



Guida alle operazioni di base

Console di gestione AWS



Version 1.0

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

Console di gestione AWS: Guida alle operazioni di base

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

Qual è il Console di gestione AWS?	1
Caratteristiche di Console di gestione AWS	1
Console di AWS servizio individuali	2
Accedere al Console di gestione AWS	2
Accesso Console di gestione AWS con dispositivi mobili	2
Nozioni di base su un servizio	4
Navigazione unificata	5
Accesso al menu Servizi	6
Ricerca di prodotti, servizi, funzionalità e altro	6
Ricerca di AWS prodotti	7
Perfezionamento della ricerca	8
Visualizzazione delle funzionalità di un servizio	8
Avvio AWS CloudShell	8
Accesso alle AWS notifiche e agli eventi Health	9
Ottenere supporto	9
Configurazione di Console di gestione AWS	10
Configurazione delle impostazioni unificate	10
Scegli la tua regione	13
Favorites (Preferiti)	15
Modifica della password	19
Cambiare la lingua del Console di gestione AWS	22
Accesso alle tue informazioni AWS	24
Accesso alle informazioni sull'account	25
Accesso alle informazioni sull'organizzazione	25
Accesso alle informazioni sulle quote di servizio	26
Accesso alle informazioni di fatturazione	26
Accesso a più account	26
Utilizzo delle azioni consigliate	27
Caratteristiche delle azioni AWS consigliate	28
Utilizzo delle azioni consigliate	28
Monitoraggio con registri CloudTrail	29
AWS Console Home	32
Visualizzazione di tutti i AWS servizi	32
Lavorare con i widget	32

Gestione dei widget	33
Le mie applicazioni	34
Funzionalità di myApplications	35
Servizi correlati	36
Accesso a myApplications	36
Prezzi	36
Regioni supportate	36
Applicazioni	38
Resources	46
Dashboard myApplications	49
Chattare con Amazon Q	54
Inizia a usare Amazon Q	54
Domande di esempio	54
Console di gestione AWS Accesso privato	55
Console Regioni AWS di servizio e funzionalità supportate	55
Panoramica dei controlli di sicurezza di Console di gestione AWS Private Access	61
Restrizioni relative all'account Console di gestione AWS dalla tua rete	61
Connettività dalla propria rete a Internet	61
Endpoint VPC e configurazione DNS richiesti	61
Configurazione di DNS	62
Endpoint VPC e DNS configurazione per i servizi AWS	64
Implementazione delle policy di controllo dei servizi e delle policy degli endpoint VPC	66
Policy di controllo dei servizi	66
Policy di endpoint VPC	67
Implementazione di policy basate su identità e altri tipi di policy	68
Chiavi contestuali delle condizioni AWS globali supportate	69
Come funziona Console di gestione AWS Private Access con aws: SourceVpc	69
In che modo si riflettono i diversi percorsi di rete CloudTrail	70
Prova Private Access Console di gestione AWS	71
Test della configurazione con Amazon EC2	71
Configurazione di prova con Amazon WorkSpaces	86
Test della configurazione VPC con le policy IAM	103
Architettura di riferimento	104
AWS Personalizzazione dell'esperienza utente	106
Accesso alla personalizzazione dell'esperienza utente	106
Nozioni di base	106

Documentazione di riferimento delle API	107
Azioni	107
Errori comuni	112
Monitoraggio con registri CloudTrail	114
Eventi di gestione UXC in CloudTrail	114
Esempi di eventi UXC	29
AWS politiche gestite	117
AWSManagementConsoleBasicUserAccess	117
AWSManagementConsoleAdministratorAccess	118
Aggiornamenti delle policy	119
Markdown in AWS	121
Paragrafi, Interlinea e Linee orizzontali	121
Intestazioni	122
Formattazione del testo	122
Link	123
Elenchi	123
Tabelle e pulsanti (CloudWatch dashboard)	123
Risoluzione dei problemi	125
La pagina non si sta caricando correttamente	125
Il mio browser visualizza un errore di «accesso negato» durante la connessione al Console di gestione AWS	126
Il mio browser mostra errori di timeout durante la connessione a Console di gestione AWS	127
Vorrei cambiare la lingua di Console di gestione AWS ma non riesco a trovare il menu di selezione della lingua in fondo alla pagina	127
Cronologia dei documenti	128
.....	cxxxii

Qual è il Console di gestione AWS?

[Console di gestione AWS](#) Si tratta di un'applicazione basata sul Web che contiene e fornisce l'accesso centralizzato a tutte le singole console di AWS servizio. È possibