvazione doveva approvare una richiesta di modifica, altrimenti il livello non veniva approvato. Ora è possibile specificare quante approvazioni sono necessari e per il livello e aggiungere altrettanti approvatori o un numero maggiore. Ad esempio, è possibile richiedere tre approvazioni per un livello ma specificare fino a cinque approvatori. Le approvazioni di tre di questi approvatori sono sufficienti per approvare il livello. Per ulteriori informazioni, consulta la pagina [Informazioni sulle approvazioni nei modelli di modifica](#).

23 gennaio 2023

[Novità: Configurazione dell'applicazione di patch per un'intera organizzazione mediante una policy di patch in Quick Setup](#)

22 dicembre 2022

Con Quick Setup, uno strumento di Systems Manager, ora è possibile creare policy di patch basate su Patch Manager. Una policy di patch definisce la pianificazione e la baseline delle patch da utilizzare per applicare automaticamente le patch ai nodi gestiti. Con una singola configurazione delle policy di patch, è possibile definire l'applicazione di patch per tutti gli account in tutte le regioni dell'organizzazione, per regioni e account selezionati o per una singola coppia account-regione. Per ulteriori informazioni, consulta i seguenti argomenti.

- [Utilizzo delle policy di patch di Quick Setup](#)
- [Automatizzazione dell'applicazione di patch a livello di organizzazione mediante una policy di patch Quick Setup](#)



[Application Manager si integra con Amazon EC2 per visualizzare informazioni relative alle istanze nel contesto di un'applicazione.](#)

Application Manager visualizza lo stato dell'istanza, lo stato e lo stato di integrità di Amazon EC2 Auto Scaling per un'applicazione selezionata in un formato grafico. La scheda Instances (Istanze) include inoltre una tabella con le seguenti informazioni per ogni istanza dell'applicazione.

22 dicembre 2022

- Stato dell'istanza (Pending [In attesa], Stopping [In arresto], Running [In esecuzione], Stopped [Arrestata])
- Stato ping per SSM Agent
- Stato e nome dell'ultimo runbook Automation Systems Manager elaborato nell'istanza
- Conteggio degli allarmi di Amazon CloudWatch Logs per stato.
  - ALARM: il parametro o l'espressione non rientra nella soglia definita.
  - OK: il parametro o l'espressione rientra nella soglia definita.
  - INSUFFICIENT\_DATA : l'allarme è stato appena attivato, il parametro non è disponibile o la quantità di dati non è sufficientemente

te affinché il parametro determini lo stato dell'alarme.

- Integrità del gruppo Auto Scaling per i gruppi con dimensionamento automatico padre e singoli

[Pianificazione dell'avvio e dell'interruzione delle istanze Amazon EC2 tramite Quick Setup](#)

Ora è possibile implementare la soluzione Pianificatore risorse per automatizzare l'avvio e l'interruzione delle istanze Amazon EC2 utilizzando Quick Setup. Per ulteriori informazioni, consulta [Pianificatore risorse](#).

19 dicembre 2022

## [OpsCenter ora supporta l'utilizzo di OpsItems su più account](#)

16 novembre 2022

OpsCenter supporta l'utilizzo di OpsItems da un account di gestione (un account di gestione di AWS Organizations o un account amministratore delegato di Systems Manager) e da un account membro durante una sessione. Una volta configurato, gli utenti possono eseguire i seguenti tipi di azione:

- Creare, visualizzare e aggiornare OpsItems in un account membro
- Visualizza informazioni dettagliate sulle AWS risorse specificate OpsItems in un account membro
- Avviare i runbook Automation Systems Manager per risolvere i problemi relativi alle risorse AWS di un account membro

Per ulteriori informazioni, consulta [Configurazione di OpsCenter per l'utilizzo di OpsItems su più account](#).

[Tieni traccia dei dettagli delle richieste di Change Manager modifica utilizzando AWS CloudTrail Lake](#)

11 novembre 2022

Ora puoi utilizzare un data store di eventi in AWS CloudTrail Lake per acquisire ed esaminare i dettagli sulle richieste di modifica inviate Change Manager per la tua organizzazione o il tuo account. Queste informazioni includono dettagli verificabili sull'identità dell'utente che ha creato la richiesta di modifica, l'indirizzo IP da cui è stata effettuata la richiesta, il luogo Regioni AWS in cui sono state apportate le modifiche, le risorse mirate e altro ancora. Per informazioni, consulta le sezioni [Monitoraggio degli eventi della richiesta di modifica](#) e [Analisi dei dettagli delle richieste di modifica, dei processi e delle tempistiche](#).

[Controlli aggiuntivi delle attività di Systems Manager Automation tramite allarmi CloudWatch](#)

È ora possibile implementare un controllo aggiuntivo quando si eseguono automazioni su più account e regioni utilizzando CloudWatch gli allarmi. Applicando un CloudWatch allarme metrico o composito a un'automazione, puoi controllare quando un'automazione si arresta in base alle metriche definite. Per ulteriori informazioni sull'applicazione di un CloudWatch allarme a un'automazione in esecuzione e su più account e regioni, consulta [Eseguire un'automazione in più regioni e account \(console\)](#)

09 novembre 2022

[Aggiornato: 'Utilizzo Parameter Store dei parametri nelle AWS Lambda funzioni'](#)

Abbiamo fornito informazioni aggiuntive per aiutarti a utilizzare l'estensione Lambda AWS Parameters and Secrets per recuperare i valori dei parametri e memorizzarli nella cache per un uso futuro nelle funzioni Lambda. L'utilizzo dell'estensione Lambda può ridurre i costi riducendo il numero di chiamate API a Parameter Store. Per informazioni, consulta [Utilizzo dei Parameter Store parametri nelle funzioni. AWS Lambda](#)

25 ottobre 2022

## [Controlli aggiuntivi delle attività di Systems Manager tramite CloudWatch allarmi](#)

26 settembre 2022

È ora possibile implementare un controllo aggiuntivo o durante l'esecuzione di automazioni e comandi utilizzando CloudWatch gli allarmi. È inoltre possibile aggiungere un CloudWatch allarme a un'automazione o a un comando quando viene registrato con un'operazione di State Manager associata a una finestra di manutenzione. Applicando un CloudWatch allarme composito a un'automazione o a un comando, è possibile controllare quando un'automazione o un comando si interrompe in base alla metrica definita. Per ulteriori informazioni sull'applicazione di un CloudWatch allarme a un'automazione o a un comando, consultate le seguenti procedure:

- [Come vengono selezionate le patch di sicurezza](#)
- [Come vengono installate le patch](#)
- [Funzionamento delle regole della baseline delle patch in Amazon Linux 1, Amazon Linux 2 e Amazon Linux 2022.](#)

## [Controlli aggiuntivi delle attività di Systems Manager mediante CloudWatch allarmi](#)

26 settembre 2022

È ora possibile implementare un controllo aggiuntivo o durante l'esecuzione di automazioni e comandi utilizzando CloudWatch gli allarmi. È inoltre possibile aggiungere un CloudWatch allarme a un'automazione o a un comando quando viene registrato con un'operazione di State Manager associata a una finestra di manutenzione. Applicando un CloudWatch allarme composito a un'automazione o a un comando, è possibile controllare quando un'automazione o un comando si interrompe in base alla metrica definita. Per ulteriori informazioni sull'applicazione di un CloudWatch allarme a un'automazione o a un comando, consultate le seguenti procedure:

- [Esecuzione di un'automazione semplice](#)
- [Esecuzione di comandi dalla console](#)
- [Creazione di un'associazione](#)
- [Per assegnare task a una finestra di manutenzione](#)

### [Chiarimento dei requisiti del piano istanze avanzate](#)

Sulla base del feedback dei clienti, abbiamo chiarito gli scenari che richiedono l'attivazione del piano istanze avanzate in [Configurazione dei livelli di istanza](#).

21 settembre 2022

### [Distribuisce Amazon CloudWatch Agent utilizzando Quick Setup](#)

Ora puoi distribuire l'Amazon CloudWatch agente utilizzando Quick Setup. Per ulteriori informazioni, consulta la pagina [Distribuzione di pacchetti Distributor con Quick Setup](#).

20 settembre 2022



[la chiave 'PatchGroup' ora è supportata per i gruppi di patch quando i metadati delle istanze EC2 sono consentiti](#)

Quando [consenti i tag nei metadati dell'istanza EC2](#), la chiave tag creata non deve contenere spazi. In precedenza, ciò impediva ai clienti di aggiungere alcune delle loro istanze EC2 ai gruppi di patch in Patch Manager perché la chiave tag Patch Group doveva essere applicata alle istanze. Patch Manager supporta ora sia Patch Group (con uno spazio) che PatchGroup (senza spazio) come chiave tag per identificare le istanze di un gruppo di patch. Le istanze EC2 in cui i tag sono consentiti nei metadati dell'istanza possono ora essere aggiunti ai gruppi di patch in Patch Manager. Per informazioni, consulta [Informazioni sui gruppi di patch](#).

31 agosto 2022

[Nuovo argomento: "Il modo in cui vengono calcolate le date di rilascio e di aggiornamento dei pacchetti"](#)

Nelle linee di base delle patch gestite da AWS, le nuove patch vengono approvate automaticamente 7 giorni dopo il rilascio o l'aggiornamento. Nelle baseline delle patch personalizzate che hai create, è possibile specificare facoltativamente quanti giorni aspettare dopo il rilascio o l'aggiornamento per approvarne e automaticamente l'installazione. Per Amazon Linux 1 e Amazon Linux 2, il modo in cui vengono calcolate le date di rilascio e di aggiornamento più recenti è influenzato da vari fattori. Per aiutarti a evitare risultati imprevisti durante la scelta dei ritardi di approvazione automatica, questi fattori sono spiegati nell'argomento [Il modo in cui vengono calcolate le date di rilascio e di aggiornamento dei pacchetti](#).

24 agosto 2022

[Contenuto aggiornato:](#)  
[Applicazione di patch a un'AMI](#)  
[e aggiornamento di un gruppo](#)  
[Auto Scaling](#)

Abbiamo aggiornato la procedura guidata per [Aggiornamento delle AMIs per gruppi Auto Scaling](#) per utilizzare i modelli di avvio anziché le configurazioni di avvio. Inoltre, abbiamo implementato le operazioni e i runtime di Automazione più recenti nel contenuto dei runbook.

22 giugno 2022

## [Change Manager: impedisce agli utenti di creare richieste approvabili in automatico](#)

15 giugno 2022

È possibile configurare i modelli di modifica in Change Manager in modo che supportino le approvazioni automatiche: ciò significa che gli utenti con le autorizzazioni IAM necessarie possono scegliere di avviare la richiesta di modifica senza richiedere un'ulteriore approvazione. Inoltre, ora è possibile impedire a singoli utenti, gruppi o ruoli IAM l'invio di richieste con approvazione automatica, anche se sono supportate da un modello di modifica. Questo risultato si ottiene attraverso l'uso di una nuova chiave di condizione IAM, `ssm:AutoApprove`. Per ulteriori informazioni, consulta la sezione [Controllo dell'accesso ai flussi di lavoro del runbook di approvazione automatica](#)

[Aggiornamento delle informazioni in merito ai ruoli delle attività della finestra di manutenzione](#)

In precedenza, la console di Systems Manager offriva la possibilità di scegliere il ruolo collegato al servizio IAM `AWSServiceRoleForAmazonSSM` gestito da AWS da utilizzare come ruolo di manutenzione per le attività. Non è più consigliato utilizzare questo ruolo e la relativa policy associata, `AmazonSSMServiceRolePolicy`, per le attività della finestra di manutenzione. Invece, è opportuno creare un ruolo e una policy personalizzati per le attività della finestra di manutenzione. Per ulteriori informazioni, consulta la sezione [Configurazione di Maintenance Windows](#).

09 giugno 2022

[Supporto dell'inoltro alla porta agli host remoti per Session Manager](#)

Ora Session Manager supporta le sessioni di inoltro alla porta agli host remoti. Non è necessario che l'host remoto sia gestito da Systems Manager. Per ulteriori informazioni, consulta la sezione [Avvio di una sessione \(inoltro alla porta all'host remoto\)](#).

25 maggio 2022

[Contenuto aggiornato:  
istruzioni per l'installazione  
manuale di SSM Agent sulle  
istanze Linux Amazon EC2](#)

In risposta ai feedback dei clienti, abbiamo revisionato gli argomenti che forniscono istruzioni per l'installazione manuale di SSM Agent sulle istanze Amazon EC2. Questi argomenti ora forniscono comandi tramite file disponibili a livello globale che è possibile copiare e incollare per l'installazione rapida su istanze EC2 in qualsiasi Regione AWS. Questi argomenti forniscono inoltre informazioni utili per la creazione di comandi di installazione che utilizzano i file disponibili nella tua regione di lavoro. Quest'ultimo approccio è consigliato quando installi l'agente su più istanze utilizzando uno script o un modello. Per ulteriori informazioni, consulta le istruzioni per il tuo sistema operativo Linux nella sezione [Installazione manuale di SSM Agent sulle istanze EC2 per Linux](#).

09 maggio 2022

[Nuovo argomento: Amazon Machine Images \(AMIs\) con SSM Agent preinstallato](#)

In risposta ai feedback dei clienti, abbiamo centralizzato le informazioni su quali AMIs gestite da AWS includono SSM Agent preinstallato. In questo argomento vengono inoltre fornite istruzioni su come verificare che un'istanza Amazon EC2 creata da queste AMIs sia stata installata correttamente e sia in esecuzione. Nei rari casi in cui l'agente non sia installato correttamente o sia installato ma non avviato, forniamo anche informazioni sull'avvio o l'installazione manuale dell'agente su queste istanze. Per informazioni dettagliate, consulta l'argomento [Amazon Machine Images \(AMIs\) con SSM Agent preinstallato](#).

08 maggio 2022

[Nuova sezione su State Manager](#)

È stata aggiunta una nuova sezione che descrive i dettagli di quando State Manager esegue associazioni. Per ulteriori informazioni, consulta la sezione [Informazioni sulla pianificazione di associazioni](#).

27 aprile 2022

## [Patch Manager ora supporta Rocky Linux](#)

Ora è possibile utilizzare Patch Manager per applicare patch ai nodi Rocky Linux. Molte delle regole che si applicano a RHEL 8 per l'applicazione di patch si applicano anche a Rocky Linux. Rocky Linux 8 utilizza il nuovo AWS-DefaultRockyLinuxPatchBaseline. Per ulteriori informazioni, consulta i seguenti argomenti:

- [Come vengono selezionate le patch di sicurezza](#)
- [Come vengono installate le patch](#)
- [Funzionamento delle regole delle baseline delle patch in RHEL, CentOS Stream e Rocky Linux.](#)

14 aprile 2022



## [Patch Manager ora supporta CentOS Stream 8](#)

È ora possibile utilizzare Patch Manager per applicare patch alle istanze CentOS Stream 8 e Red Hat Enterprise Linux (RHEL) 4.4-4.5. Molte delle regole che si applicano a RHEL 8 per l'applicazione di patch si applicano anche a CentOS Stream 8. CentOS Stream 8 utilizza AWS-DefaultCentOSPatchBaseline. Per ulteriori informazioni, consulta i seguenti argomenti:

- [Come vengono selezionate le patch di sicurezza](#)
- [Come vengono installate le patch](#)
- [Funzionamento delle regole delle baseline delle patch in RHEL e CentOS Stream](#)

## [Creazione di un ruolo assunto per Change Manager](#)

Una nuova sezione chiarisce i requisiti per la creazione e l'implementazione di un ruolo assunto per Change Manager. Un ruolo assunto è un ruolo di servizio AWS Identity and Access Management (IAM) che consente a Change Manager di eseguire in modo sicuro i flussi di lavoro dei runbook specificati in una richiesta di modifica approvata per tuo conto. Il ruolo garantisce a AWS Systems Manager (AWS STS) AssumeRole fiducia a. Change Manager. Per ulteriori informazioni, consulta [Configurazione di ruoli e autorizzazioni per Change Manager](#).

18 marzo 2022

## [Approvazione o rifiuto delle richieste di modifica di Change Manager in blocco](#)

Nella console di Systems Manager è ora possibile selezionare più richieste di modifica da approvare o rifiutare in un'unica operazione. Per informazioni, consulta [Revisione e approvazione o rifiuto delle richieste di modifica \(console\)](#).

8 marzo 2022

## [Supporto per i nodi gestiti Rocky Linux e Windows Server 2022](#)

1° marzo 2022

Systems Manager supporta i nodi gestiti Rocky Linux e Windows Server 2022, inclusi dispositivi edge e macchine ibride ubicate on-premises o con altri provider cloud. Per utilizzare Systems Manager con questi sistemi operativi, è necessario completare tutte le procedure di configurazione di Systems Manager richieste, incluse le procedure per ambienti ibridi o dispositivi edge, se applicabili. Per ulteriori informazioni, consulta [Configurazione di Systems Manager](#). Per le macchine Rocky Linux, è necessario anche installare manualmente SSM Agent. Per ulteriori informazioni, consulta [Installazione manuale di SSM Agent su istanze Rocky Linux](#). Per le istanze Amazon Elastic Compute Cloud (Amazon EC2) di Windows Server 2022, SSM Agent è installato per impostazione predefinita.

[Come consentire ad Automation di adattarsi alle esigenze di simultaneità e visualizzare i relativi parametri di utilizzo](#)

Ora puoi consentire ad Automation di modificare automaticamente la quota di automazione simultanea e visualizzare le metriche di utilizzo dell'automazione pubblicate su CloudWatch. Per ulteriori informazioni sulla simultaneità adattiva, consulta [Adattamento di Automazione alle proprie esigenze di simultaneità](#). Per ulteriori informazioni su come visualizzare le metriche di utilizzo dell'automazione, consulta [Monitoring Automation with Amazon CloudWatch](#).

27 gennaio 2022

[Come consentire ad Automation di adattarsi alle esigenze di simultaneità e visualizzare i relativi parametri di utilizzo](#)

Ora puoi consentire ad Automation di modificare automaticamente la quota di automazione simultanea e visualizzare le metriche di utilizzo dell'automazione pubblicate su CloudWatch. Per ulteriori informazioni sulla simultaneità adattiva, consulta [Adattamento di Automazione alle proprie esigenze di simultaneità](#). Per ulteriori informazioni su come visualizzare le metriche di utilizzo dell'automazione, consulta [Monitoring Automation with Amazon CloudWatch](#).

27 gennaio 2022

[Documenti di Systems Manager organizzati per categorie](#)

I documenti di Systems Manager di proprietà di Amazon sono ora organizzati per tipo e categorie per aiutarti nella ricerca.

13 gennaio 2022

[Creare e richiamare integrazioni relative ad Automation](#)

Ora è possibile inviare messaggi utilizzando webhook durante un'automazione creando un'integrazione. Le integrazioni possono essere richiamate durante un'automazione utilizzando la nuova operazione `aws:invokeWebhook` nel runbook. Per ulteriori informazioni sulla creazione di integrazioni, consulta [Creazione di integrazioni webhook per Automazione](#). Per ulteriori informazioni sull'operazione `aws:invokeWebhook`, consulta [aws:invokeWebhook: richiamo dell'integrazione di un webhook di Automazione](#).

13 gennaio 2022

[Funzionalità non disponibili  
nella versione new Regione  
AWS](#)

Le seguenti funzionalità di Systems Manager al momento non sono disponibili nella nuova Regione Asia Pacifico (Giacarta).

13 dicembre 2021

- Application Manager
- Change Calendar
- Change Manager
- Explorer
- Fleet Manager
- Strumento di gestione degli incidenti
- Quick Setup

### [Visualizzazione dei dettagli sui costi delle risorse per un'applicazione](#)

Application Manager è integrato con Gestione costi e fatturazione AWS il widget Cost Explorer. Dopo aver abilitato Esploratore dei costi nella console di gestione fatturazione e costi, il widget Esploratore dei costi in Application Manager mostra i dati di costo per una specifica applicazione o componente dell'applicazione non container. È possibile utilizzare i filtri nel widget per visualizzare i dati dei costi in base a diversi periodi di tempo, granularità e tipi di costo in un grafico a barre o a linee. Per ulteriori informazioni, consulta [Visualizzazione delle informazioni generali relative a un'applicazione](#).

7 dicembre 2021

### [Gestisci i processi utilizzando Fleet Manager](#)

È ora possibile utilizzare Fleet Manager per gestire i processi sui nodi. Per ulteriori informazioni, consulta [Utilizzo degli stack](#).

06 dicembre 2021

### Cambio terminologico: le istanze gestite sono ora nodi gestiti

Con il supporto per i dispositivi AWS IoT Greengrass principali, la frase istanza gestita è stata modificata in nodo gestito nella maggior parte della documentazione di Systems Manager. La console di Systems Manager, le chiamate API, i messaggi di errore e i documenti SSM continuano a utilizzare il termine istanza.

29 novembre 2021



## Supporto per dispositivi edge

29 novembre 2021

Systems Manager supporta le seguenti configurazioni di dispositivi edge.

- **AWS IoT Greengrass:**  
Systems Manager ora supporta qualsiasi dispositivo configurato AWS IoT Greengrass ed esegue il software AWS IoT Greengrass Core. Per integrare i dispositivi AWS IoT Greengrass principali, è necessario creare un ruolo di servizio AWS Identity and Access Management (IAM). È inoltre necessario utilizzare la AWS IoT Greengrass console per l'implementazione SSM Agent come AWS IoT Greengrass componente sui dispositivi. Per ulteriori informazioni, consulta [Configurazione AWS Systems Manager per dispositivi edge](#).
- **Dispositivi edge in un ambiente ibrido:** Systems Manager supporta anche i dispositivi AWS IoT Core e i dispositivi non AWS IoT dopo averli configurati come macchine locali. Per integrare i dispositivi, è necessario creare un ruolo di servizio IAM,

creare un'attivazione del nodo gestito per un ambiente ibrido e installare manualmente SSM Agent sui dispositivi. Per ulteriori informazioni, vedere [Configurazione AWS Systems Manager per ambienti ibridi](#)

[Collegati all'istanza gestita tramite desktop remoto.](#)

È ora possibile utilizzare Fleet Manager per connettersi a istanze Windows gestite mediante Remote Desktop Protocol (RDP). Queste sessioni Desktop remoto basate su Amazon DCV offrono connessioni sicure alle istanze direttamente dal browser. Per ulteriori informazioni, consulta [Connessione tramite Remote Desktop](#).

23 novembre 2021

[Specifica la durata massima della sessione e fornire i motivi delle sessioni](#)

Ora, è possibile specificare una durata massima della sessione per tutte le sessioni Session Manager in un Regione AWS nel tuo Account AWS. Quando una sessione raggiunge la durata specificata, viene terminata. Ora è possibile anche aggiungere un motivo all'avvio di una sessione. Per ulteriori informazioni, consulta [Specifica della durata della sessione massima](#).

16 novembre 2021

### [Patch Manager ora supporta il sistema operativo Raspberry Pi OS](#)

È ora possibile utilizzare Patch Manager per applicare patch alle istanze Raspberry Pi OS. Patch Manager supporta l'applicazione di patch a Raspberry Pi OS 9 (Stretch) e 10 (Buster). Poiché il Debian-based sistema operativo Raspberry Pi OS è, ad esso si applicano molte delle stesse regole di patching. Debian Server Per ulteriori informazioni, consulta i seguenti argomenti:

16 novembre 2021

- [Come vengono selezionate le patch di sicurezza](#)
- [Come vengono installate le patch](#)
- [Come funzionano le regole di base delle patch Debian Server](#)

### [Accedi al portale della Knowledgebase di Red Hat](#)

Utilizza Fleet Manager per accedere al portale della Knowledgebase RHEL per trovare soluzioni, articoli, documentazione e video sull'utilizzo dei prodotti Red Hat. Per ulteriori informazioni, consulta [Accesso al portale della Knowledge base di Red Hat](#).

03 novembre 2021

[Modifica di blocco OpsItems](#)

OpsCenter ora supporta la modifica di blocco OpsItems. È possibile selezionare più OpsItems e modificare uno dei seguenti campi: Stato, Priorità, Gravità, Categoria. Per ulteriori informazioni, consulta [Modifica di OpsItems](#).

15 ottobre 2021

[Crea parametri di input che popolino le risorse AWS](#)

Ora è possibile creare parametri di input nei runbook Automation che popolano risorse in AWS nella Console di gestione AWS. Per informazioni, consulta [Creazione di parametri di input che popolano le risorse. AWS](#)

14 ottobre 2021

[Nuova opzione di interruzione della chiamata delle attività per le finestre di manutenzione](#)

Ora è possibile scegliere di bloccare l'avvio di qualsiasi nuova chiamata di attività dopo il raggiungimento del tempo limite specificato per una finestra di manutenzione. Per ulteriori informazioni, vedi [Assegnazione di attività a una finestra di manutenzione \(console\)](#).

13 ottobre 2021

## [Supporto Patch Manager per macOS 11.3.1 e 11.4 \(Big Sur\)](#)

1° ottobre 2021

Istanze Amazon Elastic Compute Cloud (Amazon EC2) per macOS 11.3.1 e 11.4 (Big Sur) ora possono essere applicati tramite patch Patch Manager. Questo si aggiunge al supporto esistente per macOS 10.14.x (Mojave) e 10.15.x (Catalina). Per informazioni sull'utilizzo delle Patch Manager, consulta [AWS Systems ManagerPatch Manager](#).

## [Approfondimenti sulle applicazioni in Application Manager](#)

Application Managers  
CloudWatch integra con Amazon Application Insights. Approfondimenti sulle applicazioni identifica e configura i log, i parametri chiave e gli allarmi tra le risorse dell'applicazione e stack tecnologico. Approfondimenti sulle applicazioni controlla in modo continuo i parametri e i log per rilevare e correlare anomalie ed errori. Quando il sistema rileva errori o anomalie, Application Insights genera CloudWatch eventi che puoi utilizzare e per impostare notifiche o intraprendere azioni. È possibile abilitare e visualizzare Approfondimenti sulle applicazioni nelle schede Panoramica e Monitoraggio su Application Manager. Per ulteriori informazioni su Application Insights, consulta [What is Amazon CloudWatch in Application Insights](#) nella Amazon CloudWatch User Guide.

21 settembre 2021

## [Importare eventi da altri calendari in Change Calendar](#)

È ora possibile importare gli eventi da un calendario di terza parte in un calendario in Change Calendar. In precedenza, ogni evento doveva essere inserito manualmente in un calendario. Dopo aver esportato un calendario da un provider di calendario di terza parte supportato a un file iCalendar (.ics), importarlo in Change Calendar e i relativi eventi sono inclusi nelle regole per il calendario aperto o chiuso in Systems Manager. I provider supportati includono Google Calendar, Microsoft Outlook e iCloud Calendar. Per ulteriori informazioni, consulta [Importazione e gestione di eventi da calendari di terze parti](#).

08 settembre 2021

### [Nuove funzionalità di assegnazione di tag e runbook in Application Manager](#)

I miglioramenti apportati ai tag includono la possibilità di aggiungere o eliminare tag da una risorsa specifica o da tutte le risorse in un'applicazione Application Manager. I miglioramenti del runbook includono la possibilità di visualizzare un elenco filtrato di runbook per un tipo di risorsa specifico o di avviare un runbook su tutte le risorse dello stesso tipo. Per ulteriori informazioni, consulta [Utilizzo dei tag in Application Manager](#) e [Utilizzo di runbook in Application Manager](#).

31 agosto 2021

### [Nuovo esempio: crea una richiesta di modifica utilizzando il AWS CLI](#)

Un esempio di creazione di una richiesta di modifica con AWS CLI è stato aggiunto al Change Manager capitolo. L'esempio utilizza il campione AWS-HelloWorldChangeTemplate di modifica modello e AWS-HelloWorld runbook:

20 agosto 2021

- [Creazione di richieste di modifica \(AWS CLI\)](#)



### [Nuova sezione: Utilizzare i parametri in Amazon EKS](#)

Una nuova sezione è stata aggiunta al capitolo Parameter Store. Questo argomento è una spiegazione passo per passo su come utilizzare i parametri nei cluster Amazon EKS. Per ulteriori informazioni, consulta [Utilizza parametri Parameter Store di Amazon Elastic Kubernetes Service](#).

19 agosto 2021

### [Hook del ciclo di vita Patch Manager aggiornati](#)

Patch Manager fornisce ora un hook del ciclo di vita, ovvero la possibilità di eseguire un documento di comando di Systems Manager, per un ulteriore punto durante un'operazione di applicazione di patch. Applica patch ora. Se pianifichi il riavvio dell'istanza programmata dopo l'esecuzione di Applica patch ora, è possibile specificare un hook del ciclo di vita da eseguire al termine del riavvio. Per ulteriori informazioni, consulta [Utilizzo degli hook del ciclo di vita "Applica patch ora"](#) e [Informazioni sul documento SSM AWS-RunPatchBaselineWithHooks](#).

09 agosto 2021

## [Auto-approvals ora supportato per Change Manager le richieste](#)

30 luglio 2021

È ora possibile configurare i modelli di modifica in Change Manager per supportare le approvazioni automatiche, il che significa che gli utenti con le autorizzazioni IAM necessarie possono scegliere di avviare la richiesta di modifica senza richiedere un'ulteriore approvazione. Gli utenti che hanno accesso ai modelli di approvazione automatica possono comunque scegliere di specificare gli approvatori, se lo desiderano. Per aiutarti a controllare i processi Change Manager, le approvazioni sono ancora necessarie per tutte le richieste durante i periodi di blocco delle modifiche. Per ulteriori informazioni, consulta i seguenti argomenti:

- [Creazione di modelli di modifica](#)
- [Creazione di richieste di modifica](#)
- [Prova il modello di Hello World modifica AWS gestito](#)

## [OpsCenterInformazioni dettagliate operative](#)

OpsCenter effettua un'analisi automatica di OpsItems nel tuo account e genera approfondimenti. Una panoramica include informazioni per aiutarti a capire quanti duplicati OpsItems sono presenti nel tuo account e quali fonti li stanno creando. Gli approfondimenti forniscono inoltre best practice consigliate e runbook Automation per risolvere gli OpsItems duplicati. Per ulteriori informazioni, consulta [Utilizzo di informazioni dettagliate operative](#).

13 luglio 2021

## [Visualizzare le istanze arrestate in Fleet Manager](#)

È ora possibile visualizzare quali istanze sono running e quali istanze sono stopped dalla console di Fleet Manager. Per ulteriori informazioni, consulta [AWS Systems ManagerFleet Manager](#).

12 luglio 2021

## [Nuovo argomento: Creazione di runbook Automation](#)

Un nuovo argomento [Creazione di runbook Automation](#), fornisce indicazioni ed esempi narrativi su come creare contenuti per runbook Automation personalizzati.

08 luglio 2021

## [AWS CloudFormation creazione di stack e template in Application Manager](#)

Application Manager ti aiuta a fornire e gestire le risorse per le tue applicazioni integrandoti con [CloudFormation](#). Puoi creare, modificare ed eliminare CloudFormation modelli e stack in. Application Manager include anche una libreria di modelli in cui è possibile clonare, creare e archiviare modelli. Application Manager CloudFormation visualizza le stesse informazioni sullo stato corrente di uno stack. I modelli e gli aggiornamenti dei modelli vengono archiviati in Systems Manager fino al provisioning dello stack, momento in cui vengono visualizzate anche le modifiche CloudFormation. Per ulteriori informazioni, vedere [Lavorare con CloudFormation Stacks in Application Manager](#).

08 luglio 2021

## [Nuovo argomento: Ruota automaticamente le chiavi private per SSM Agent sulle istanze ibride](#)

Un nuovo argomento [Impostazione della rotazione automatica della chiave privata](#) fornisce istruzioni su come rafforzare la posizione di sicurezza configurando SSM Agent per ruotare automaticamente la chiave privata dell'ambiente ibrido.

15 giugno 2021

### [Session Managerplugin per la AWS CLI versione 1.2.205.0](#)

È AWS CLI stata rilasciata una nuova versione del Session Manager plugin per. Per ulteriori informazioni, consulta [Cronologia di rilascio e della versione più recente del plugin Session Manager.](#)

10 giugno 2021

### [Nuovi ruoli collegati al servizio IAM](#)

Quando abiliti le informazioni dettagliate operative di OpsCenter, Systems Manager crea un nuovo ruolo collegato ai servizi AWS Identity and Access Management (IAM) chiamato `AWSSSMOpsInsightsServiceRolePolicy`. Per ulteriori informazioni su questo ruolo, vedere [Utilizzo dei ruoli per creare informazioni operative OpsItems in Systems ManagerOpsCenter: AWSSSMOpsInsightsServiceRolePolicy](#).

09 giugno 2021

### [NovitàPatch ManagerRisoluzione dei problemi di contenuto per Linux](#)

Un nuovo argomento [Errori durante l'esecuzioneAWS-RunPatchBaseline Su Linux](#), fornisce descrizioni e soluzioni per diversi problemi che potrebbero verificarsi durante l'applicazione di patch a istanze gestite con sistemi operativi Linux.

08 giugno 2021

[Supporto migliorato per le attività delle finestre di manutenzione che non richiedono destinazioni specificate \(console\)](#)

28 maggio 2021

È ora possibile creare i processi della finestra di manutenzione nella console senza dover specificare una destinazione nell'attività se non è necessaria. In precedenza, questa opzione era disponibile solo quando si utilizzava l'API AWS CLI or. Questa opzione si applica all'automazione e ai tipi di AWS Step Functions attività. AWS Lambda Ad esempio, se crei un processo di Automazione e le risorse da aggiornare sono specificate nei parametri del documento di Automazione, non dovrai più specificare una destinazione nel processo stesso. Per ulteriori informazioni, consulta [Registrazione delle attività della finestra di manutenzione senza destinazioni](#), [Assegnazione di attività a una finestra di manutenzione \(console\)](#) e [Schedule automations with maintenance windows](#) (Pianificazione delle automazioni con finestre di manutenzione).

[Riposizionamento del documento di riferimento ai runbook di Automazione](#)

Il documento di riferimento al runbook di Automazione è stato spostato in una nuova posizione. Per ulteriori informazioni, consulta [Documentazione di riferimento ai runbook Systems Manager Automation](#).

10 maggio 2021

[Strumento di gestione degli incidenti AWS Systems Manager avvio](#)

Incident Manager è una console di gestione degli incidenti progettata per aiutare gli utenti a mitigare e ripristinare gli incidenti che interessano le loro applicazioni AWS ospitate. Per ulteriori informazioni, consulta la [Guida per l'utente di Strumento di gestione degli incidenti AWS Systems Manager](#).

10 maggio 2021

[State Manager supporta Change Calendar](#)

È ora possibile specificare i nomi Change Calendar delle risorse Amazon (ARN) quando crei o aggiorni un'associazione State Manager. State Manager applica le associazioni solo quando il calendario delle modifiche è aperto, non quando è chiuso. Per ulteriori informazioni, consulta [Creazione di associazioni e Modifica e creazione di una nuova versione di un'associazione](#).

06 maggio 2021

## [Clonazione di documenti di Systems Manager](#)

Utilizzando la console Documenti di Systems Manager è ora possibile copiare il contenuto da un documento esistente a un nuovo documento che è possibile modificare. Per ulteriori informazioni, consulta [Clonazione di un documento SSM](#).

04 maggio 2021

## [Integra Security Hub CSPM con e ExplorerOpsCenter](#)

Ora puoi integrare Explorer e con. OpsCenter AWS Security Hub CSPM Security Hub CSPM offre una visione completa dello stato della sicurezza AWS e consente di verificare l'ambiente rispetto agli standard e alle best practice del settore della sicurezza. Se integrato con Explorer, puoi visualizzare i risultati della sicurezza nel widget Security Hub CSPM sulla dashboard. Explorer Se integrato con OpsCenter, è possibile creare risultati CSPM OpsItems per Security Hub. Per ulteriori informazioni, vedere [Ricezione di risultati da AWS Security Hub CSPM in Explorer](#) e [Ricezione di risultati da AWS Security Hub CSPM in. OpsCenter](#)

27 aprile 2021



Nuovo argomento: Convenzioni dei documenti

È stato aggiunto un nuovo argomento per consentire agli utenti di comprendere le convenzioni tipografiche comuni della Guida per l'utente di AWS Systems Manager . Per ulteriori informazioni, vedi [Convenzioni dei documenti](#).

21 aprile 2021

Argomento aggiornato: Informazioni sull'applicazione di patch rilasciata da Microsoft su Windows Server

L'argomento [Informazioni sull'applicazione di patch alle applicazioni rilasciate da Microsoft in data Windows Server](#) odierna chiarisce che, per Patch Manager poter applicare patch alle applicazioni rilasciate da Microsoft sulle istanze Windows Server gestite, l'opzione di aggiornamento di Windows Dammi aggiornamenti per altri prodotti Microsoft quando aggiorni Windows deve essere consentita sull'istanza.

12 Aprile 2021

[Riorganizzazione della documentazione di riferimento al runbook di Automazione](#)

Per facilitare la ricerca dei runbook necessari e la navigazione del documento di riferimento in modo più efficiente, è stato riorganizzato il contenuto nel documento di riferimento al runbook di Automazione in base al relativo Servizio AWS. Per visualizzare queste modifiche , consulta [Documento di riferimento ai runbook di Automazione di Systems Manager](#).

12 Aprile 2021

### [Patch Manager: generazione di report sulla conformità delle patch .csv](#)

Patch Manager ora supporta la possibilità di generare report sulla conformità delle patch per le istanze e di salvare il report in un bucket S3 di tua scelta in formato .csv. Quindi, utilizzando uno strumento come [Amazon Quick](#), puoi analizzare i dati del rapporto di conformità delle patch. È possibile generare un report sulla conformità delle patch per una singola istanza o per tutte le istanze del proprio Account AWS. È possibile generare un rapporto una tantum su richiesta o impostare una pianificazione per la creazione automatica dei rapporti. È possibile anche specificare un argomento Amazon Simple Notification Service per fornire notifiche quando viene generato un report. Per ulteriori informazioni, consulta [Generazione di report sulla conformità delle patch CSV](#).

09 aprile 2021

### [EliminaParameter StoreEtichette dei parametri](#)

È ora possibile eliminare Parameter Store etichette dei parametri utilizzando la console di Systems Manager o la AWS CLI. Per ulteriori informazioni, consulta [utilizzo di etichette per parametri](#).

06 aprile 2021

[Pianificazione del riavvio delle istanze quando si utilizza Applica patch ora](#)

Patch Manager ora supporta la pianificazione di un tempo per il riavvio delle istanze dopo l'installazione delle patch utilizzando la funzionalità Applica patch ora. Ciò si aggiunge alle opzioni esistenti per riavviare le istanze solo se necessario per completar e l'installazione di una patch o per saltare tutti i riavvii dopo l'operazione di applicazione delle patch. Per informazioni, consulta [Applicazione di patch a istanze on demand](#).

1° aprile 2021

[Nuovo argomento: Scopri parametri pubblici](#)

Parameter Store i parametri pubblici possono ora essere trovati utilizzando la console o Systems Manager. AWS CLI Per ulteriori informazioni, consulta [Trovare parametri pubblici](#).

1° aprile 2021

[Aggiornamenti Applica patch ora: archivia i log in S3 ed esegui gli hook del ciclo di vita](#)

Quando si esegue l'operazione Applica patch ora di Patch Manager, è possibile scegliere un bucket S3 in cui archiviare in automatico i log di applicazione di patch. Inoltre, è possibile scegliere di eseguire i documenti di comando di Systems Manager (documenti SSM) come hook del ciclo di vita in tre punti durante l'operazione: Prima dell'installazione, Dopo l'installazione, e All'uscita. Per ulteriori informazioni, consulta [Applicazione di patch a istanze on demand](#).

31 marzo 2021

[Systems Manager ora segnala le modifiche alle politiche AWS gestite](#)

A partire dal 24 marzo 2021, le modifiche alle politiche gestite sono riportate nell'argomento [Systems Manager Aggiornamenti alle politiche AWS gestite](#). La prima modifica elencata è l'aggiunta del supporto per lo Explorer strumento di segnalazione OpsData e OpsItems per più account e regioni.

24 marzo 2021

[Explorer consente automaticamente la sincronizzazione dei dati delle risorse da tutte le OpsData fonti in base agli account in AWS Organizations](#)

Quando si crea una sincronizzazione dei dati delle risorse, se si sceglie una delle AWS Organizations opzioni, Systems Manager consente automaticamente tutte le OpsData fonti selezionate Regioni AWS per tutte le fonti Account AWS presenti nell'organizzazione (o nelle unità organizzative selezionate). Ciò significa, ad esempio, che anche se non hai consentito Explorer l'accesso e Regione AWS se selezioni un' AWS Organizations opzione per la sincronizzazione dei dati delle risorse, Systems Manager effettua automaticamente la raccolta OpsData da quella regione. Per ulteriori informazioni, consulta [Informazioni sulle sincronizzazioni dei dati delle risorse di più account e regioni](#).

24 marzo 2021

[Systems Manager Automation fornisce una nuova variabile di sistema per i runbook](#)

Con la nuova variabile di `global:AWS_PARTITION` sistema, puoi specificare la AWS partizione in cui si trova una risorsa durante la creazione dei runbook. Per ulteriori informazioni, consulta [variabili del sistema di automazione](#).

18 marzo 2021

### [Consenti più livelli di approvazione perChange Managerrichieste di modifica](#)

Quando crei un modello di modifica Change Manager, è ora possibile richiedere che più di un livello di approvatori concedano l'autorizzazione per l'esecuzione di una richiesta di modifica. Ad esempio, è possibile richiedere ai revisori tecnici di approvare prima una richiesta di modifica creata da un modello di modifica e quindi richiedere un secondo livello di approvazione da parte di uno o più manager. Per ulteriori informazioni consulta [creazione di modelli di modifica](#).

04 marzo 2021

### [Patch Manager ora supporta Oracle Linux 8.x](#)

È ora possibile utilizzare Patch Manager per applicare patch alle istanze di Oracle Linux 8.x, attraverso la versione 8.3. Per ulteriori informazioni, consulta i seguenti argomenti:

1 marzo 2021

- [Come vengono selezionate le patch di sicurezza](#)
- [Come vengono installate le patch](#)
- [Funzionamento delle baseline delle patch in Oracle Linux](#)

[OpsCenter Visualizza altri OpsItems per una risorsa selezionata](#)

Per aiutarti a esaminare i problemi e fornire un contesto per un problema, puoi visualizzare un elenco di risorse OpsItems specifici e. AWS Nell'elenco vengono visualizzati lo stato, la gravità e il titolo di ogni OpsItem. L'elenco include anche collegamenti profondi a ogni OpsItem. Per ulteriori informazioni, consulta [Visualizzazione di altri OpsItems per una risorsa specifica](#).

1° marzo 2021

[Definire le preferenze di applicazione di patch in runtime](#)

È ora possibile definire le preferenze di applicazione di patch in runtime utilizzando la funzionalità di sostituzione della baseline. Per ulteriori informazioni, vedere [Utilizzo del BaselineOverride parametro](#).

25 febbraio 2021



## [Nuovo tipo di documento Systems Manager](#)

09 febbraio 2021

AWS CloudFormation i modelli possono ora essere archiviati come documenti di Systems Manager. L'archiviazione dei CloudFormation modelli come documenti di Systems Manager consente di sfruttare le funzionalità dei documenti di Systems Manager come il controllo delle versioni, il confronto del contenuto delle versioni e la condivisione con gli account. Per ulteriori informazioni, consulta [Documenti di Systems Manager AWS](#).

## Eseguire la patch delle istanze utilizzando gli hook

02 febbraio 2021

Il nuovo documento SSM [AWS-RunPatchBaselineWithHooks](#) fornisce hook che è possibile utilizzare per eseguire documenti SSM in tre punti durante il ciclo di applicazione di patch dell'istanza. Per informazioni su [AWS-RunPatchBaselineWithHooks](#) consultare [Informazioni su documento SSM AWS-RunPatchBaselineWithHooks](#). Per una procedura guidata di esempio di un'operazione di applicazione di patch che utilizza tutti e tre gli hook, consulta [Procedura guidata: aggiornamento delle dipendenze dell'applicazione, applicazione di patch a un'istanza ed esecuzione di un controllo dell'integrità specifico dell'applicazione](#).

[Nuovo argomento: convalida di server e macchine virtuali on-premises attraverso un'impronta digitale hardware](#)

SSM Agent verifica l'identificazione dei server e delle macchine virtuali on-premises e delle macchine virtuali registrate con il servizio utilizzando un'impronta digitale computata. L'impronta digitale è una stringa opaca, memorizzata nella Vault che l'agente passa a determinate API di Systems Manager. Per informazioni sull'impronta digitale hardware e istruzioni per la configurazione di una soglia di somiglianza per assistere nella verifica della macchina, vedere [Convalida dei server on-premise e delle macchine virtuali mediante un'impronta digitale hardware](#).

25 gennaio 2021

[Nuovo argomento: Documentazione di riferimento tecnica dell'SSM Agent](#)

Il riferimento [SSM Agent tecnico sull'argomento](#) raccoglie informazioni per aiutarvi a implementare AWS Systems Manager SSM Agent e comprendere come funziona l'agente. Questo argomento include una sezione completamente nuova, con aggiornamenti [SSM Agent continui di Regioni AWS](#).

21 gennaio 2021

## [SSM Agent su Windows Server2008](#)

A partire dal 14 gennaio 2020, Windows Server 2008 non è più supportato per gli aggiornamenti delle funzionalità o della sicurezza di Microsoft. Il Windows Server per AMIs 2008 includono SSM Agent, ma l'agente non viene più aggiornato per questo sistema operativo.

5 gennaio 2021

## [Supporto migliorato per le attività della finestra di manutenzione che non richiedono obiettivi specifici \(AWS CLI e solo API\)](#)

Ora puoi creare attività della finestra di manutenzione senza dover specificare un obiettivo nell'attività se non è richiesto (AWS CLI e solo API). Questo vale per l'automazione AWS Lambda e i tipi di AWS Step Functions attività. Ad esempio, se crei un processo di Automazione e le risorse da aggiornare sono specificate nei parametri dei runbook Automation, non dovrai più specificare una destinazione nel processo stesso. Per ulteriori informazioni, consulta [Registrazione delle attività della finestra di manutenzione senza destinazioni](#) e [Schedule automations with maintenance windows](#) (Pianificazione delle automazioni con finestre di manutenzione).

23 dicembre 2020

### [Nuove caratteristiche di Automation](#)

Una nuova proprietà condivisa è stata aggiunta ai runbook di Systems Manager Automation. La `onCancel` proprietà consente di specificare a quale passaggio deve procedere l'automazione se un utente annulla l'automazione. Per ulteriori informazioni, consulta [proprietà condivise da tutte le operazioni](#).

21 dicembre 2020

### [Nuovo argomento: Lavorare con le associazioni utilizzando IAM](#)

È stato aggiunto un nuovo argomento al capitolo State Manager di Systems Manager che descrive le best practice per la creazione di associazioni utilizzando IAM. Per ulteriori informazioni, consulta [Uso delle associazioni con IAM](#).

18 dicembre 2020

### [State Manager supporta ora più regioni e più account](#)

Ora è possibile creare o aggiornare le associazioni con più aree geografiche o account. Per ulteriori informazioni, consulta [Creazione di un'associazione](#).

15 dicembre 2020

## Nuovo strumento: Fleet Manager

Fleet Manager, uno strumento in AWS Systems Manager, è un'esperienza di interfaccia utente (UI) unificata che consente di gestire in remoto il parco di server in esecuzione in sede o in locale AWS. Con Fleet Manager è possibile visualizzare lo stato di integrità e delle prestazioni dell'intero parco istanze server da un'unica console. È inoltre possibile raccogliere dati da singole istanze per eseguire processi comuni di risoluzione dei problemi e gestione dalla console. Per informazioni, consulta [AWS Systems Manager Fleet Manager](#).

15 dicembre 2020

## Nuovo strumento: Change Manager

Amazon Web Services è stato rilasciato Change Manager, un framework di gestione delle modifiche aziendali per la richiesta, l'approvazione, l'implementazione e la creazione di report sulle modifiche operative alla configurazione e all'infrastruttura delle applicazioni. Da un singolo account amministratore delegato, se lo utilizzi AWS Organizations, puoi gestire le modifiche su più account. Account AWS Regioni AWS In alternativa, utilizzando un account locale, è possibile gestire le modifiche di un singolo Account AWS. Change ManagerUtilizzalo per gestire le modifiche alle AWS risorse e alle risorse locali. Per informazioni, consulta [AWS Systems Manager Change Manager](#).

15 dicembre 2020

## Nuovo strumento: Application Manager

Application Manager ti aiuta a indagare e risolvere i problemi relativi alle tue AWS risorse nel contesto delle tue applicazioni. Application Manager aggrega le informazioni operative provenienti da più strumenti Servizi AWS e Systems Manager in un unico strumento. Console di gestione AWS Per informazioni, consulta [AWS Systems Manager Application Manager](#).

15 dicembre 2020



## [AWS Systems Manager supporta istanze Amazon EC2 per macOS](#)

30 novembre 2020

In tandem con il rilascio del supporto Amazon Elastic Compute Cloud (Amazon EC2) per istanze macOS, Systems Manager ora supporta molte operazioni su istanze EC2 per macOS. Versioni supportate includono macOS 10.14.x (Mojave) e 10.15.x (Catalina). Per ulteriori informazioni, consulta i seguenti argomenti.

- Per informazioni sull'installazione di SSM Agent sulle istanze EC2 per macOS consulta [Installazione e configurazione di SSM Agent sulle istanze EC2 per macOS..](#)
- Per informazioni sull'applicazione di patch delle istanze EC2 per macOS consulta [Come vengono installate le patch e Creazione di una baseline delle patch personalizzata \(macOS\).](#)
- Per informazioni generali sul supporto per le istanze EC2 per macOS, consulta [Istanze Amazon EC2 Mac](#) nella Guida per l'utente di Amazon EC2.

[Pseudo parametri della finestra di manutenzione: nuovo tipo di risorsa supportato per {{TARGET\\_ID}} e {{RESOURCE\\_ID}}](#)

Un tipo di risorsa aggiuntivo è ora disponibile per l'utilizzo con gli pseudo parametri {{TARGET\_ID}} e {{RESOURCE\_ID}} . Ora è possibile utilizzare il tipo di risorsa AWS::RDS::DBCluster con entrambi questi pseudo parametri . Per informazioni sugli pseudoparametri della finestra di manutenzione, consulta la pagina [Utilizzo di pseudoparametri durante la registrazione delle attività della finestra di manutenzione](#).

27 novembre 2020

[Session Manager plugin per la versione 1.2.30.0 AWS CLI](#)

È AWS CLI stata rilasciata a una nuova versione del Session Manager plugin per. Per ulteriori informazioni, consulta [Cronologia di rilascio e versione più recente del Session Manager](#).

24 novembre 2020

[Nuovo argomento: Confronto delle versioni dei documenti SSM](#)

È ora possibile confrontare le differenze di contenuto tra le versioni dei documenti SSM nella console Documenti di Systems Manager. Per ulteriori informazioni, consulta [Confronto delle versioni dei documenti SSM](#).

24 novembre 2020

[Systems Manager ora supporta le policy endpoint VPC](#)

È ora possibile creare criteri per gli endpoint di interfaccia VPC per Systems Manager. Per ulteriori informazioni, consulta [Creazione di una policy di interfaccia per endpoint VPC](#).

18 novembre 2020

[Nuovo argomento: Specificare un valore di timeout della sessione inattiva](#)

È ora possibile specificare il tempo necessario per consentire a un utente di essere inattivo prima che una sessione finisca con Session Manager. Per ulteriori informazioni, consulta [Specificare un valore di timeout della sessione di inattività](#).

18 novembre 2020

[Novità funzionalità di registrazione di Session Manager](#)

Ora puoi inviare un flusso continuo di registri dei dati di JSON-formatted sessione ad Amazon CloudWatch Logs. Per ulteriori informazioni, consulta [Streaming dei dati delle sessioni con Amazon CloudWatch Logs](#).

18 novembre 2020

[Nuovo argomento: Verifica della firma dell'SSM Agent](#)

È ora possibile verificare e la firma crittografica del pacchetto di installazione per l'SSM Agent sulle istanze Linux. Per ulteriori informazioni, consulta [Schemi e funzionalità dei documenti SSM](#).

17 novembre 2020

### [Nuovo argomento: Informazioni sugli stati di automazione](#)

È stato aggiunto un nuovo argomento al capitolo Systems Manager Automation che descrive gli stati delle operazioni e delle automazioni. Per ulteriori informazioni, consulta [Informazioni sugli stati di automazione](#).

17 novembre 2020

### [Nuovi tipi di fonte per il plug-in aws:downloadContent](#)

Git e HTTP ora sono supportati come tipi di origine per il plug-in `aws:downloadContent`. Per ulteriori informazioni, consulta [aws:downloadContent](#).

17 novembre 2020

### [Nuova funzionalità di schema del documento di Systems Manager \(documento SSM\)](#)

Nei documenti SSM con la versione dello schema 2.2 o versioni successive, il parametro `precondition` supporta ora il riferimento ai parametri di input del documento. Per ulteriori informazioni, consulta [Schemi e funzionalità dei documenti SSM](#).

17 novembre 2020

[Nuova fonte di dati in Explorer:  
AWS Config](#)

Explorer ora mostra le informazioni sulla AWS Config conformità, incluso un riepilogo generale delle AWS Config regole conformi e non conformi, il numero di risorse conformi e non conformi e dettagli specifici su ciascuna di esse (quando si approfondisce una regola o una risorsa non conforme). Per ulteriori informazioni, consulta [Modifica delle origini dati dello Strumento di esplorazione Systems Manager](#).

11 novembre 2020

[Nuovo argomento: Esecuzione  
e di gruppi Auto Scaling con  
associazioni](#)

Una nuova sezione è stata aggiunta a State Manager, che descrive le procedure consigliate per la creazione di associazioni per l'esecuzione di gruppi Auto Scaling. Per ulteriori informazioni, consulta [Esecuzione dei gruppi con scalabilità automatica con associazioni](#).

10 novembre 2020

[Quick Setup supporta ora  
il targeting di un gruppo di  
risorse](#)

Quick Setup ora supporta la scelta di un gruppo di risorse come destinazione per il tipo di installazione locale. Per ulteriori informazioni, consulta [Scelta degli obiettivi per Quick Setup](#).

05 novembre 2020

[Patch Manager aggiunge supporto per Debian Server 10 LTS, Oracle Linux 7.9 LTS, e Ubuntu Server 20.10 STR](#)

04 novembre 2020

Ora è possibile utilizzare Patch Manager per patchare le istanze Debian Server 10 LTS, Oracle Linux 7.9 LTS e Ubuntu Server 20.10 STR. Per ulteriori informazioni, consulta i seguenti argomenti:

- [Prerequisiti di Patch Manager](#)
- [Come vengono selezionate le patch di sicurezza](#)
- [Come vengono installate le patch](#)
- [Funzionamento delle regole della baseline delle patch in Debian Server](#)
- [Funzionamento delle baseline delle patch in Oracle Linux](#)
- [Funzionamento delle regole delle baseline delle patch in Ubuntu Server](#)

### [Nuovo supporto per EventBridge AWS Systems ManagerChange Calendar](#)

Amazon EventBridge ora fornisce supporto per Change Calendar eventi nelle regole degli eventi. Quando lo stato di un calendario cambia, EventBridge può avviare l'azione mirata che hai definito come EventBridge regola. Per informazioni sull'utilizzo degli eventi EventBridge e di Systems Manager, vedere i seguenti argomenti.

04 novembre 2020

- [Configurazione EventBridge per gli eventi di Systems Manager](#)
- [Riferimento: modelli e tipi di EventBridge eventi Amazon per Systems Manager](#)

### [Configura CloudWatch per creare a OpsItems partire dagli allarmi](#)

Puoi configurare Amazon in modo CloudWatch da creare automaticamente un OpsItem in Systems Manager OpsCenter quando un allarme entra in ALARM uno stato. In questo modo puoi diagnosticare e risolvere rapidamente i problemi con AWS le risorse da un'unica console. Per ulteriori informazioni, consulta [Configurazione per la creazione CloudWatch a OpsItems partire dagli allarmi](#).

04 novembre 2020

## [Supporto per Ubuntu Server20.10](#)

AWS Systems Manager ora supporta la versione Ubuntu Server 20.10 a breve termine (STR). Per ulteriori informazioni, consulta i seguenti argomenti:

22 ottobre 2020

- [Sistemi operativi supportati](#)
- [Installazione dell'SSM Agent per un ambiente ibrido \(Linux\)](#)
- [Installazione manuale di SSM Agent sulle istanze Ubuntu Server](#)
- [Controllo dello stato di SSM Agent e avvio dell'agente](#)

## [Nuovo argomento: Consenti profili shell configurabili](#)

Ora è possibile consentire a profili di shell configurabili con Session Manager. Consentendo i profili di shell configurabili, è possibile personalizzare le preferenze all'interno di sessioni quali le preferenze della shell, le variabili di ambiente, le directory di lavoro ed eseguire più comandi all'avvio di una sessione. Per ulteriori informazioni, consulta [Consenti profili shell configurabili](#).

21 ottobre 2020



[I risultati di conformità delle patch ora segnalano quali CVE vengono risolte con quali patch](#)

Per la maggior parte dei sistemi Linux supportati, quando si visualizzano i risultati di conformità delle patch per le istanze gestite, i dettagli che è possibile visualizzare ora segnalano quali problemi comuni di vulnerabilità ed esposizione (CVE) vengono risolti con quali patch disponibili. Queste informazioni consentono di determinare con quale urgenza è necessario installare una patch mancante o non riuscita. Per informazioni, consultare [visualizzazione dei dati di conformità delle patch](#).

20 ottobre 2020

### [Supporto esteso per i metadati delle patch Linux](#)

Ora è possibile visualizzare molti dettagli sulle patch Linux disponibili in Patch Manager. È possibile scegliere di visualizzare i dati delle patch come architettura, epoch, versione, ID CVE, ID dell'Advisory, ID Bugzilla, repository e altro ancora. Inoltre, l'operazione API [DescribeAvailablePatches](#) è stata aggiornata per supportare i sistemi operativi Linux e il filtraggio in base a questi nuovi tipi di metadati delle patch disponibili. Per ulteriori informazioni, consulta i seguenti argomenti:

16 ottobre 2020

- [Visualizzazione delle patch disponibili](#)
- [DescribeAvailablePatches](#) e [Patch](#) nella Documentazione di riferimento API di AWS Systems Manager
- [describe-available-patches](#) nella AWS Systems Manager sezione del AWS CLI Command Reference

### [Session Managerplugin per la AWS CLI versione 1.2.7.0](#)

È AWS CLI stata rilasciata una nuova versione del Session Manager plugin per. Per ulteriori informazioni, consulta [Cronologia di rilascio e della versione più recente del plugin Session Manager](#).

15 ottobre 2020

[Nuovo argomento: Schema del documento di sessione](#)

Nuovo argomento [Schema del documento di sessione](#) descrive gli elementi dello schema di un documento di sessione. Queste informazioni consentono di creare documenti di sessione personalizzati in cui è possibile specificare le preferenze per i tipi di sessioni utilizzate con Session Manager.

15 ottobre 2020

[Nuovo argomento: Ricerca di testo libero per documenti SSM](#)

La casella di ricerca nella pagina Documenti di Systems Manager supporta ora la ricerca a testo libero. La ricerca a testo libero confronta il termine o i termini di ricerca immessi con il nome del documento in ogni documento SSM. Per ulteriori informazioni, consulta [Utilizzo della ricerca a testo libero](#).

15 ottobre 2020

[Nuovo argomento: Risoluzione dei problemi relativi alla disponibilità delle istanze gestite di Amazon EC2](#)

Nuovo argomento [Risoluzione dei problemi di disponibilità delle istanze gestite di Amazon EC2](#) ti aiuta a capire perché un'istanza Amazon EC2 che hai confermato è in esecuzione non è disponibile negli elenchi di istanze gestite disponibili in Systems Manager.

06 ottobre 2020

## [Parameter Store riorganizzazione dei capitoli](#)

1° ottobre 2020

Per aiutarti a trovare in modo più efficiente le informazioni di cui hai bisogno, abbiamo riorganizzato i contenuti nel capitolo Parameter Store della Guida per l'utente di AWS Systems Manager . La maggior parte dei contenuti è ora organizzata nelle sezioni [Configurazione di Parameter Store](#) e [Uso di Parameter Store](#). Inoltre, l'argomento [AWS Systems ManagerParameter Store](#) è stato ampliato per includere le seguenti sezioni:

- Quali sono i vantaggi di Parameter Store per la mia organizzazione?
- A chi è consigliato l'uso di Parameter Store?
- Quali sono le funzionalità di Parameter Store?
- Che cos'è un parametro?

## [Nuovi argomenti relativi alla conformità delle patch](#)

Per aiutarti a identificare le istanze gestite che non rispettano la conformità delle patch, comprendere i diversi tipi di scansioni di conformità delle patch e adottare le misure appropriate per rendere conformi le istanze, sono stati aggiunti gli argomenti seguenti.

24 settembre 2020

- [Identificazione di istanze non conformi](#)
- [Applicazione di patch a istanze non conformi](#)
- [Visualizzazione dei risultati di conformità delle patch](#)

## [SSM Agent versione 3.0](#)

Systems Manager ha lanciato una nuova versione di SSM Agent.

21 settembre 2020

[Argomenti nuovi e aggiornati:  
Amazon EventBridge sostituisce  
CloudWatch Events per la  
gestione degli eventi](#)

18 settembre 2020

CloudWatch Gli Events EventBridge sono lo stesso servizio e la stessa API di base, ma EventBridge forniscono più funzionalità ed è ora il modo preferito per gestire i tuoi eventi in AWS. (Le modifiche apportate in uno dei due CloudWatch sistemi o EventBridge si riflettono in ogni console). I riferimenti agli CloudWatch eventi e alle procedure esistenti nella Guida per l'AWS Systems Manager utente sono stati aggiornati per riflettere EventBridge il supporto. Inoltre, sono stati aggiunti i nuovi argomenti.

- [Monitoraggio degli eventi  
Systems Manager](#)
- [Configurazione EventBridge per gli eventi di Systems Manager](#)
- [Esempi di tipo di destinazione Systems Manager](#)
- [Riferimento: modelli e tipi di EventBridge eventi Amazon per Systems Manager](#)

## [Integrazione e AWS Security Hub CSPMPatch Manager](#)

17 settembre 2020

Ora puoi integrarti Patch Manager con AWS Security Hub CSPM. Security Hub CSPM offre una visione completa dello stato della sicurezza AWS e consente di verificare l'ambiente rispetto agli standard e alle best practice del settore della sicurezza. Se integrato con Patch Manager, Security Hub CSPM monitora lo stato di applicazione delle patch delle flotte dal punto di vista della sicurezza. Per ulteriori informazioni, consulta [Integrazione con Patch ManagerAWS Security Hub CSPM](#)

14 settembre 2020

Pseudoparametri della  
finestra di manutenzione:  
Nuovi tipi di risorse supportat  
i per {{TARGET\_ID}} e  
{{RESOURCE\_ID}}

Quando si registra un processo della finestra di manutenzione, è possibile utilizzare l'opzione `--task-invocation-parameters` per specificare i parametri univoci per ciascuno dei quattro tipi di task. È possibile anche fare riferimento a determinati valori utilizzando la sintassi degli pseudoparametri, ad esempio `{{TARGET_ID}}` e `{{RESOURCE_ID}}`. Durante l'esecuzione del processo della finestra di manutenzione vengono passati i valori corretti invece dei segnaposto degli pseudoparametri. Due tipi di risorse aggiuntivi sono ora disponibili per l'utilizzo con gli pseudoparametri `{{TARGET_ID}}` e `{{RESOURCE_ID}}`. È ora possibile utilizzare i tipi di risorse `AWS::RDS::DBInstance` e `AWS::SSM::ManagedInstance` con entrambi questi pseudo parametri. Per informazioni sugli pseudoparametri della finestra di manutenzione, consulta la pagina [Utilizzo di pseudoparametri durante la registrazione](#)



## [delle attività della finestra di manutenzione.](#)

### [Istanze patch su richiesta con la nuova opzione "Applica patch ora"](#)

09 settembre 2020

È ora possibile utilizzare e la console di Systems Manager per applicare patch alle istanze o cercare patch mancanti in qualsiasi momento. È possibile eseguire questa operazione senza dover creare o modificare una pianificazione oppure specificare le opzioni di configurazione dell'applicazione di patch complete per soddisfare le esigenze immediate di applicazione di patch. È sufficiente specificare se eseguire la scansione o l'installazione delle patch e identificare le istanze di destinazione per l'operazione. Patch Manager applica automaticamente la baseline delle patch predefinita corrente per i tipi di istanza e applica le opzioni relative alle best practice per il numero di istanze a cui è stata applicata la patch contemporaneamente e il numero di errori consentiti prima che l'operazione abbia esito negativo. Per ulteriori informazioni, consulta [Quote di istanze on demand](#).

### [Nuovo argomento: controllo dello stato di SSM Agent e avvio dell'agente](#)

Il nuovo argomento [Controllo dello stato di SSM Agent e avvio dell'agente](#) fornisce comandi per verificare se SSM Agent è in esecuzione su ciascun sistema operativo di supporto. Fornisce anche i comandi per avviare l'agente se non è in esecuzione.

07 settembre 2020

### [Patch Manager ora supporta Ubuntu Server 20.04 LTS](#)

È ora possibile utilizzare Patch Manager per applicare patch Ubuntu Server alle istanze di 20.04 LTS. Per ulteriori informazioni, consulta i seguenti argomenti:

31 agosto 2020

- [Come vengono selezionate le patch di sicurezza](#)
- [Come vengono installate le patch](#)
- [Funzionamento delle regole della baseline delle patch in Ubuntu Server](#)

### [Nuovo argomento per Casi d'uso e best practice](#)

È stato aggiunto un nuovo argomento per consentire agli utenti di comprendere rapidamente le differenze tra Maintenance Windows e State Manager. Per ulteriori informazioni, consulta [Scegliere tra State Manager e Maintenance Windows](#).

28 agosto 2020

### [Nuove caratteristiche di OpsCenter](#)

OpsCenter include nuove funzionalità che consentono di individuare ed eseguire rapidamente i runbook Automation per risolvere i problemi. Per ulteriori informazioni, consulta [Funzionalità del runbook di automazione in OpsCenter](#).

19 agosto 2020

### [Nuova fonte di dati in Explorer: casi Supporto AWS](#)

Explorer ora visualizza le informazioni sui Supporto casi. È necessario disporre di un account Enterprise o Business configurato con Supporto. Per ulteriori informazioni, consulta [Modifica delle origini dati di Systems Manager Explorer](#).

13 agosto 2020

### [Distributor fornisce ora un pacchetto di terze parti di Trend Micro](#)

Distributor include ora un pacchetto di terze parti di Trend Micro. È possibile utilizzare Distributor per installare l'agente Trend Micro Cloud One nelle istanze gestite. Trend Micro Cloud One ti aiuta a proteggere i tuoi carichi di lavoro nel cloud. Per ulteriori informazioni, consulta [AWS Distributor](#).

12 agosto 2020

[Il plug-in del documento  
aws:configurePackage  
include ora il parametro  
AdditionalArguments.](#)

Il plug-in `aws:configurePackage` per i documenti di comando Systems Manager ora supporta la fornitura di parametri aggiuntivi agli script (installazione, disinstallazione e aggiornamento) con il nuovo parametro `additionalArguments`. Per ulteriori informazioni, consulta l'argomento [aws:configurePackage](#).

11 agosto 2020

[AppConfigcontenuto spostato  
in una guida utente separata](#)

Le informazioni sugli AWS AppConfig sono state spostate in una guida per l'utente separata. Per ulteriori informazioni, consulta [What Is AWSAppConfig?](#) AppConfig ha anche una pagina di destinazione della [documentazione separata](#) con collegamenti alla guida per l'utente, al riferimento alle AppConfig API e a un nuovo AppConfig workshop.

03 agosto 2020

## [Quick Setup ora supporta AWS Organizations](#)

Quick Setup ora supporta la AWS Organizations configurazione rapida dei ruoli di sicurezza richiesti e degli strumenti di Systems Manager di uso comune su più account e regioni. Per ulteriori informazioni, consulta [AWS Systems Manager Quick Setup](#).

23 luglio 2020

## [Nuova origine dati in Explorer: conformità delle associazioni](#)

Explorer ora visualizza i dati di conformità delle associazioni da State Manager. Per ulteriori informazioni, consulta [Modifica delle origini dati dello Strumento di esplorazione Systems Manager](#).

23 luglio 2020

## [Nuovo documento di comando di Systems Manager per attivare e disattivare Kernel Live Patching](#)

Il documento AWS-ConfigureKernelLivePatching è ora disponibile per l'utilizzo con Run Command quando si desidera attivare o disattivare Kernel Live Patching su istanze Amazon Linux 2. Questo documento sostituisce la necessità di creare documenti di comando personalizzati per questi processi. Per informazioni, consulta [Utilizzo di Kernel Live Patching nelle istanze Amazon Linux 2](#)

22 luglio 2020

## [Quote di automazione aggiornate](#)

Le service quotas per la funzione Automazione sono state aggiornate, inclusa una coda separata per le automazioni di controllo della velocità. Per ulteriori informazioni, consulta l'articolo relativo alle [automazione AWS Systems Manager](#).

20 luglio 2020

[Specifica il numero di giorni di offset di pianificazione per una finestra di manutenzione utilizzando la console](#)

Utilizzando la console Systems Manager, è ora possibile specificare diversi giorni di attesa dopo la data e l'ora specificate da un'espressione CRON prima di eseguire una finestra di manutenzione. (In precedenza, questa opzione era disponibile solo quando si utilizzava un AWS SDK o uno strumento a riga di comando). Ad esempio, se l'espressione CRON pianifica una finestra di manutenzione per l'esecuzione il terzo martedì di ogni mese alle 23:30 - `cron(0 30 23 ? * TUE#3 *)` - e specifichi l'offset di pianificazione 2, la finestra verrà eseguita due giorni dopo alle 23:30. Per ulteriori informazioni, consulta [Espressioni Cron e della frequenza per Systems Manager](#) e [Specificare il numero di giorni di offset di pianificazione per una finestra di manutenzione](#).

17 luglio 2020

## [Aggiorna utilizzando PowerShell Run Command](#)

Per aiutarti ad eseguire l'aggiornamento PowerShell alla versione 5.1 sulle tue istanze R2 Windows Server 2012 e 2012, abbiamo aggiunto una procedura dettagliata alla Guida per l' AWS Systems Manager utente. Per ulteriori informazioni, consulta [Update using PowerShell Run Command](#)

30 giugno 2020

## [Patch Managersupporta ora CentOS 8.0 e 8.1](#)

È ora possibile utilizzare Patch Manager per applicare patch alle istanze CentOS 8.0 e 8.1. Per ulteriori informazioni, consulta i seguenti argomenti:

27 giugno 2020

- [Come vengono selezionate le patch di sicurezza](#)
- [Come vengono installate le patch](#)
- [Come installare SSM Agent su nodi Linux ibridi](#)



## [AppConfig si integra con AWS CodePipeline](#)

25 giugno 2020

AppConfig è un'azione di distribuzione integrata per AWS CodePipeline. CodePipeline è un servizio di distribuzione continua completamente gestito che consente di automatizzare le pipeline di rilascio per aggiornamenti rapidi e affidabili di applicazioni e infrastrutture. CodePipeline automatizza le fasi di creazione, test e distribuzione del processo di rilascio ogni volta che viene apportata una modifica al codice, in base al modello di rilascio definito. L'integrazione di AppConfig with CodePipeline offre i seguenti vantaggi. Per ulteriori informazioni, vedere [AppConfig Integrazione con CodePipeline](#).

- I clienti che gestiscono l'orchestrazione ora dispongono di un mezzo leggero per implementare le modifiche alla configurazione delle proprie applicazioni senza dover implementare l'intera base di codice.
- I clienti che desiderano utilizzarlo AppConfig per gestire le implementazioni

di configurazione ma sono limitati perché AppConfig non supportano il codice o l'archivio di configurazione corrente, ora hanno a disposizione opzioni aggiuntive. CodePipeline supporta AWS CodeCommit, GitHub, e BitBucket (solo per citarne alcuni).

### [Nuovo capitolo: Integrazioni di prodotti e servizi](#)

Per aiutarvi a capire come Systems Manager si integra con Servizi AWS altri prodotti e servizi, è stato aggiunto un nuovo capitolo alla Guida per l' AWS Systems Manager utente. Per ulteriori informazioni, consulta [Integrazioni di prodotti e servizi con Systems Manager](#).

23 giugno 2020

### [Riorganizzazione dei capitoli sull'automazione](#)

Per aiutarti a trovare ciò di cui hai bisogno, abbiamo riorganizzato gli argomenti nel capitolo Automation della Guida per l'utente di AWS Systems Manager . Ad esempio, le operazioni di Automation e i riferimenti ai runbook Automation sono ora sezioni di primo livello del capitolo. Per ulteriori informazioni, consulta [Automation di AWS Systems Manager](#).

23 giugno 2020

### [Specifica il numero di giorni di offset di pianificazione per una finestra di manutenzione](#)

Utilizzando uno strumento a riga di comando o AWS SDK, è ora possibile specificare diversi giorni di attesa dopo la data e l'ora specificate da un'espressione CRON prima di eseguire una finestra di manutenzione. Ad esempio, se l'espressione CRON pianifica una finestra di manutenzione per l'esecuzione il terzo martedì di ogni mese alle 23:30 - `cron(0 30 23 ? * TUE#3 *)` - e specifichi l'offset di pianificazione 2, la finestra verrà eseguita due giorni dopo alle 23:30. Per ulteriori informazioni, consulta [Espressioni Cron e della frequenza per Systems Manager](#) e [Specificare il numero di giorni di offset di pianificazione per una finestra di manutenzione](#).

19 giugno 2020

### [Supporto di Patch Manager per Kernel Live Patching sulle istanze Amazon Linux 2](#)

Kernel Live Patching for Amazon Linux 2 consente di applicare vulnerabilità di sicurezza e patch di bug critici a un kernel Linux in esecuzione, senza riavvii o interruzioni delle applicazioni in esecuzione. Ora è possibile abilitare la caratteristica e applicare le patch live del kernel utilizzando Patch Manager. Per informazioni, consulta [Utilizzo di Kernel Live Patching nelle istanze Amazon Linux 2](#)

16 giugno 2020

### [Patch Manager aumenta il supporto della versione di Oracle Linux](#)

Finora, Patch Manager supportava solo la versione 7.6 di Oracle Linux. Come indicato nei [prerequisiti di Patch Manager](#), il supporto ora include le versioni 7.5-7.8.

16 giugno 2020

[Scenario di esempio per utilizzare il parametro InstallOverrideList nelle operazioni di applicazione di patch](#)

Il nuovo argomento [Scenario di esempio per l'utilizzo del parametro InstallOverrideList](#) descrive una strategia per l'utilizzo del parametro `InstallOverrideList` nel documento `AWS-RunPatchBaseline` per applicare diversi tipi di patch a un gruppo di destinazione, in diverse pianificazioni della finestra di manutenzione, pur utilizzando una singola baseline delle patch.

11 giugno 2020

[Strategie di implementazione predefinite per AppConfig](#)

AppConfig ora offre strategie di implementazione predefinite. Per ulteriori informazioni, consulta [Creazione di una strategia di implementazione](#).

10 giugno 2020

[Patch Manager ora supporta  
Red Hat Enterprise Linux  
\(RHEL\) 7.8-8.2](#)

È ora possibile utilizzare Patch Manager per applicare patch alle istanze RHEL 7.8 - 8.2. Per ulteriori informazioni, consulta i seguenti argomenti:

- [Come vengono selezionate le patch di sicurezza](#)
- [Come vengono installate le patch](#)
- [Funzionamento delle regole della baseline delle patch in RHEL](#)
- [Installazione manuale di SSM Agent sulle istanze Red Hat Enterprise Linux](#)
- [Come installare SSM Agent su nodi Linux ibridi](#)

9 giugno 2020

### [Explorer supporta l'amministrazione delegata](#)

Se Explorer aggregi dati da più risorse Regioni AWS e Account AWS utilizzi la sincronizzazione dei dati delle risorse con AWS Organizations, ti consigliamo di configurare un amministratore delegato per Explorer. Un amministratore delegato migliora la sicurezza di Explorer limitando il numero di amministratori Explorer che possono creare o eliminare le sincronizzazioni dei dati delle risorse di più account e dell'area a un solo individuo. Inoltre, non è più necessario accedere all'account AWS Organizations di gestione per amministrare le sincronizzazioni dei dati delle risorse in Explorer. Per ulteriori informazioni, consulta [Configurazione di un amministratore delegato](#).

3 giugno 2020

### [Applica associazione State Manager solo all'intervallo Cron specificato successivo](#)

Se non desideri che un'associazione State Manager venga eseguita immediatamente dopo la creazione, è possibile scegliere l'opzione Applica associazione solo all'intervallo Cron specificato successivo nella console Systems Manager. Per ulteriori informazioni, consulta [Creazione di un'associazione](#).

3 giugno 2020

[Nuova fonte di dati in:  
ExplorerAWS Compute  
Optimizer](#)

Explorer ora visualizza i dati da AWS Compute Optimizer. Ciò include un conteggio delle istanze EC2 con Provisioning insufficiente e Provisioning eccessivo, risultati dell'ottimizzazione, dettagli sui prezzi su richiesta e suggerimenti per il tipo e il prezzo dell'istanza. Per ulteriori informazioni, consulta i dettagli per la configurazione AWS Compute Optimizer in [Configurazione dei servizi correlati](#).

26 maggio 2020

[Installazione degli aggiornamenti delle versioni secondarie di Windows e Linux con Patch Manager](#)

Il nuovo argomento [Tutorial: creazione di una baseline delle patch per l'installazione di Windows Service Pack \(console\)](#) illustra come creare una baseline delle patch dedicata esclusivamente all'installazione di Windows Service Pack. L'argomento [Creazione di una baseline delle patch personalizzata \(Linux\)](#) è stato aggiornato con informazioni sull'inclusione di aggiornamenti di versione secondaria per i sistemi operativi Linux nelle baseline delle patch.

21 maggio 2020



### [Parameter Store riorganizzazione dei capitoli](#)

Tutti gli argomenti relativi alla configurazione o all'impostazione delle opzioni per le operazioni Parameter Store sono stati consolidati nella sezione [Impostazioni Parameter Store](#) . Ciò riguarda gli argomenti [Gestione dei livelli dei parametri](#) e [Aumento di throughput diParameter Store](#), che sono stati trasferiti da altre parti del capitolo.

18 maggio 2020

### [Nuovo argomento per la creazione di stringhe di data e ora per l'interazione con le operazioni API di Systems Manager.](#)

Nel nuovo argomento [Creazione di stringhe di data e ora formattate per Systems Manager](#) viene descritto come creare stringhe di data e ora formattate per l'interazione con le operazioni API di Systems Manager .

13 maggio 2020

### [Informazioni sulle autorizzazioni per la crittografia dei parametri SecureString](#)

Il nuovo argomento [Limitazione dell'accesso ai parametri di Systems Manager mediante le politiche IAM](#) spiega la differenza tra la crittografia dei SecureString parametri utilizzando un AWS KMS key e l'utilizzo di quelli forniti da Chiave gestita da AWS AWS

13 maggio 2020

### [Patch Manager ora supporta i sistemi operativi Debian Server e Oracle Linux 7.6](#)

Ora è possibile utilizzare Patch Manager per applicare patch alle istanze Debian Server e Oracle Linux . Patch Manager supporta l'applicazione di patch per le versioni Debian Server 8.x e 9.x e Oracle Linux 7.6. Per ulteriori informazioni, consulta i seguenti argomenti:

- [Come vengono selezionate le patch di sicurezza](#)
- [Come vengono installate le patch](#)
- [Funzionamento delle regole della baseline delle patch in Debian Server](#)
- [Funzionamento delle regole della baseline delle patch in Oracle Linux](#)

### [Crea State Manager associazioni destinate a AWS Resource Groups](#)

Oltre a indirizzare i tag, le singole istanze e tutte le istanze presenti nel tuo Account AWS, ora puoi creare State Manager associazioni destinate alle istanze. AWS Resource Groups Per maggiori dettagli, consulta [Informazioni su destinazioni e controlli di velocità nelle associazioni di State Manager](#)

### [Nuovo tipo di dati `aws:ec2:image` in Parameter Store per convalidare ID AMI](#)

05 maggio 2020

Quando create un `String` parametro, ora potete specificare un tipo di dati `aws:ec2:image` per assicurarvi che il valore del parametro immesso sia un formato ID valido Amazon Machine Image (AMI). Il supporto per i formati di ID di AMI consente di evitare di aggiornare tutti gli script e i modelli con un nuovo ID ogni volta che l'AMI che si desidera utilizzare nei processi viene modificata. È possibile creare un parametro con il tipo di dati `aws:ec2:image` e, per il relativo valore, immettere l'ID di un'AMI. Si tratta dell'AMI da cui si desidera creare nuove istanze. Dopodiché dovrai fare riferimento a questo parametro nei modelli e nei comandi. Quando si è pronti per utilizzare un'AMI diversa, aggiornare il valore del parametro. Parameter Store convalida il nuovo ID AMI e non è necessario aggiornare gli script e i modelli. Per ulteriori informazioni, consulta [supporto dei parametri nativi per gli ID di Amazon Machine Image](#)

## [Gestione dei codici di uscita nei comandi Run Command](#)

Run Command consente di definire come i codici di uscita vengono gestiti negli 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. Tuttavia, utilizzando il seguente approccio, è possibile includere un'istruzione condizionale dello shell (interprete di comandi) per uscire dallo script se un comando prima di quello finale dà esito negativo. Alcuni esempi sono riportati nel nuovo argomento [Gestione dei codici di uscita nei comandi Run Command](#).

05 maggio 2020

## [Rilasciati nuovi parametri pubblici per le zone di disponibilità e le zone locali](#)

Sono stati distribuiti parametri pubblici per rendere disponibili a livello di programmazione informazioni sulle zone di disponibilità e le zone locali AWS . Questi sono oltre ai parametri pubblici dell'infrastruttura globale esistenti per Servizi AWS e Regioni AWS. Per ulteriori informazioni, vedere [Chiamare i parametri pubblici per Servizi AWS, regioni, endpoint, zone di disponibilità, zone locali e zone di lunghezza d'onda](#).

04 maggio 2020

[Nuova fonte di dati in:  
ExplorerAWS Trusted Advisor](#)

Explorer ora visualizza i dati da AWS Trusted Advisor. Ciò include lo stato dei controlli delle best practice e delle raccomandazioni nelle seguenti aree: ottimizzazione dei costi, sicurezza, tolleranza ai guasti, prestazioni e quote di servizio. Per ulteriori informazioni, consulta i dettagli per la configurazione Trusted Advisor in [Configurazione dei servizi correlati](#).

04 maggio 2020

## [Creazione di associazioni State Manager che eseguono ricette Chef](#)

È possibile creare associazioni 19 marzo 2020

State Manager che eseguono cookbook e ricette Chef utilizzando il documento `AWS-ApplyChefRecipes` . Questo documento offre i seguenti vantaggi per l'esecuzione di ricette Chef:

- Supporta più versioni di Chef (da Chef 11 a Chef 14).
- Installa automaticamente il software client Chef nelle istanze di destinazione.
- Opzionalmente esegue controlli di conformità di Systems Manager su istanze di destinazione e memorizza i risultati dei controlli di conformità in un bucket S3.
- Esegue più cookbook e ricette in un'unica esecuzione del documento.
- Opzionalmente esegue le ricette in modalità `why-run`, per mostrare quali ricette cambieranno nelle istanze di destinazione senza apportare modifiche.
- Facoltativamente applica attributi JSON personalizzati alle esecuzioni `chef-client` .

	Per ulteriori informazioni, consulta <a href="#">Creazione di associazioni che eseguono ricette Chef</a>	
<a href="#">Sincronizza i dati di inventari o da più bucket Amazon Account AWS S3 a un bucket Amazon S3 centrale</a>	È possibile sincronizzare i dati di inventario di Systems Manager da più bucket S3 Account AWS a un bucket S3 centrale. Gli account devono essere definiti in. AWS Organizations Per ulteriori informazioni, consulta <a href="#">Creazione di un Inventory Resource Data Sync per più account definiti in AWS Organizations</a> .	16 marzo 2020
<a href="#">Archiviare configurazioni AppConfig in Amazon S3</a>	In precedenza, AppConfig supportava solo le configurazioni delle applicazioni archiviate nei documenti Systems Manager (SSM) o nei parametri Parameter Store. Oltre a queste opzioni, AppConfig ora supporta l'archiviazione delle configurazioni in Amazon S3. Per ulteriori informazioni, consulta <a href="#">Informazioni sulle configurazioni archiviate in Amazon S3</a> .	13 marzo 2020
<a href="#">SSM Agent installato di default su Amazon ECS-optimized AMIs</a>	SSM Agent è ora installato di default su Amazon ECS-Optimized AMIs. Per ulteriori informazioni, consulta la pagina <a href="#">Uso di SSM Agent</a> .	25 febbraio 2020

## [Creare configurazioni AppConfig nella console](#)

AppConfig consente di creare una configurazione dell'applicazione nella console al momento della creazione di un profilo di configurazione. Per ulteriori informazioni, vedere [Creare una configurazione e un profilo di configurazione](#).

13 febbraio 2020

## [Auto-approve solo le patch rilasciate fino a una data specificata](#)

Oltre all'opzione per l'approvazione automatica delle patch per l'installazione un determinato numero di giorni dopo il rilascio, Patch Manager ora supporta la possibilità di approvare automaticamente solo le patch rilasciate entro una data specificata. Ad esempio, se specifichi il 07 luglio 2020 come data limite nella baseline delle patch, le patch rilasciate dall'8 luglio 2020 in poi non verranno installate automaticamente. Per ulteriori informazioni, consulta [Informazioni sulle baseline personalizzate e Creare una baseline delle patch \(console\)](#).

12 febbraio 2020



06 febbraio 2020

[Utilizzare lo pseudo parametro {{RESOURCE\\_ID}} nelle attività della finestra di manutenzione](#)

Quando registri un'attività della finestra di manutenzione, devi specificare i parametri univoci del tipo di attività. È possibile anche fare riferimento a determinati valori utilizzando la sintassi degli pseudoparametri, ad esempio `{{TARGET_ID}}` , `{{TARGET_TYPE}}` e `{{WINDOW_TARGET_ID}}` . Quando viene eseguita, l'operazione della finestra di manutenzione trasmette i valori corretti invece dei segnaposto degli pseudoparametri. Per supportare le risorse che fanno parte di un gruppo di risorse come una destinazione, è possibile utilizzare lo pseudoparametro `{{RESOURCE_ID}}` per passare valori per risorse quali tabelle DynamoDB, bucket S3 e altri tipi supportati. Per ulteriori informazioni, consulta i seguenti argomenti in [Tutorial: creazione e configurazione di una finestra di manutenzione \(AWS CLI\)](#):

- [Utilizzo degli pseudo parametri durante la registrazione delle attività della finestra di manutenzione](#)

- [Esempi: registrazione dei task con una finestra di manutenzione](#)

## [Rieseguire rapidamente i comandi](#)

05 febbraio 2020

Systems Manager include due opzioni che consentono di eseguire nuovamente un comando dalla pagina nella console. Run Command AWS Systems Manager Riesegui: questo pulsante consente di eseguire lo stesso comando senza apportarvi modifiche. Copia su nuovo: questo pulsante copia le impostazioni di un comando in un nuovo comando e ti dà la possibilità di modificare tali impostazioni prima di eseguirlo. Per ulteriori informazioni, consulta [Riesecuzione dei comandi](#).

### [Ripristino dal livello istanze avanzate al livello istanze standard](#)

Se in precedenza sono state configurate tutte le istanze on-premises in esecuzione e nell'ambiente ibrido per utilizzare il livello istanze avanzate, ora è possibile configurare rapidamente queste istanze per utilizzarle e il livello istanze standard. Il ripristino al livello delle istanze standard si applica a tutte le istanze ibride in una e una singola. Account AWS Regione AWS Il ripristino del livello istanze standard influisce sulla disponibilità di alcuni strumenti di Systems Manager. Per ulteriori informazioni, consulta [Ripristino dal livello istanze avanzate al livello istanze standard](#)

16 gennaio 2020

[Nuova opzione per ignorare il riavvio dell'istanza dopo l'installazione della patch](#)

In precedenza, le istanze gestite venivano sempre riavviate dopo l'installazione di Patch Manager. Un nuovo `RebootOption` parametro nel documento SSM AWS-RunPatchBaseline consente di specificare se si desidera che le istanze si riavviino automaticamente dopo l'installazione di nuove patch. Per ulteriori informazioni, consultate [Nome del parametro: RebootOption nell'argomento Informazioni sul documento SSM. AWS-RunPatchBaseline](#)

15 gennaio 2020

[Nuovo argomento: 'Esecuzione di PowerShell script su istanze Linux'](#)

Un nuovo argomento che descrive come utilizzare per Run Command eseguire PowerShell script su istanze Linux. Per ulteriori informazioni, consulta [Esecuzione di PowerShell script su istanze Linux.](#)

10 gennaio 2020

### [Aggiornamenti per "Configurare l'SSM Agent per l'utilizzo di un proxy"](#)

I valori da specificare durante la configurazione dell'SSM Agent per l'uso di un proxy sono stati aggiornati per riflettere le opzioni sia per i server proxy HTTP che per i server proxy HTTPS. Per ulteriori informazioni, consulta [Configurazione dell'SSM Agent per l'uso di un proxy](#).

09 gennaio 2020

[Il nuovo capitolo "Sicurezza" delinea le pratiche per la protezione delle risorse di Systems Manager](#)

24 dicembre 2019

Il nuovo capitolo [Sicurezza](#) nella Guida per l'utente di AWS Systems Manager consente di comprendere come applicare il [modello di responsabilità condivisa](#) quando si utilizza Systems Manager. I seguenti argomenti illustrano come configurare Systems Manager per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzarne altri Servizi AWS che ti aiutino a monitorare e proteggere e le tue risorse di Systems Manager.

 Note

Nell'ambito di questo aggiornamento, il capitolo della guida per l'utente relativo all'autenticazione e al controllo degli accessi è stato sostituito da una nuova sezione più semplice, [Gestione delle identità e degli accessi per AWS Systems Manager](#).

## [Nuovi runbook Automation personalizzati di esempio](#)

23 dicembre 2019

Un insieme di runbook Automation personalizzati di esempio è stato aggiunto alla guida per l'utente. In questi esempi viene illustrato come utilizzare varie operazioni di automazione per semplificare i processi di implementazione, risoluzione dei problemi e manutenzione e come facilitare la scrittura dei runbook di Automazione personalizzati. Per ulteriori informazioni, consulta [Esempi di runbook di Automazione personalizzati](#). È possibile anche visualizzare il contenuto del runbook di Automazione gestito da Amazon nella console Systems Manager. Per ulteriori informazioni, consulta [Documentazione di riferimento ai runbook Systems Manager Automation](#).

## [Supporto per Oracle Linux](#)

Systems Manager ora supporta Oracle Linux 7.5 e 7.7. Per informazioni sull'installazione manuale di SSM Agent nelle istanze EC2 per istanze Oracle Linux, consulta [Oracle Linux](#). Per informazioni sull'installazione dell'SSM Agent sui server Oracle Linux in un ambiente ibrido, consulta [Come installare SSM Agent su nodi Linux ibridi](#).

19 dicembre 2019



## [Avviare le sessioni Session Manager dalla console Amazon EC2](#)

18 dicembre 2019

È ora possibile avviare sessioni Session Manager dalla console Amazon Elastic Compute Cloud (Amazon EC2). L'utilizzo dei processi relativi alla sessione dalla console Amazon EC2 richiede autorizzazioni IAM diverse sia per gli utenti sia per gli amministratori. Puoi fornire le autorizzazioni per utilizzare e solo la Session Manager console, per utilizzare AWS CLI solo la console Amazon EC2 o per utilizzare tutti e tre gli strumenti. Per ulteriori informazioni, consulta i seguenti argomenti.

- [Policy IAM predefinite di avvio rapido per Session Manager](#)
- [Avvio di una sessione \(console Amazon EC2\)](#)

## [CloudWatch supporto per Run Command metriche e allarmi](#)

AWS Systems Manager ora pubblica metriche sullo stato dei Run Command comandi per CloudWatch, consentendoti di impostare allarmi in base a tali metriche. I valori di stato terminale relativi ai comandi per i quali è possibile monitorare i parametri includono Success, Failed e Delivery Timed Out. Per ulteriori informazioni, consulta [Monitoraggio delle Run Command metriche tramite Amazon. CloudWatch](#)

17 dicembre 2019

## [Nuovo strumento di Systems Manager: Change Calendar](#)

Utilizzare la Change Calendar di Systems Manager per specificare periodi di tempo (eventi) durante i quali si desidera limitare o impedire modifiche del codice (ad esempio da runbook Automation o funzioni AWS Lambda ) alle risorse. Change Calendar (Modifica calendario) è un nuovo tipo di documento di Systems Manager che memorizza i dati di [iCalendar 2.0](#) in formato di testo semplice. Per ulteriori informazioni, consulta [Modifica del calendario di AWS Systems Manager](#).

11 dicembre 2019

## Nuovo strumento Systems Manager: AWSAppConfig

25 novembre 2019

Utilizza AppConfig per creare, gestire e implementare rapidamente le configurazioni delle applicazioni. AppConfig supporta implementazioni controllate per applicazioni di qualsiasi dimensione. È possibile utilizzarlo AppConfig con applicazioni ospitate su istanze EC2 AWS Lambda, contenitori, applicazioni mobili o dispositivi IoT. Per evitare errori durante l'implementazione delle configurazioni delle applicazioni, AppConfig include validatori. Un validator e fornisce un controllo sintattico o semantico per assicurarsi che la configurazione da implementare funzioni come previsto. Durante l'implementazione di una configurazione, AppConfig monitora l'applicazione per assicurarsi che la distribuzione abbia esito positivo. Se il sistema rileva un errore o se l'implementazione attiva un allarme, AppConfig ripristina la modifica per ridurre al minimo l'impatto per gli utenti dell'applicazione. Per ulteriori informazioni, consulta [AWSAppConfig](#).

## [Nuovo strumento di Systems Manager: Systems Manager Explorer](#)

18 novembre 2019

AWS Systems Manager Explorer è una dashboard operativa personalizzabile che riporta informazioni sulle AWS risorse. Explorer mostra una vista aggregata dei dati operativi (OpsData) per te Account AWS e per tutti Regioni AWS. In Explorer, OpsData include metadati sulle istanze EC2, dettagli sulla conformità delle patch e elementi di lavoro operativi (). OpsItems Explorer fornisce un contesto su come OpsItems sono distribuite tra le unità aziendali o le applicazioni, come si evolvono nel tempo e come variano in base alla categoria. È possibile raggruppare e filtrare le informazioni Explorer per concentrarti sugli elementi rilevanti e per cui è necessario prendere misure. Quando si identificano problemi con priorità elevata, è possibile utilizzare OpsCenter di Systems Manager per eseguire runbook Automation e risolvere rapidamente tali problemi. Per informazioni, consultare, [AWS Systems Manager Explorer](#).

 Note

La configurazione per Systems Manager OpsCenter è integrata con la configurazione di Explorer. Se hai già configurato OpsCenter, è comunque necessario o completare l'installazione integrata per verificare le impostazioni e le opzioni. Se non è stato configurato OpsCenter, è possibile utilizzare l'installazione integrata per iniziare a utilizzare entrambi gli strumenti. Per ulteriori informazioni, consulta [Nozioni di base su Explorer e OpsCenter](#).

## [Funzionalità di ricerca dei parametri migliorate](#)

15 novembre 2019

Gli strumenti per la ricerca dei parametri ora semplificano la ricerca dei parametri in presenza di un numero elevato nell'account o quando non si ricorda il nome esatto di un parametro. Lo strumento di ricerca ora consente di filtrare per `contains`. In precedenza, gli strumenti di ricerca supportavano la ricerca dei nomi dei parametri solo da `equals` e `begins-with`. Per ulteriori informazioni, consulta [Ricerca dei parametri di Systems Manager](#).

[Nuovo Document Builder  
basato su console per  
Automazione | Supporto per  
l'esecuzione di script nelle fasi  
di Automazione](#)

14 novembre 2019

È ora possibile utilizzare Systems Manager Automation per creare e condividere playbook operativi standardizzati per garantire la coerenza tra gli utenti e. Account AWS Regioni AWS Con questa possibilità di eseguire script e aggiungere documentazione in linea ai runbook Automation utilizzando Markdown, è possibile ridurre gli errori ed eliminare i passaggi manuali come la navigazione delle procedure scritte nelle wiki e l'esecuzione dei comandi del terminale.

Per ulteriori informazioni, consulta i seguenti argomenti.

- [Procedura guidata: uso di Document Builder per la creazione di un runbook Automation personalizzato](#)
- [aws:executeScript](#) (Documentazione di riferimento delle operazioni di Automazione)
- [Creazione di runbook Automation mediante Document Builder](#)
- [Nuove funzionalità di automazione in Systems Manager](#) nel Blog di notizie AWS

## [Esecuzione di un aggiornamento del pacchetto sul posto con Distributor](#)

11 novembre 2019

In precedenza, quando si voleva installare un aggiornamento per un pacchetto con Distributor, l'unica scelta era quella di disinstallare l'intero pacchetto e reinstallare la nuova versione. Ora è possibile scegliere di eseguire un aggiornamento sul posto. Durante un aggiornamento sul posto, Distributor installa solo i file nuovi o modificati dall'ultima installazione, in base allo script di aggiornamento incluso nel pacchetto. Con questa opzione, l'applicazione pacchetto può rimanere disponibile e non essere messa offline durante l'aggiornamento. Per ulteriori informazioni, consulta i seguenti argomenti.

- [Creazione di un pacchetto](#)
- [Installazione o aggiornamento dei pacchetti](#)



### [Nuova funzione di aggiornamento automatico SSM Agent](#)

Con una sola azione, puoi configurare tutte le tue Account AWS istanze in modo che verifichino e scarichino automaticamente nuove versioni di SSM Agent. Per fare ciò, scegli Agent auto update nella pagina Managed instances della AWS Systems Manager console. Per informazioni, consulta [Automatizzazione degli aggiornamenti all'SSM Agent](#).

05 novembre 2019

### [Limita Session Manager l'accesso utilizzando i tag AWS forniti da](#)

È ora disponibile un secondo metodo per controllare l'accesso degli utenti alle operazioni di sessione. Questo nuovo metodo consente di creare policy di accesso IAM utilizzando tag di sessione forniti da AWS anziché utilizzare la variabile `{aws:username}`. L'utilizzo AWS di questi tag di sessione forniti consente alle organizzazioni che utilizzano ID federati di controllare l'accesso degli utenti alle sessioni. Per ulteriori informazioni, consulta [Autorizzazione degli utenti a terminare solo le sessioni da essi avviate](#).

02 ottobre 2019

[Nuovo documento SSM](#)  
[Command per applicare](#)  
[Playbook Ansible](#)

24 settembre 2019

È possibile creare associazioni State Manager che eseguono playbook Ansible utilizzando il documento AWS-Apply AnsiblePlaybooks . Questo documento offre i seguenti vantaggi per l'esecuzione di Playbook:

- Supporto per l'esecuzione di Playbook complessi
- Supporto per il download di Playbook da GitHub e Amazon Simple Storage Service (Amazon S3)
- Supporto per la struttura di Playbook compressa
- Registrazione migliorata
- Possibilità di specificare quale Playbook eseguire quando i Playbook sono raggruppati in bundle

Per ulteriori informazioni, consulta [Creazione di associazioni che eseguono playbook Ansible](#)

## [Supporto dell'inoltro alla porta per Session Manager](#)

Session Manager ora supporta le sessioni di inoltro alla porta. 29 agosto 2019

Il port forwarding consente di creare tunnel sicuri tra le istanze distribuite in sottoreti private, senza la necessità di avviare il servizio SSH sul server, aprire la porta SSH nel gruppo di sicurezza o utilizzare un bastion host. Analogamente ai tunnel SSH, il port forwarding consente di inoltrare il traffico tra il laptop alle porte aperte dell'istanza. Dopo aver configurato l'inoltro alla porta, è possibile connetterti alla porta locale e accedere all'applicazione server in esecuzione all'interno dell'istanza. Per ulteriori informazioni, consulta i seguenti argomenti:

- [Inoltro della porta tramite AWS Systems ManagerSession Manager](#) sul Blog di notizie AWS .
- [Avvio di una sessione \(inoltro alla porta\)](#)

## [Specificare un livello dei parametri predefinito o automatizzare la selezione del livello](#)

Ora è possibile specificare un livello dei parametri di default da utilizzare per le richieste di creazione o aggiornamento di un parametro che non specifica un livello. È possibile impostare il livello predefinito su parametri standard, parametri avanzati o una nuova opzione. Intelligent-Tiering Intelligent-Tiering valuta ogni PutParameter richiesta e crea un parametro avanzato solo quando richiesto. (I parametri avanzati sono necessari se la dimensione del valore del parametro è superiore a 4 KB, una policy dei parametri è associata al parametro o un massimo di 10.000 parametri supportati per il livello standard sono già stati creati per il livello standard). Per ulteriori informazioni sulla specificazione di un livello predefinito e sull'utilizzo Intelligent-Tiering, vedere [Specificazione di un livello di parametro predefinito.](#)

27 agosto 2019

[Sezione Lavorare con le associazioni aggiornata con CLI e procedure PowerShell](#)

La sezione Lavorare con le associazioni è stata aggiornata per includere la documentazione procedurale per la gestione delle associazioni utilizzando l' AWS CLI o. AWS Strumenti per PowerShell Per informazioni, consulta [Utilizzo delle associazioni in Systems Manager.](#)

26 agosto 2019

[Sezione relativa alle esecuzioni di Working with Automation aggiornata con CLI e procedure PowerShell](#)

La sezione Lavorare con le esecuzioni di automazione è stata aggiornata per includere la documentazione procedurale per l'esecuzione dei flussi di lavoro di automazione utilizzando o. AWS CLI AWS Strumenti per PowerShell Per informazioni, consulta [Uso delle esecuzioni di Automazione.](#)

20 agosto 2019

[OpsCenter si integra con](#)  
[Approfondimenti sulle](#)  
[applicazioni](#)

OpsCenter si integra con Amazon CloudWatch Application Insights for .NET e SQL Server. Ciò significa che è possibile creare automaticamente OpsItems per i problemi rilevati nelle applicazioni. Per informazioni su come configurare Application Insights per la creazione OpsItems, consulta Configurare, [configurare e gestire l'applicazione per il monitoraggio](#) nella Amazon CloudWatch User Guide.

07 agosto 2019

## [Nuova funzionalità della console: AWS Systems Manager Quick Setup](#)

07 agosto 2019

Quick Setup è una nuova caratteristica nella console Systems Manager che consente di configurare rapidamente diversi componenti di Systems Manager sulle istanze EC2. In particolare, Configurazione rapida consente di configurare i seguenti componenti sulle istanze scelte o di riferimento utilizzando tag:

- Un ruolo di profilo di istanza AWS Identity and Access Management (IAM) per Systems Manager.
- Un aggiornamento pianificato, bimensile di SSM Agent.
- Una raccolta pianificata di metadati di Inventory ogni 30 minuti.
- Una scansione giornaliera delle istanze per identificare le patch mancanti.
- Installazione e configurazione di un agente di Amazon CloudWatch.
- Un aggiornamento mensile pianificato dell'agente di Amazon CloudWatch.

Per ulteriori informazioni, consulta [Configurazione](#)

[rapida di AWS Systems  
Manager.](#)



## [Registrazione di un gruppo di risorse come una destinazione della finestra di manutenzione](#)

23 luglio 2019

Oltre a registrare le istanze gestite come destinazione di una finestra di manutenzione, ora puoi registrare un gruppo di risorse come destinazione della finestra di manutenzione. Maintenance Window supporta tutti i tipi di AWS risorse supportati i AWS Resource Groups tra cui `AWS::EC2::Instance`, `AWS::DynamoDB::Table`, `AWS::OpsWorks::Instance`, `AWS::Redshift::Cluster`, e altro. Con questa versione è anche possibile inviare comandi a un gruppo di risorse, ad esempio utilizzando la Run Command console o il AWS CLI [send-command](#) comando. Per ulteriori informazioni, consulta i seguenti argomenti:

- [Assegnazione di destinazioni a una finestra di manutenzione \(console\)](#)
- [Esempi: registrazione delle destinazioni con una finestra di manutenzione](#)
- [Uso di destinazioni e controlli di velocità per l'invio di comandi a un parco istanze](#)

[Creazione pacchetto  
semplificato e controllo delle  
versioni con AWS Systems  
Manager Distributor](#)

Distributor dispone di un nuovo flusso di lavoro di creazione pacchetti semplificato che è in grado di generare in automatico un manifesto del pacchetto, script e hash del file per tuo conto. È possibile inoltre utilizzare il flusso di lavoro semplificato quando aggiungi una versione a un pacchetto esistente.

22 luglio 2019

[Nuovo riquadro di categorie  
dei documenti per Automazio  
ne Systems Manager](#)

Systems Manager include un nuovo riquadro categorie documento quando si esegue l'automazione nella console. Utilizza questo riquadro per filtrare i runbook Automation in base al loro scopo.

18 luglio 2019

[Supporto per l'avvio di  
sessioni Session Manager  
utilizzando le credenziali  
utente del sistema operativo](#)

Per impostazione predefinita, le sessioni Session Manager vengono avviate utilizzando le credenziali di un account `ssm-user` generato dal sistema che viene creato su un'istanza gestita. Su computer Linux, è ora possibile avviare sessioni utilizzando le credenziali di un account del sistema operativo. Per ulteriori informazioni, consulta [Abilitazione del supporto Run As per istanze Linux](#).

09 luglio 2019

[Supporto per l'avvio di sessioni Session Manager tramite SSH](#)

È ora possibile utilizzare AWS CLI per avviare una sessione SSH su un'istanza gestita utilizzando Session Manager. Per informazioni sull'abilitazione delle sessioni SSH con Session Manager, consulta [\(Facoltativo\) Attivazione delle connessioni SSH mediante Session Manager](#). Per informazioni sull'avvio di una sessione SSH con Session Manager, consulta [Avvio di una sessione \(SSH\)](#).

09 luglio 2019

[Supporto per la modifica delle password su istanze gestite](#)

Ora è possibile ripristinare le password su computer che gestisci usando Systems Manager (istanze gestite). È possibile ripristinare la password utilizzando la console Systems Manager o la AWS CLI. Per ulteriori informazioni, consulta [Reimpostazione delle password nelle istanze gestite](#).

09 luglio 2019

## Revisioni a «Che cos'è AWS Systems Manager?»

Il contenuto introduttivo in [Che cos'è AWS Systems Manager?](#) è stato ampliato per fornire una descrizione maggiore del servizio e per rispecchiare gli strumenti di Systems Manager distribuiti di recente. Inoltre, per altri contenuti della sezione, sono stati creati argomenti specifici per aumentare la visibilità.

10 giugno 2019

## Nuovo strumento di Systems Manager: OpsCenter

06 giugno 2019

OpsCenter fornisce una posizione centrale in cui gli ingegneri operativi e i professionisti IT possono visualizzare, esaminare e risolvere gli elementi di lavoro operativi (OpsItems) relativi alle AWS risorse. OpsCenter è progettato per ridurre i tempi medi di risoluzione dei problemi che influiscono sulle AWS risorse. Questo strumento di Systems Manager aggrega e standardizza OpsItems su tutti i servizi, mentre fornisce dati investigativi contestuali su ogni OpsItem, OpsItems correlati e risorse correlate. OpsCenter fornisce, inoltre, runbook Systems Manager Automation utilizzabili per risolvere velocemente i problemi. È possibile specificare i dati ricercabili e personalizzati per ogni OpsItem. È inoltre possibile visualizzare i report di riepilogo generati in automatico su OpsItems in base allo stato e all'origine. Per ulteriori informazioni, consulta [AWS Systems Manager OpsCenter](#).

[Modifiche al riquadro di navigazione sinistro di Systems Manager nel Console di gestione AWS](#)

Il riquadro di navigazione sinistro di Systems Manager in Console di gestione AWS include nuove intestazioni, inclusa una nuova intestazione per Ops Center, che forniscono un raggruppamento più logico degli strumenti di Systems Manager.

06 giugno 2019

[Tutorial rivisto per la creazione e la configurazione di una finestra di manutenzione utilizzando AWS CLI](#)

La sezione [Tutorial: creazione e configurazione di una finestra di manutenzione \(AWS CLI\)](#) è stata riorganizzata in modo da fornire una procedura articolata in fasi semplici. È infatti possibile creare una singola finestra di manutenzione, identificare una singola destinazione e impostare l'esecuzione di un'operazione semplice da parte della finestra di manutenzione. Durante l'intera procedura verranno forniti esempi e informazioni che potrai utilizzare per creare comandi di registrazione di operazioni personalizzate, nonché informazioni su come utilizzare pseudoparametri quali `{{TARGET_ID}}` . Per ulteriori informazioni ed esempi, consulta i seguenti argomenti:

31 maggio 2019

- [Esempi: registrazione delle destinazioni con una finestra di manutenzione](#)
- [Esempi: registrazione delle operazioni con una finestra di manutenzione](#)
- [Informazioni sulle opzioni `register-task-with-maintenance-windows`](#)

- [Utilizzo degli pseudo parametri durante la registrazione delle attività della finestra di manutenzione](#)

### [Notifiche sugli aggiornamenti SSM Agent](#)

Per ricevere notifiche sugli aggiornamenti dell'SSM Agent, iscriviti alla pagina [Note di rilascio dell'SSM Agent](#) su GitHub.

24 maggio 2019

### [Ricevi notifiche o attiva le operazioni in base alle modifiche in Parameter Store](#)

L'argomento [Configura notifiche o attiva azioni in base Parameter Store agli eventi](#) ora ti aiuta a configurare EventBridge le regole di Amazon per rispondere alle modifiche in. Parameter Store È possibile ricevere notifiche o attivare altre operazioni quando si verifica uno qualsiasi dei seguenti casi:

22 maggio 2019

- Un parametro viene creato, aggiornato o eliminato.
- Una versione dell'etichetta del parametro viene creata, aggiornata o eliminata.
- Un parametro scade, sta per scadere o non è stato modificato in un determinato periodo di tempo.



[Modifiche importanti ai contenuti Configurazione e Nozioni di base](#)

15 maggio 2019

Abbiamo ampliato e riorganizzato i contenuti Configurazione e Nozioni di base nella Guida per l'utente di AWS Systems Manager . I contenuti di Configurazione sono stati divisi in due sezioni. Una sezione è incentrata sui processi per la configurazione di Systems Manager per configurare e gestire le proprie istanze EC2. L'altra è incentrata su processi per l'impostazione di Systems Manager per configurare e gestire i server on-premises e le macchine virtuali (VM) in un ambiente ibrido. Entrambe le sezioni ora presentano tutti gli argomenti di configurazione come fasi numerate principali, nell'ordine di completamento consigliato. Un nuovo capitolo Nozioni di base è destinato ad aiutare gli utenti finali a cominciare a utilizzare Systems Manager dopo il completamento dei processi di configurazione dell'account e del servizio.

- [Configurazione AWS Systems Manager](#)
- [Configurazione AWS Systems Manager per ambienti ibridi](#)

- [Guida introduttiva con AWS Systems Manager](#)

## [Includere patch per applicazioni Microsoft nelle baseline delle patch \(Windows\)](#)

7 maggio 2019

Patch Manager supporta ora gli aggiornamenti delle patch per applicazioni Microsoft su istanze Windows Server. In precedenza, erano supportate solo le patch per il sistema operativo Windows Server. Patch Manager fornisce due baseline delle patch predefinite per istanze Windows Server. La baseline delle patch AWS-WindowsPredefinedPatchBaseline-OS si applica solo a patch del sistema operativo. AWS-WindowsPredefinedPatchBaseline-OS-Applications si applica al sistema operativo Windows Server e alle applicazioni Microsoft su Windows. Per ulteriori informazioni sulla creazione di una baseline delle patch personalizzata che includa le patch per applicazioni Microsoft, consulta la prima procedura in [Creazione di una baseline delle patch predefinita](#). Inoltre, come parte di questo aggiornamento, vengono modificati i nomi delle baseline predefinite delle patch AWS fornite. Per ulteriori informazioni, consulta [Baseline predefinite](#).

[Esempi di registrazione degli obiettivi delle finestre di manutenzione utilizzando il AWS CLI](#)

Il nuovo argomento [Esempi: registrazione delle destinazioni con una finestra di manutenzione](#) fornisce tre comandi di esempio che illustrano modi diversi con i quali è possibile specificare le destinazioni per una finestra di manutenzione quando si utilizza AWS CLI. L'argomento illustra anche il caso d'uso migliore per ciascuno dei comandi di esempio.

3 maggio 2019

## [Aggiornamenti ad argomenti del gruppo di patch](#)

1 maggio 2019

L'argomento [Informazioni sui gruppi di patch](#) è stato aggiornato per includere una sezione su come le istanze gestite determinano la baseline delle patch appropriata da utilizzare durante le operazioni di applicazione di patch. Inoltre, sono state aggiunte le istruzioni per l'utilizzo della AWS CLI console di Systems Manager per aggiungere un gruppo di patch o PatchGroup tag alle istanze gestite e come aggiungere un gruppo di patch o una baseline PatchGroup di patch. Se sono presenti [tag consentiti nei metadati dell'istanza EC2](#), è necessario utilizzare **PatchGroup** (senza spazio). Per ulteriori informazioni, consulta [Creazione di un gruppo di patch](#) e [Aggiunta di un gruppo di patch a una baseline delle patch](#).

## Nuove caratteristiche di Parameter Store

25 aprile 2019

Parameter Store offre le seguenti nuove funzionalità:

- Parametri avanzati:  
Parameter Store ora consente di configurare i parametri individualmente per utilizzare un livello di parametri standard (il livello predefinito) o un livello di parametri avanzati. I parametri avanzati offrono una quota maggiore per il valore del parametro, una quota più elevata per il numero di parametri che è possibile creare per mano Account AWS e la possibilità di utilizzare Regione AWS politiche relative ai parametri. Per ulteriori informazioni sui parametri avanzati, consulta [Informazioni sui parametri avanzati di Systems Manager](#).
- Policy dei parametri:  
Le policy dei parametri consentono di gestire un set di parametri abilitando o l'assegnazione criteri specifici a un parametro, ad esempio una data di scadenza o il time to live. Le policy dei parametri sono particolarmente utili per forzare l'aggiorn

amento o l'eliminazione di password e dati di configurazione archiviati in Parameter Store. Le policy dei parametri sono disponibili solo per i parametri che utilizzano il piano parametri avanzati. Per ulteriori informazioni, consulta la sezione [Uso di policy di parametri](#).

- Throughput: più elevato: ora è possibile aumentare il throughput di Parameter Store fino a un massimo di 1.000 transazioni al secondo. Per ulteriori informazioni, consulta [Aumento del throughput di Parameter Store](#).

#### [Aggiornamenti alla sezione Automation](#)

La sezione Automazione è stata aggiornata per facilitarne l'individuazione. Inoltre, sono stati aggiunti tre nuovi argomenti alla sezione Automazione:

17 aprile 2019

- [Esegui un'automazione passo dopo passo](#)
- [Esegui un'automazione che richiede approvazioni](#)
- [Pianificazione delle automazioni con State Manager associazioni](#)

## [Crittografa i dati della sessione utilizzando una chiave AWS KMS](#)

4 aprile 2019

Per impostazione predefinita, Session Manager utilizza TLS 1.2 per crittografare i dati delle sessioni trasmessi tra i computer locali di utenti nell'account e le istanze EC2. Ora puoi scegliere di crittografare ulteriormente i dati utilizzando una AWS KMS key che è stata creata in. AWS Key Management Service. È possibile usare una chiave che è stata creata nell'account Account AWS o una che è stata condivisa con un altro account. Per informazioni su come specificare una chiave KMS per crittografare i dati della sessione, vedi [Attivare la crittografia con AWS KMS chiave dei dati della sessione \(console\)](#), [Creare Session Manager preferenze \(\)](#) o [Session Manager Aggiornare le preferenze \(AWS CLI\)](#). [AWS CLI](#)



[Configurazione delle notifiche  
Amazon SNS per AWS  
Systems Manager](#)

Sono state aggiunte istruzioni per l'utilizzo della console AWS CLI o di Systems Manager per configurare le notifiche Run Command e le Run Command attività di Amazon SNS registrate in una finestra di manutenzione. Per ulteriori informazioni, consulta l'argomento relativo alla [configurazione delle notifiche Amazon SNS per AWS Systems Manager](#).

6 marzo 2019

## [Istanze avanzate per server e VM in ambienti ibridi](#)

AWS Systems Manager offre un livello di istanze standard e un livello di istanze avanzate per server e macchine virtuali nel tuo ambiente ibrido. Il livello di istanze standard consente di registrare un massimo di 1.000 server o VM ciascuno. Account AWS Regione AWS Se devi registrare più di 1.000 server o macchine virtuali in un singolo account e in una singola Regione, utilizza il piano istanze avanzate. È possibile creare tutte le istanze che desideri nel piano istanze avanzate, ma tutte le istanze configurate per Systems Manager sono disponibili e si pagano in base all'utilizzo effettivo. Le istanze avanzate consentono inoltre di connettersi alle macchine ibride utilizzando AWS Systems Manager Session Manager. Session Manager fornisce un accesso interattivo tramite shell alle tue istanze. Per ulteriori informazioni su come abilitare le istanze avanzate, consulta [Abilitazione del piano istanze avanzate](#).

4 marzo 2019

### [Creazione di associazioni State Manager che utilizzano documenti SSM condivisi](#)

È possibile creare State Manager associazioni che utilizzano i runbook SSM Command and Automation condivisi da altri. Account AWS La creazione di associazioni utilizzando documenti SSM condivisi consente di mantenere Amazon EC2 e l'infrastruttura ibrida in uno stato uniforme anche quando le istanze non si trovano nello stesso account. Per ulteriori informazioni sulla condivisione di documenti SSM, consulta [Documenti di AWS Systems Manager](#). Per ulteriori informazioni sulla creazione di un'associazione State Manager, consulta [Creazione di un'associazione](#).

28 febbraio 2019

### [Visualizza gli elenchi degli eventi di Systems Manager supportati dalle regole di Amazon EventBridge](#)

Il nuovo argomento [Monitoring Systems Manager events with Amazon EventBridge](#) fornisce un riepilogo dei vari eventi emessi da Systems Manager in EventBridge cui è possibile impostare regole di monitoraggio degli eventi.

25 febbraio 2019

## [Aggiunta di tag durante la creazione di risorse Systems Manager](#)

Systems Manager supporta ora la possibilità di aggiungere tag ad alcuni tipi di risorse quando vengono create. Le risorse che puoi etichettare quando le crei con AWS CLI o un SDK includono finestre di manutenzione, linee di base delle patch, Parameter Store parametri e documenti SSM. È possibile inoltre assegnare tag a un'istanza gestita quando crei un'attivazione per la stessa. Quando si utilizza la console Systems Manager, è possibile aggiungere i tag alle finestre di manutenzione, alle baseline delle patch e ai parametri.

24 febbraio 2019

## [Creazione automatica dei ruoli IAM per l'inventario di Systems Manager](#)

In precedenza, era necessario creare un ruolo AWS Identity and Access Management (IAM) e allegare policy separate a questo ruolo per visualizzare i dati di inventario nella pagina di visualizzazione dei dettagli dell'inventario nella console. Non è più necessario creare questo ruolo o collegare le policy. Quando si sceglie una sincronizzazione remota dei dati nella pagina di visualizzazione dei dettagli dell'inventario, Systems Manager crea automaticamente il `Amazon-GlueServicePolicyForSSM` ruolo e gli assegna la policy `Amazon-GlueServicePolicyForSSM - {S3 bucket name}` e la `AWSGlueServiceRole` policy. Per ulteriori informazioni, consulta [Esecuzione di query sui dati di Inventory da più Regioni e account](#).

14 febbraio 2019

### [Procedure guidate Maintenance Windows per aggiornare SSM Agent](#)

Sono state aggiunte due nuove procedure guidate alla documentazione di Maintenance Windows. Le procedure dettagliate descrivono come utilizzare la console di Systems Manager o AWS CLI creare una finestra di manutenzione che si aggiorni automaticamente. SSM Agent Per ulteriori informazioni, consulta [Procedure guidate di Maintenance Windows](#).

11 febbraio 2019

### [Utilizzo di parametri pubblici di Parameter Store](#)

È stata aggiunta una breve sezione che descrive i parametri pubblici di Parameter Store. Per ulteriori informazioni, consulta [Utilizzo dei parametri pubblici di Systems Manager](#).

31 gennaio 2019

### [Usa il per creare le preferenze AWS CLISession Manager](#)

Sono state aggiunte istruzioni per l'utilizzo AWS CLI di per creare Session Manager preferenze, come CloudWatch Logs, opzioni di registrazione del bucket S3 e impostazioni di crittografia delle sessioni. Per ulteriori informazioni, consulta [AWS CLI Usare le preferenze per creare. Session Manager](#)

22 gennaio 2019

[Esecuzione di flussi di lavoro di automazione Systems Manager utilizzando State Manager](#)

AWS Systems Manager State Manager ora supporta la creazione di associazioni che utilizzano i runbook di SSM Automation. State Manager precedentemente supportate solo command e policy documenti, il che significava che era possibile creare associazioni destinate solo alle istanze gestite. Con il supporto per runbook Automation SSM, è ora possibile creare associazioni che fanno riferimento a tipi di risorse AWS differenti. Per ulteriori informazioni, consulta [esecuzione di flussi di lavoro di automazione Systems Manager utilizzando State Manager](#).

22 gennaio 2019

[Aggiornamenti dei riferimenti per le espressioni Cron e della frequenza e le opzioni di pianificazione della finestra di manutenzione](#)

L'argomento della guida di riferimento alle [Espressioni Cron e della frequenza per Systems Manager](#) è stato modificato. La nuova versione fornisce ulteriori esempi e spiegazioni migliorate su come utilizzare le espressioni Cron e della frequenza per pianificare le finestre di manutenzione e le associazioni di State Manager. Il nuovo argomento [Opzioni di pianificazione e periodo attivo per Maintenance Windows](#) spiega inoltre l'interazione tra le diverse opzioni di pianificazione per le finestre di manutenzione, tra cui data di inizio, data di fine, fuso orario e frequenza di pianificazione.

6 dicembre 2018

[Attivazione della registrazione di debug dell'SSM Agent](#)

È possibile attivare la registrazione di debug dell'SSM Agent modificando il file `seelog.xml` nel template sull'istanza gestita. Per ulteriori informazioni, consulta l'argomento relativo all'[abilitazione della registrazione di debug dell'SSM Agent](#).

30 novembre 2018



## [Supporto per le architetture del processore ARM64](#)

AWS Systems Manager ora supporta le versioni ARM64 dei sistemi operativi Amazon Linux 2, Red Hat Enterprise Linux 7.6 e Ubuntu Server (18.04 LTS e 16.04 LTS). Per ulteriori informazioni, consulta le istruzioni per l'installazione di [Amazon Linux 2](#), [RHEL](#), e [Ubuntu Server 18.04 e 16.04 LTS con pacchetti Snap](#). Per ulteriori informazioni sul tipo di istanza A1, consulta [Istanze per uso generico](#) nella Guida per l'utente di Amazon EC2.

26 novembre 2018

[Crea e distribuisce pacchetti utilizzando AWS Systems Manager Distributor](#)

20 novembre 2018

AWS Systems Manager Distributor Usandolo, impacchettate il vostro software o trovate pacchetti software AWS forniti da agenti, ad esempio, da AmazonCloudWatchAgent. AWS Systems Manager Distributor pubblica risorse, ad esempio pacchetti software, su istanze gestite. AWS Systems Manager La pubblicazione di un pacchetto notifica la disponibilità di versioni specifiche del documento del pacchetto, un documento di Systems Manager creato quando aggiungi il pacchetto in Distributor, alle istanze gestite identificate con gli ID istanza gestita, gli ID Account AWS, i tag o una Regione AWS. Per ulteriori informazioni, consulta [AWS Systems Manager Distributor](#).

[Esegui contemporaneamente flussi di lavoro di AWS Systems Manager automazione su più account Regioni AWS e Account AWS da un account centrale](#)

È possibile eseguire contemporaneamente flussi di lavoro di AWS Systems Manager automazione su più unità organizzative (OU) Account AWS e/o su più Regioni AWS unità AWS organizzative (OU) da un account di gestione di Automation. L'esecuzione in simultanea delle istanze di automazione in più regioni e account o in più unità organizzative (OU) riduce il tempo richiesto per amministrare le risorse AWS e contemporaneamente potenzia la sicurezza dell'ambiente di elaborazione. Per ulteriori informazioni, consulta [Esecuzione dei flussi di lavoro di automazione in più e. Regioni AWS Account AWS](#)

19 novembre 2018

## [Interroga i dati di inventario da più Regioni AWS e Account AWS](#)

Systems Manager Inventory si integra con Amazon Athena per aiutarti a interrogare i dati di inventario da più Regioni AWS e Account AWS. L'integrazione con Athena utilizza la sincronizzazione dei dati delle risorse in modo da poter visualizzare i dati di inventario di tutte le istanze gestite nella pagina Inventory Detail View della console. AWS Systems Manager Per ulteriori informazioni, consulta [Esecuzione di query sui dati di Inventory da più Regioni e account.](#)

15 novembre 2018

## [Creazione di associazioni State Manager che eseguono file MOF](#)

15 novembre 2018

È possibile eseguire file MOF (Managed Object Format) per applicare uno stato target alle istanze gestite di Windows Server con State Manager utilizzando il documento SSM di `AWS-ApplyDSCMofs`. Il documento `AWS-ApplyDSCMofs` è caratterizzato da due modalità di esecuzione. La prima consente di configurare l'associazione per analizzare e segnalare se le istanze gestite sono attualmente nello stato target definito nei file MOF specificati. La seconda consente di eseguire i file MOF e modificare la configurazione delle istanze in base alle risorse e ai relativi valori definiti nei file MOF. Il `AWS-ApplyDSCMofs` documento consente di scaricare ed eseguire i file di configurazione MOF da Amazon Simple Storage Service (Amazon S3), da una condivisione locale o da un sito Web sicuro con un dominio HTTPS. Per ulteriori informazioni, consulta [Creazione di associazioni che eseguono file MOF](#).

[Limitazione dell'accesso amministrativo in sessioni di Session Manager](#)

Le sessioni di Session Manager vengono avviate tramite le credenziali di un account utente creato con privilegi di amministratore o root di default denominati `ssm-user`. Informazioni su come limitare il controllo amministrativo per questo account sono ora disponibili nell'argomento relativo a [abilitazione o disabilitazione delle autorizzazioni amministrative dell'account ssm-account](#).

13 novembre 2018

[Esempi YAML nelle informazioni di riferimento relative alle operazioni di Automation](#)

La [Documentazione di riferimento delle operazioni di Automazione](#) ora include un esempio YAML per ciascuna operazione che già prevede un esempio JSON.

31 ottobre 2018

### [Assegnazione di livelli di gravità della conformità alle associazioni](#)

È ora possibile assegnare livelli di gravità della conformità alle associazioni State Manager. Questi livelli di gravità sono riportati nel pannello di controllo relativo alla conformità e possono essere utilizzati anche per filtrare i report di conformità. I livelli di gravità da assegnare includono Critico, Elevato, Medio, Basso e Non specificato. Per ulteriori informazioni, consulta [Creazione di un'associazione \(console\)](#).

26 ottobre 2018

### [Utilizzo di destinazioni e controlli di velocità in Automazione e State Manager](#)

Controlla l'esecuzione delle Automazioni e delle associazioni State Manager in tutto il parco istanze delle risorse utilizzando destinazioni, simultaneità e soglie di errore. Per ulteriori informazioni, consulta [Uso di destinazioni e controlli di velocità per l'esecuzione di flussi di lavoro di Automazione su un parco istanze](#) e [Uso di destinazioni e controlli di velocità con associazioni di State Manager](#).

23 ottobre 2018

[Specifica gli intervalli di tempo attivi e i fusi orari internazionali per le finestre di manutenzione](#)

Puoi anche specificare le date in cui una finestra di manutenzione non deve essere eseguita prima o dopo (data di inizio e data di fine). È possibile specificare il fuso orario internazionale su cui basare la pianificazione della finestra di manutenzione. Per ulteriori informazioni, consulta [Creazione di una finestra di manutenzione \(console\)](#) e [Aggiornamento di una finestra di manutenzione \(AWS CLI\)](#).

9 ottobre 2018

[Gestione di un elenco personalizzato di patch per la baseline delle patch in un bucket S3](#)

Con il nuovo parametro 'InstallOverrideList' nel documento di comando `SSMAWS-RunPatchBaseline`, puoi specificare un URL https o un URL in stile percorso Amazon Simple Storage Service (Amazon S3) per un elenco di patch da installare. Questo elenco di installazione delle patch, gestito in un bucket S3 in formato YAML, sostituisce le patch specificate dalla baseline delle patch predefinita. Per ulteriori informazioni, consulta Nome del parametro: [InstallOverrideList](#)

5 ottobre 2018



### [Controllo esteso sulla possibile installazione delle dipendenze patch](#)

In passato, una patch nell'elenco delle patch rifiutate identificata come una dipendenza di un'altra patch veniva installata ugualmente. Ora è possibile scegliere se installare queste dipendenze o bloccarne l'installazione. Per ulteriori informazioni, consulta [Creazione di una baseline delle patch personalizzata](#).

5 ottobre 2018

### [Creazione di flussi di lavoro di automazione dinamici con branching condizionale](#)

L'azione `aws:branch` Automazione consente di creare un flusso di lavoro di automazione dinamico che valuta più scelte in un unico passaggio e quindi passa a una fase diversa del runbook di automazione in base ai risultati di tale valutazione. Per ulteriori informazioni, consulta [Using conditional statements in runbooks](#) (Utilizzo di istruzioni condizionali nei runbook).

26 settembre 2018

[Usa il per aggiornare le preferenze AWS CLISession Manager](#)

Le istruzioni per l'uso della CLI per aggiornare Session Manager le preferenze, come CloudWatch Logs e le opzioni di registrazione del bucket S3, sono state aggiunte alla Guida per l'utente. AWS Systems Manager Per informazioni, consulta [Use the AWS CLI to update preferences. Session Manager](#)

25 settembre 2018

[Requisito dell'SSM Agent aggiornato per Session Manager](#)

Session Manager richiede ora l'SSM Agent versione 2.3.68.0 o successiva. Per ulteriori informazioni sui prerequisiti di Session Manager, consulta [Fase 1: Verifica dei prerequisiti di Session Manager](#).

17 settembre 2018

[Gestione delle istanze senza aprire porte in ingresso o gestire host bastione utilizzando Session Manager](#)

11 settembre 2018

Utilizzando Session Manager, uno strumento completamente gestito in AWS Systems Manager, puoi gestire le tue istanze EC2 tramite una shell interattiva basata su browser o tramite AWS CLI. Session Manager fornisce una gestione delle istanze sicura e verificabile senza la necessità di aprire porte in entrata, mantenere bastion host o gestire chiavi SSH. Session Manager consente inoltre di rispettare le politiche aziendali che richiedono un accesso controllato alle istanze, rigide pratiche di sicurezza e registri completamente verificabili con dettagli di accesso alle istanze, fornendo comunque agli utenti finali un semplice accesso multiplatforma in un unico passaggio alle istanze EC2. Per ulteriori dettagli, consulta [Ulteriori informazioni su Session Manager](#).

[Richiamando altro da un flusso di lavoro di Systems Manager Automation Servizi AWS](#)

È possibile richiamare altri Servizi AWS e altri strumenti di Systems Manager nel flusso di lavoro di automazione utilizzando tre nuove azioni (o plug-in) di automazione nei runbook di Automation. Per ulteriori informazioni, consulta [Utilizzo degli output delle operazioni come input](#).

28 agosto 2018

[Utilizza le chiavi di Manager-specifica condizione di Systems nelle policy IAM](#)

L'argomento [Specifica delle condizioni in una policy](#) è stato aggiornato per elencare le chiavi di condizione IAM per Systems Manager che è possibile integrare nelle policy. È possibile anche utilizzare queste chiavi per specificare le condizioni che determinano l'applicazione di una policy. L'argomento include anche i collegamenti a policy di esempio e ad altri argomenti correlati.

18 agosto 2018

[Aggregazione dei dati di inventario con gruppi per vedere quali istanze sono o meno configurate per raccogliere un tipo di inventario](#)

I gruppi ti consentono di vedere rapidamente il numero di istanze gestite che sono o meno configurate per raccogliere uno o più tipi di Inventory. Con i gruppi, devi specificare uno o più tipi di Inventory nonché un filtro che utilizzi l'operatore `exists`. Per ulteriori informazioni, consulta [Aggregazione dei dati di Inventory](#).

16 agosto 2018

[Visualizzazione di cronologia e monitoraggio delle modifiche per inventario e conformità di configurazione](#)

È ora possibile visualizzare la cronologia e il monitoraggio delle modifiche dei dati di Inventory raccolti dalle istanze gestite. È anche possibile visualizzare la cronologia e il rilevamento delle modifiche per l'applicazione di patch di Patch Manager e le associazioni State Manager riportate in Conformità di configurazione. Per ulteriori informazioni, consulta [Visualizzazione della cronologia e del monitoraggio delle modifiche di Inventario](#).

9 agosto 2018

## [Parameter Store si integra con Secrets Manager](#)

26 luglio 2018

Parameter Store è ora integrato AWS Secrets Manager in modo da poter recuperare i segreti di Secrets Manager quando ne usi altri Servizi AWS che già supportano i riferimenti ai Parameter Store parametri. Questi servizi includono Amazon EC2, Amazon Elastic Container Service, AWS Lambda, CloudFormation AWS CodeBuild AWS CodeDeploy, e altri strumenti di Systems Manager. Avvalendoti di Parameter Store per fare riferimento ai segreti di Secrets Manager, configura un processo coerente e sicuro per la chiamata e l'utilizzo di segreti e dati di riferimento in script di configurazione e codice. Per informazioni, consulta [Referencing AWS Secrets Manager secrets from Parameter Store parameters](#).

## [Collegamento di etichette ai parametri dell'Parameter Store](#)

Un'etichetta di parametro è un alias definito dall'utente che consente di semplificare la gestione delle diverse versioni di un parametro. Quando modifichi un parametro, Systems Manager ne salva automaticamente una nuova versione e incrementa automaticamente il numero di versione di un'unità. Un'etichetta può aiutarti a ricordare lo scopo di una versione del parametro in presenza di più versioni. Per informazioni, consulta [Etichettatura dei parametri](#).

26 luglio 2018

## Creazione di flussi di lavoro di automazione dinamici

Come impostazione predefinita, le fasi (oppure operazioni) definite nella sezione `mainSteps` di un runbook Automation vengono eseguite in ordine sequenziale. Al completamento di un'operazione, viene avviata l'operazione successiva specificata nella sezione `mainSteps`. Con questa versione, è ora possibile creare flussi di lavoro di Automazione che eseguono il branching condizionale. È possibile quindi creare flussi di lavoro di Automazione in grado di rispondere dinamicamente alle modifiche della condizione e passare a una fase specificata. Per informazioni, consulta [Using condition al statements in runbooks](#) (Utilizzo di istruzioni condizionali nei runbook).

18 luglio 2018



[SSM Agent ora preinstallato su Ubuntu Server 16.04 AMIs mediante Snap](#)

A partire dalle istanze create da Ubuntu Server 16.04 AMIs identificate dal codice 20180627, SSM Agent viene preinstallato tramite pacchetti Snap. Per le istanze create da AMIs precedenti, è necessario continuare a utilizzare i pacchetti di installazione deb. Per ulteriori informazioni, consulta [Informazioni sulle installazioni dell'SSM Agent su istanze di Ubuntu Server 16.04 a 64 bit.](#)

7 luglio 2018

[Revisione delle autorizzazioni minime dei bucket S3 richieste da SSM Agent](#)

Il nuovo argomento [Informazioni sulle autorizzazioni minime dei bucket S3 per SSM Agent](#) fornisce informazioni sui bucket Amazon Simple Storage Service (Amazon S3) a cui le risorse potrebbero dover accedere per eseguire operazioni di Systems Manager. È possibile specificare questi bucket in una policy personalizzata se vuoi limitare l'accesso ai bucket S3 per un profilo dell'istanza o un endpoint VPC al minimo richiesto per utilizzare Systems Manager.

5 luglio 2018

[Visualizzazione della cronologia di esecuzione completa per un ID di associazione State Manager specifico](#)

Il nuovo argomento [Visualizzazione della cronologia delle associazioni](#) descrive come visualizzare tutte le esecuzioni per un ID di associazione specifico e quindi visualizzare i dettagli di esecuzione relativi a una o più risorse.

2 luglio 2018

[Patch Manager introduzione del supporto per Amazon Linux 2](#)

È ora possibile utilizzare Patch Manager per l'applicazione di patch alle istanze Amazon Linux 2. Per informazioni generali sul supporto del sistema operativo per Patch Manager, consulta [Prerequisiti di Patch Manager](#). Per informazioni sulle coppie chiave-valore supportate per Amazon Linux 2 [PatchFilter](#) nella definizione di un filtro patch, consulta l'AWS Systems Manager API Reference.

26 giugno 2018

[Invia l'output del comando ad Amazon Logs CloudWatch](#)

Il nuovo argomento [Configurazione di Amazon CloudWatch Logs per Run Command](#) descrive come inviare l'Run Commandoutput a CloudWatch Logs.

18 giugno 2018

[Crea o elimina rapidamente la sincronizzazione dei dati delle risorse per Inventory utilizzando CloudFormation](#)

11 giugno 2018

È possibile utilizzarlo CloudFormation per creare o eliminare una sincronizzazione dei dati delle risorse per Systems Manager Inventory. Per utilizzarla CloudFormation, aggiungi la ResourceDataSync [risorsa](#) AWS: :SSM:: al tuo CloudFormation modello. Per ulteriori informazioni, consulta [Uso di modelli AWS CloudFormation](#) nella Guida per l'utente di AWS CloudFormation . È possibile anche creare manualmente una sincronizzazione dati risorsa per l'inventario, come descritto nella pagina relativa alla [Creazione di un Resource Data Sync per Inventory](#).

[AWS Systems Manager Le notifiche di aggiornamento della Guida per l'utente sono ora disponibili tramite RSS](#)

La versione HTML della Guida per l'utente di Systems Manager supporta ora un feed RSS di aggiornamenti che sono documentati nella pagina [cronologia di aggiornamento della documentazione di Systems Manager](#). Il feed RSS include gli aggiornamenti effettuati da giugno 2018 in poi. Gli aggiornamenti annunciati in precedenza sono tuttora disponibili nella pagina della cronologia di aggiornamento della documentazione di Systems Manager. Utilizza il pulsante RSS nel pannello del menu in alto per registrarti al feed.

06 giugno 2018

[Specifica di un codice di uscita negli script per riavviare le istanze gestite](#)

Il nuovo argomento [Riavvio delle istanze gestite da script](#) descrive come indicare a Systems Manager di riavviare le istanze gestite specificando il codice di uscita negli script eseguiti con Run Command.

3 giugno 2018

[Crea un evento in Amazon EventBridge ogni volta che l'inventario personalizzato viene eliminato](#)

Il nuovo argomento [Visualizzazione delle azioni di eliminazione dell'inventario in EventBridge](#) descrive come configurare Amazon EventBridge per creare un evento ogni volta che un utente elimina un inventario personalizzato.

1° giugno 2018

## Aggiornamenti prima di giugno 2018

La tabella seguente descrive le modifiche importanti apportate a ogni versione della Guida per l'utente di AWS Systems Manager prima di giugno 2018.

Modifica	Description	Data di rilascio
Fai l'inventario di tutte le istanze gestite nel tuo Account AWS	<p>Puoi inventariare tutte le istanze gestite presenti nel tuo sistema Account AWS creando un'associazione globale di inventario. Per ulteriori informazioni, consulta <a href="#">Fai l'inventario di tutti i nodi gestiti nel tuo Account AWS</a>.</p> <div> <p> <b>Note</b></p> <p>Le associazioni di inventario globale sono disponibili in SSM Agent 2.0.790.0 o versione successiva. Per informazioni su come aggiornare l'SSM Agent sulle istanze, consulta <a href="#">Aggiornamento di SSM Agent utilizzando Run Command</a>.</p> </div>	03 maggio 2018
SSM Agent installato per impostazione predefinita su Ubuntu Server 18	SSM Agent è installato, per impostazione predefinita, su Ubuntu Server 18.04 LTS a 64 bit e 32 bit AMIAMI.	02 maggio 2018
Nuovo argomento	Il nuovo argomento <a href="#">Esecuzione di comandi utilizzando una versione specifica del documento</a> descrive come utilizzare e il parametro document-version per specificare quale versione di un documento SSM utilizzare quando viene eseguito il comando.	1° maggio 2018
Nuovo argomento	Il nuovo argomento <a href="#">Eliminazione di un inventario personalizzato</a> descrive come eliminare i dati dell'inventario personalizzato da Amazon S3 utilizzando AWS CLI. L'argomento descrive inoltre come utilizzare SchemaDeleteOption per gestire l'inventario personalizzato	19 aprile 2018

Modifica	Description	Data di rilascio
	disattivando o eliminando un tipo di inventario personalizzato. Questa nuova funzionalità utilizza l'operazione <a href="#">DeleteInventory</a> API.	
Notifiche Amazon SNS per SSM Agent	È possibile effettuare la sottoscrizione a un argomento Amazon SNS per ricevere notifiche quando è disponibile una nuova versione dell'SSM Agent. Per ulteriori informazioni, consulta <a href="#">Abbonarsi a Agente SSM notifiche</a> .	9 aprile 2018
Supporto dell'applicazione di patch per CentOS	Systems Manager supporta ora l'applicazione di patch per le istanze di CentOS. Per informazioni sulle versioni di CentOS supportate, consulta <a href="#">Patch Manager prerequisiti</a> . Per ulteriori informazioni sull'applicazione di patch, consulta <a href="#">In che modo Patch Manager operazioni funzionano</a> .	29 marzo 2018
Nuova sezione	Per fornire un'unica fonte per le informazioni di riferimento nella guida per l'utente di AWS Systems Manager , è stata introdotta una nuova sezione, <a href="#">AWS Systems Manager riferimento</a> . Ulteriori contenuti verranno aggiunti a questa sezione non appena disponibili.	15 marzo 2018
Nuovo argomento	Il nuovo argomento <a href="#">Formati dei nomi dei pacchetti per gli elenchi delle patch approvate e rifiutate</a> offre dettagli relativi ai formati dei nomi di pacchetto che è possibile inserire negli elenchi delle patch approvate e delle patch rifiutate per una baseline delle patch personalizzata. Vengono forniti formati di esempio per ogni tipo di sistema operativo supportato da Patch Manager.	09 marzo 2018

Modifica	Description	Data di rilascio
Nuovo argomento	Systems Manager ora si integra con <a href="#">Chef Chef InSpec</a> . InSpec è un framework di runtime open source che consente di creare profili leggibili dall'uomo su Amazon S3. GitHub È quindi possibile utilizzare Systems Manager per eseguire analisi della conformità e visualizzare le istanze conformi e non conformi. Per ulteriori informazioni, consulta <a href="#">Utilizzo Chef InSpec profili con Systems Manager Compliance</a> .	07 marzo 2018
Nuovo argomento	Il nuovo argomento <a href="#">Utilizzo di ruoli collegati ai servizi per Systems Manager</a> descrive come utilizzare un ruolo AWS Identity and Access Management (IAM) collegato ai servizi con Systems Manager. I ruoli collegati al servizio sono attualmente richiesti solo quando si utilizza l'inventario di Systems Manager per raccogliere i metadati su tag e gruppi di risorse.	27 febbraio 2018
Argomenti nuovi e aggiornati	<p>Ora è possibile utilizzare Patch Manager per installare patch presenti in un repository di origine diverso da quello predefinito configurato nell'istanza. Ciò è utile per l'applicazione di patch a istanze con aggiornamenti non correlati alla sicurezza, contenuti di Personal Package Archives (PPA) per Ubuntu Server, aggiornamenti per le applicazioni aziendali interne e così via. È possibile specificare un repository di origine delle patch alternativo al momento della creazione di una baseline delle patch personalizzata. Per ulteriori informazioni, consulta i seguenti argomenti:</p> <ul style="list-style-type: none"> <li>• <a href="#">Come specificare un repository alternativo di origine delle patch (Linux)</a></li> <li>• <a href="#">Utilizzo delle baseline delle patch personalizzate</a></li> <li>• <a href="#">Creazione di una baseline delle patch con repository personalizzati per varie versioni dei sistemi operativi</a></li> </ul>	06 febbraio 2018

Modifica	Description	Data di rilascio
Nuovo argomento	Il nuovo argomento <a href="#">Documenti sul comando SSM per l'applicazione di patch a nodi gestiti</a> descrive i sette documenti SSM disponibili, utili per assicurarti che alle istanze gestite vengano applicate patch mediante gli aggiornamenti della sicurezza più recenti.	10 gennaio 2018
Aggiornamenti importanti relativi al supporto di Linux	<p>Vari argomenti sono stati aggiornati con le seguenti informazioni:</p> <ul style="list-style-type: none"> <li>• Per impostazione predefinita, SSM Agent è installato sulle AMIs Amazon Linux 1 di base con data 2017.09 e successiva.</li> <li>• Installa manualmente SSM Agent su altre versioni di Linux, incluse immagini non di base come Amazon. ECS-Optimized AMIs</li> </ul>	09 gennaio 2018
Nuovo argomento	Un nuovo argomento, <a href="#">Documento di comando SSM per l'applicazione di patch: AWS-RunPatchBaseline</a> , fornisce dettagli sul funzionamento di tale documento SSM nei sistemi Windows e Linux. Vengono inoltre fornite informazioni sui due parametri disponibili nel documento AWS-RunPatchBaseline, <code>Operation</code> , e <code>Snapshot ID</code> .	05 gennaio 2018
Nuovi argomenti	Una nuova sezione, <a href="#">In che modo Patch Manager operazioni funzionano</a> , fornisce dettagli tecnici che illustrano come Patch Manager determina le patch di sicurezza da installare e la relativa modalità di installazione in ciascun sistema operativo supportato. Vengono inoltre fornite informazioni sulle regole della baseline delle patch in varie distribuzioni del sistema operativo Linux.	02 gennaio 2018



Modifica	Description	Data di rilascio
Modifica del titolo e spostamento delle informazioni di riferimento relative alle operazioni di automazione di Systems Manager	In base ai feedback dei clienti, la guida di riferimento alle operazioni di Automazione è ora denominata Guida di riferimento ai runbook Systems Manager Automation. Tale riferimento è inoltre stato spostato nel nodo Risorse condivise > Documenti così da avvicinarlo a <a href="#">Documentazione di riferimento del plugin per i documenti di comando</a> . Per ulteriori informazioni, consulta <a href="#">Riferimento alle operazioni del servizio di automazione di Systems Manager</a> .	20 dicembre 2017
Nuovo capitolo e nuovi contenuti sul monitoraggio	Un nuovo capitolo <a href="#">Registrazione e monitoraggio AWS Systems Manager</a> , fornisce istruzioni per l'invio di metriche e dati di log ad Amazon CloudWatch Logs. Un nuovo argomento fornisce istruzioni per la migrazione delle attività di monitoraggio sull'istanza, solo su Windows Server istanze a 64 bit, dall'SSM Agent all'agente. <a href="#">Invio dei log dei nodi a CloudWatch registri unificati (CloudWatch agente)</a> CloudWatch	14 dicembre 2017
Nuovo capitolo	Un nuovo capitolo fornisce informazioni complete sull'uso di <a href="#">AWS Identity and Access Management (IAM)</a> e AWS Systems Manager su come proteggere l'accesso alle risorse tramite l'uso di credenziali. <a href="#">Gestione delle identità e degli accessi per AWS Systems Manager</a> Queste credenziali forniscono le autorizzazioni necessarie per accedere alle AWS risorse, ad esempio l'accesso ai dati archiviati nei bucket S3 e l'invio di comandi e la lettura dei tag sulle istanze EC2.	11 dicembre 2017
Modifiche al riquadro di navigazione a sinistra	Sono state apportate modifiche alle intestazioni nel riquadro di navigazione a sinistra di questa Guida per l'utente, per garantirne la corrispondenza con le intestazioni nella nuova <a href="#">console AWS Systems Manager</a> .	08 dicembre 2017

Modifica	Description	Data di rilascio
Varie modifiche a re:Invent 2017	<ul style="list-style-type: none"> <li>Lancio ufficiale di AWS Systems Manager: AWS Systems Manager (precedentemente Amazon EC2 Systems Manager) è un'interfaccia unificata che consente di centralizzare i dati operativi e automatizzare le attività tra le risorse. AWS Puoi accedere alla nuova console qui. AWS Systems Manager <a href="https://console.aws.amazon.com/systems-manager/">https://console.aws.amazon.com/systems-manager/</a> Per ulteriori informazioni, consulta <a href="#">Cosa è AWS Systems Manager?</a></li> <li>Supporto YAML: è possibile creare documenti SSM in YAML. Per ulteriori informazioni, consulta <a href="#">AWS Systems Manager Documenti di</a>.</li> </ul>	29 novembre 2017
Utilizzo Run Command per scattare VSS-Enabled istantanee dei volumi EBS	<p>utilizzando Run Command, è possibile creare snapshot coerenti a livello di applicazione di tutti i volumi <a href="#">Amazon Elastic Block Store (Amazon EBS)</a> collegati alle istanze Windows su Amazon EC2. Il processo di istantanea utilizza il <a href="#">Volume Shadow Copy Service (VSS) di Windows per eseguire backup</a> a livello di immagine delle VSS-aware applicazioni, inclusi i dati delle transazioni in sospeso tra queste applicazioni e il disco. Non è necessario inoltre arrestare le istanze o scollegarle per eseguire il backup di tutti i volumi collegati. Per ulteriori informazioni, consulta <a href="#">Take Microsoft VSS-Enabled Snapshots Using nella Amazon EC2 User Guide AWS Systems Manager</a>.</p>	20 novembre 2017

Modifica	Description	Data di rilascio
Sicurezza Systems Manager avanzata disponibile mediante gli endpoint VPC	È possibile migliorare la posizione di sicurezza delle istanze gestite (incluse le istanze gestite nell'ambiente ibrido) configurando Systems Manager per l'utilizzo di endpoint VPC di interfaccia. Gli endpoint dell'interfaccia sono basati su PrivateLink, una tecnologia che consente di accedere privatamente alle API di Amazon EC2 e Systems Manager utilizzando indirizzi IP privati. PrivateLink limita tutto il traffico di rete tra le istanze gestite, Systems Manager ed EC2 alla rete Amazon (le istanze gestite non hanno accesso a Internet). Inoltre, non hai bisogno di un gateway Internet, di un dispositivo NAT o di un gateway virtuale privato. Per ulteriori informazioni, consulta <a href="#">Migliora la sicurezza delle istanze EC2 utilizzando gli endpoint VPC per Systems Manager</a> .	07 novembre 2017

Modifica	Description	Data di rilascio
Supporto dell'inventario per file, servizi, ruoli di Windows e Registro di Windows	<p>L'inventario SSM supporta ora la raccolta delle seguenti informazioni dalle istanze gestite.</p> <ul style="list-style-type: none"> <li>• File: nome, dimensioni, versione, data di installazione, ora di modifica e dell'ultimo accesso, ecc.</li> <li>• Servizi: nome, nome visualizzato, stato, servizi dipendenti, tipo di servizio, tipo di avvio, ecc.</li> <li>• Registro di sistema di Windows: percorso della chiave del registro di sistema, nome del valore, tipo di valore e valore.</li> <li>• Ruoli Windows: nome, nome visualizzato, percorso, tipo di funzionalità, stato di installazione, ecc.</li> </ul> <p>Prima di tentare di raccogliere informazioni per questi tipi di inventario, aggiorna l'SSM Agent sulle istanze da aggiungere all'inventario. Eseguendo la versione più recente di SSM Agent, ti assicuri di poter raccogliere metadati per tutti i tipi di inventario supportati. Per informazioni su come aggiornare l'SSM Agent mediante State Manager, consulta <a href="#">Procedura dettagliata: aggiorna SSM Agent automaticamente con AWS CLI</a>.</p> <p>Per ulteriori informazioni sull'inventario, consulta <a href="#">Ulteriori informazioni su l'inventario di Systems Manager</a>.</p>	6 novembre 2017
Aggiornamenti alla documentazione di Automazione	<p>Sono state apportate diverse correzioni alle informazioni sull'impostazione e la configurazione dell'accesso per l'automazione di Systems Manager. Per ulteriori informazioni, consulta <a href="#">Configurazione del servizio di automazione</a>.</p>	31 ottobre 2017

Modifica	Description	Data di rilascio
Integrazione di GitHub e Amazon S3	<p>Esecuzione di script in remoto: Systems Manager supporta ora il download e l'esecuzione di script da un repository GitHub privato o pubblico e da Amazon S3. Utilizzando il documento SSM <code>AWS-RunRemoteScript</code> predefinito o il <code>aws:downloadContent</code> plug-in in un documento SSM personalizzato, puoi eseguire Ansible playbook e script in Python, Ruby o, solo per citarne alcuni, PowerShell. Queste modifiche migliorano ulteriormente infrastrutture as code, quando utilizzi Systems Manager per automatizzare la configurazione e l'implementazione di istanze EC2 e di istanze gestite on-premises nel tuo ambiente ibrido. Per ulteriori informazioni, consulta <a href="#">Esecuzione di script da GitHub</a> e <a href="#">Esecuzione di script da Amazon S3</a>.</p> <p>Creazione di documenti SSM compositi: Systems Manager supporta ora l'esecuzione di uno o più documenti secondari da un documento principale. Questi documenti principali che eseguono altri documenti sono chiamati compositi. I documenti compositi consentono di creare e condividere un set standard di documenti SSM secondari per attività comuni come l'avvio di software antivirus o l'aggiunta di Account AWS istanze di aggiunta di domini. È possibile eseguire i documenti compositi e secondari archiviati in Systems Manager, GitHub o Amazon S3. Dopo aver creato un documento composito, è possibile eseguirlo utilizzando il documento SSM predefinito <code>AWS-RunDocument</code>. Per ulteriori informazioni, consulta <a href="#">Creazione di documenti compositi</a> e <a href="#">Esecuzione di documenti da posizioni remote</a>.</p> <p>Documentazione di riferimento del plug-in per il documento SSM: per facilitare l'accesso, abbiamo spostato le informazioni di riferimento del plug-in per i documenti SSM, togliendole dalla Documentazione di riferimento API di Systems Manager e inserendole nella Guida per l'utente.</p>	26 ottobre 2017

Modifica	Description	Data di rilascio
	Per ulteriori informazioni, consulta <a href="#">Documentazione di riferimento del plugin per i documenti di comando</a> .	
Supporto per le versioni di parametri in Parameter Store	<p>Ora, quando modifichi un parametro, Parameter Store itera in automatico il numero di versione di 1. È possibile specificare un nome di parametro e un numero di versione specifico nelle chiamate API e nei documenti SSM. Se non specifichi un numero di versione, il sistema utilizza in automatico la versione più recente.</p> <p>Le versioni dei parametri forniscono un livello di protezione in caso di modifica accidentale di un parametro. È possibile visualizzare i valori di tutte le versioni e fare riferimento alle versioni più vecchie, se necessario. È inoltre possibile utilizzare le versioni di un parametro per visualizzare il numero di variazioni di tale parametro in un periodo di tempo. Per ulteriori informazioni, consulta <a href="#">Utilizzo delle versioni dei parametri in Parameter Store</a>.</p>	24 ottobre 2017
Support per assegnazione di tag ai documenti di Systems Manager.	È ora possibile utilizzare l' <a href="#">AddTagsToResource</a> API, il o il AWS CLI AWS Strumenti per PowerShell per etichettare i documenti di Systems Manager con coppie chiave-valore. Questa procedura aiuta a individuare velocemente risorse specifiche in base a tag a esse assegnati. Questo si aggiunge al supporto di etichettatura esistente per le istanze gestite, le finestre di manutenzione, i Parameter Store parametri e le linee di base delle patch.	03 ottobre 2017

Modifica	Description	Data di rilascio
Vari aggiornamenti della documentazione per correggere e errori o aggiornare contenuti in base al feedback	<ul style="list-style-type: none"> <li>• Aggiornamento di <a href="#">Gestione dei nodi in ambienti ibridi e multicloud con Systems Manager</a> con le informazioni per Raspbian Linux.</li> <li>• Aggiornato <a href="#">Gestire le istanze EC2 con Systems Manager</a> con nuovi requisiti per le istanze. Windows Server SSM Agent richiede Windows PowerShell 3.0 o versioni successive per eseguire determinati documenti SSM sulle Windows Server istanze (ad esempio, il documento AWS-ApplyPatchBaseline SSM precedente). Verifica che le istanze Windows Server eseguano Windows Management Framework 3.0 o versioni successive. Il framework include PowerShell. Per ulteriori informazioni, consulta <a href="#">Windows Management Framework 3.0</a>.</li> </ul>	2 ottobre 2017
Risoluzione dei problemi di istanze di Windows non raggiungibili con il flusso di lavoro di automazione EC2Rescue	EC2Rescue consente di diagnosticare e risolvere i problemi relativi alle istanze Amazon EC2 Windows Server. È possibile eseguire lo strumento come flusso di lavoro di Systems Manager Automation utilizzando il documento. AWSSupport-ExecuteEC2Rescue Il AWSSupport-ExecuteEC2Rescue documento è progettato per eseguire una combinazione di azioni, CloudFormation azioni e funzioni Lambda di Systems Manager che automatizzano i passaggi normalmente necessari per utilizzare EC2Rescue. Per ulteriori informazioni, consulta <a href="#">Esecuzione dello strumento EC2Rescue su istanze non raggiungibili</a> .	29 settembre 2017
SSM Agent installazione di default su Amazon Linux	Per impostazione predefinita, l'SSM Agent è installato su AMIs di Amazon Linux con data 2017.09 e successiva. L'SSM Agent deve essere installato manualmente su altre versioni di Linux, come descritto in <a href="#">Utilizzo di SSM Agent sulle istanze EC2 per Linux</a> .	27 settembre 2017

Modifica	Description	Data di rilascio
Miglioramenti a Run Command	<p>Run Command include i miglioramenti seguenti:</p> <ul style="list-style-type: none"> <li>• È possibile limitare l'esecuzione dei comandi a istanze specifiche creando e assegnando una policy IAM che include una condizione in base alla quale l'utente può eseguire i comandi solo sulle istanze contrassegnate con tag Amazon EC2 specifici. Per ulteriori informazioni, consulta <a href="#">Limitazione Run Command accesso basato su tag</a>.</li> <li>• Sono disponibili ulteriori opzioni per eseguire il targeting delle istanze tramite tag Amazon EC2. Ora è possibile specificare più chiavi di tag e più valori di tag al momento dell'invio di comandi. Per ulteriori informazioni, consulta <a href="#">Esecuzione di comandi su vasta scala</a>.</li> </ul>	12 settembre 2017
Systems Manager supportato su Raspbian	È ora possibile eseguire Systems Manager su dispositivi Raspbian Jessie e Raspbian Stretch, incluso Raspberry Pi (a 32 bit).	7 settembre 2017
Invia SSM Agent automaticamente i log ad Amazon Logs CloudWatch	Puoi ora effettuare una semplice modifica alla configurazione per le istanze per fare in modo che l'SSM Agent invii file di log a CloudWatch. Per ulteriori informazioni, consulta <a href="#">Invio Agente SSM da log a CloudWatch Logs</a> .	07 settembre 2017
Crittografia della sincronizzazione dati risorsa	La sincronizzazione dati risorsa di Systems Manager consente di aggregare i dati dell'inventario raccolti su dozzine o centinaia di istanze gestite in un bucket S3 centralizzato. È possibile ora crittografare la sincronizzazione dati risorsa utilizzando una chiave AWS Key Management Service . Per ulteriori informazioni, consulta <a href="#">Procedura dettagliata: utilizzo di sincronizzazione dati risorsa per aggregare dati di inventario</a> .	1° settembre 2017



Modifica	Description	Data di rilascio
Nuove procedure guidate di State Manager	<p>Sono state aggiunte due nuove procedure guidate alla documentazione di State Manager:</p> <p><a href="#">Procedura dettagliata: aggiorna SSM Agent automaticamente con AWS CLI</a></p> <p><a href="#">Spiegazione passo per passo: aggiornare automaticamente i driver PV sulle istanze EC2 per Windows Server</a></p>	31 agosto 2017
Conformità di configurazione di Systems Manager	<p>È possibile utilizzare Conformità di configurazione per eseguire la scansione del parco istanze gestite per individuare incoerenze nella configurazione e nella conformità delle patch. Puoi raccogliere e aggregare dati da più Account AWS e Regioni AWS quindi approfondire le risorse specifiche che non sono conformi. Per impostazione predefinita, la configurazione di conformità mostra i dati di conformità dell'applicazione di patch di Patch Manager e le associazioni di State Manager. È possibile anche personalizzare il servizio e creare tipi di conformità in base a requisiti aziendali o IT specifici. Per ulteriori informazioni, consulta <a href="#">AWS Systems Manager Conformità</a>.</p>	28 agosto 2017
Nuova operazione di automazione: <code>aws:executeAutomation</code>	<p>Esegue un flusso di lavoro di automazione secondari o mediante una chiamata a un runbook Automation secondario. Questa operazione consente di creare runbook Automation per i flussi di lavoro più comuni e fare riferimento a tali documenti durante l'esecuzione di un'Automazione. Questa operazione permette di semplificare i runbook Automation in quanto elimina la necessità di duplicare le fasi tra runbook simili. Per ulteriori informazioni, consulta <a href="#">AWS:ExecuteAutomation – Esegui un'altra automazione</a>.</p>	22 agosto 2017

Modifica	Description	Data di rilascio
L'automazione come obiettivo di un evento CloudWatch	Puoi avviare un flusso di lavoro di automazione specifica ndo un runbook di automazione come destinazione di un evento Amazon CloudWatch . È possibile avviare i flussi di lavoro in base a una pianificazione o quando si verifica un evento AWS di sistema specifico. Per ulteriori informazioni, consulta <a href="#">Esegui automazioni basate sugli eventi EventBridge</a> .	21 agosto 2017
Controllo delle versioni delle associazioni e aggiornamenti generali di State Manager	Ora è possibile creare diverse versioni delle associazioni di State Manager. Esiste una quota di 1.000 versioni per ogni associazione. È possibile inoltre specificare nomi per le associazioni. La documentazione di State Manager è inoltre stata aggiornata con correzioni alle informazioni obsolete e alle incoerenze. Per ulteriori informazioni, consulta <a href="#">AWS Systems Manager State Manager</a> .	21 agosto 2017

Modifica	Description	Data di rilascio
Modifiche alle Maintenance Windows	<p>Le Maintenance Windows includono i seguenti miglioramenti e modifiche:</p> <ul style="list-style-type: none"><li>• Le Maintenance Windows potevano in precedenza eseguire le operazioni solo utilizzando Run Command. È ora possibile eseguire attività utilizzando Systems Manager Automation AWS Lambda e AWS Step Functions.</li><li>• È possibile modificare le destinazioni di una finestra di manutenzione, specificare un nome di destinazione, una descrizione e un proprietario.</li><li>• È possibile modificare i processi di una finestra di manutenzione, inclusa la specifica di un nuovo documento SSM per Run Command e per le attività di automazione.</li><li>• Tutti Run Command i parametri sono ora supportati, inclusi DocumentHash, DocumentHashType, TimeoutSeconds, Comment e NotificationConfig.</li><li>• Ora è possibile utilizzare un flag safe quando tenti di annullare la registrazione di una destinazione. Se abilitato, il sistema restituisce un errore se alla destinazione viene fatto riferimento tramite un processo.</li></ul> <p>Per ulteriori informazioni, consulta <a href="#">AWS Systems Manager Intervallo di manutenzione</a>.</p>	16 agosto 2017

Modifica	Description	Data di rilascio
Nuova operazione di automazione: <code>aws:approve</code>	<p>Questa nuova operazione per i runbook Automation sospende temporaneamente l'esecuzione di un'automazione finché i principali designati non approvano o rifiutano l'operazione. Una volta raggiunto il numero richiesto di approvazioni, viene ripresa l'esecuzione dell'automazione.</p> <p>Per ulteriori informazioni, consulta <a href="#">Riferimento alle operazioni del servizio di automazione di Systems Manager</a>.</p>	10 agosto 2017
Ruolo di assunzione e dell'automazione non più richiesto	<p>In precedenza il servizio di automazione richiedeva di specificare un ruolo di servizio (o ruolo assunto) in modo tale che il servizio disponesse delle autorizzazioni necessarie per eseguire operazioni per conto dell'utente. Il servizio di automazione non richiede più questo ruolo perché il servizio ora funziona in base al contesto dell'utente che ha richiamato l'esecuzione.</p> <p>Tuttavia, i seguenti scenari richiedono ancora di specificare un ruolo di servizio di automazione:</p> <ul style="list-style-type: none"> <li>• Quando si desidera limitare le autorizzazioni di un utente per una risorsa, ma che tale utente esegua un flusso di lavoro di automazione che richiede autorizzazioni elevate. In questo scenario è possibile creare un ruolo di servizio con autorizzazioni elevate e consentire all'utente di eseguire il flusso di lavoro.</li> <li>• Le operazioni con possibili tempi di esecuzione maggiori di 12 ore richiedono un ruolo di servizio.</li> </ul> <p>Per ulteriori informazioni, consulta <a href="#">Configurazione del servizio di automazione</a>.</p>	3 agosto 2017

Modifica	Description	Data di rilascio
Conformità di configurazione	Utilizza la conformità di configurazione di Amazon EC2 Systems Manager per analizzare il parco istanze gestite e individuare incoerenze nella configurazione e nella conformità delle patch. Puoi raccogliere e aggregare dati da più Account AWS e Regioni AWS quindi analizzare in dettaglio risorse specifiche non conformi. Per ulteriori informazioni, consulta <a href="#">AWS Systems Manager Conformità</a> .	8 agosto 2017
Miglioramenti ai documenti SSM	<p>I documenti sui comandi e sulle policy di SSM offrono ora il supporto multiplatforma. Ciò significa che un singolo documento SSM può elaborare i plug-in per i sistemi operativi Windows e Linux. Cross-platform il supporto consente di consolidare il numero di documenti gestiti. Cross-platform il supporto è offerto nei documenti SSM che utilizzano la versione dello schema 2.2 o successiva.</p> <p>I documenti sui comandi di SSM che utilizzano una versione dello schema 2.0 o successiva possono ora includere più plug-in dello stesso tipo. Ad esempio, è possibile creare un documento di Comando che chiama più volte il plug-in <code>aws:runRunShellScript</code> .</p> <p>Per ulteriori informazioni sulle modifiche alla versione dello schema 2.2, consulta <a href="#">Documenti di AWS Systems Manager</a>. Per ulteriori informazioni sui plug-in SSM, consulta <a href="#">Documentazione di riferimento del plug-in per i documenti di comando</a>.</p>	12 luglio 2017

Modifica	Description	Data di rilascio
Applicazione di patch Linux	<p>Patch Manager può ora applicare patch alle seguenti distribuzioni Linux:</p> <p>Sistemi a 64 bit e a 32 bit</p> <ul style="list-style-type: none"><li>• Amazon Linux 2014.03, 2014.09 o versioni successive</li><li>• Ubuntu Server 16.04 LTS, 14.04 LTS o 12.04 LTS</li><li>• Red Hat Enterprise Linux (RHEL) 6.5 o versioni successive</li></ul> <p>Solo sistemi a 64 bit</p> <ul style="list-style-type: none"><li>• Amazon Linux 2015.03, 2015.09 o versioni successive</li><li>• Red Hat Enterprise Linux (RHEL) 7.x o versioni successive</li></ul> <p>Per ulteriori informazioni, consulta <a href="#">AWS Systems Manager Patch Manager</a>.</p> <div><p> Note</p><ul style="list-style-type: none"><li>• Per applicare patch a istanze di Linux, è necessario che le istanze eseguano SSM Agent versione 2.0.834.0 o successive. Per informazioni sull'aggiornamento dell'agente, consulta la sezione Esempio: aggiornamento dell'SSM Agent in <a href="#">Esecuzione di comandi dalla console</a>.</li><li>• Il documento SSM AWS-ApplyPatchBaseline viene sostituito dal documento AWS-RunPatchBaseline .</li></ul></div>	6 luglio 2017

Modifica	Description	Data di rilascio
Sincronizzazione dati delle risorse	<p>È possibile utilizzare la sincronizzazione dati risorsa per inviare i dati di inventario raccolti da tutte le istanze gestite da Systems Manager in un singolo bucket Amazon S3. La sincronizzazione dati delle risorse aggiorna in automatico i dati centralizzati una volta raccolti i nuovi dati di Inventory . Con tutti i dati di inventario archiviati in un bucket S3 di destinazione, puoi utilizzare servizi come Amazon Athena e Amazon Quick per interrogare e analizzare i dati aggregati . Per ulteriori informazioni, consulta. <a href="#">Creazione di un Resource Data Sync per Inventario</a> Per un esempio di come utilizzare la sincronizzazione dati risorsa, consulta <a href="#">Procedura dettagliata: utilizzo di sincronizzazione dati risorsa per aggregare dati di inventario</a>.</p>	29 giugno 2017
Systems Manager Parameter Generations	<p>La gestione di dozzine o centinaia di parametri di Systems Manager come un elenco semplice è un'attività dispendiosa in termini di tempo ed è soggetta a errori. È possibile pertanto utilizzare le gerarchie di parametri per semplificare l'organizzazione e la gestione dei parametri di Systems Manager . Una gerarchia è un nome di parametro che include un percorso definito mediante l'utilizzo di barre. Di seguito è riportato un esempio che utilizza tre livelli di gerarchia nel nome per identificare gli elementi seguenti:</p> <p>/di /Data Environment/Type computer/Application</p> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p>/Dev/DBServer/MySQL/db-string13</p> </div> <p>Per ulteriori informazioni, consulta <a href="#">Utilizzo delle gerarchie di parametri in Parameter Store</a>.</p>	22 giugno 2017

Modifica	Description	Data di rilascio
Supporto di SSM Agent per SUSE Linux Enterprise Server	È possibile installare SSM Agent su 64 bit SUSE Linux Enterprise Server(SLES). Per ulteriori informazioni, consulta <a href="#">Utilizzo di SSM Agent sulle istanze EC2 per Linux</a> .	14 giugno 2017



# Convenzioni dei documenti

Di seguito sono elencate le convenzioni tipografiche comuni per la Guida per l'utente di AWS Systems Manager .

Esempi differenziati per sistemi operativi locali o linguaggi della riga di comando

Utilizziamo schede per presentare diversi esempi di comandi in base al tipo di sistema operativo locale di un utente. Su Linux e macOS, ad esempio, la barra rovesciata (\) viene utilizzata per suddividere i comandi lunghi in più righe. Su Windows Server, ad esempio, il carattere caret (^) viene utilizzato per suddividere i comandi in più righe.

Esempio:

Linux & macOS

```
aws ssm send-command \
 --document-name "AWS-RunShellScript" \
 --targets "Key=instanceids,Values=i-02573cafcfEXAMPLE" \
 --parameters "commands=echo HelloWorld"
```

Windows

```
aws ssm send-command ^
 --document-name "AWS-RunShellScript" ^
 --targets "Key=instanceids,Values=i-02573cafcfEXAMPLE" ^
 --parameters "commands=echo HelloWorld"
```

Elementi dell'interfaccia utente

Formattazione: testo in grassetto

Esempio: Scegliere File, Proprietà.

Input utente (testo digitato da un utente)

Formattazione: testo in un tipo di carattere a spaziatura fissa

Esempio: per il nome, digita **my-new-resource**.

Il testo segnaposto per un valore obbligatorio

Formattazione: testo in *italics*

## Esempio:

```
aws ec2 register-image --image-location amzn-s3-demo-bucket/image.manifest.xml
```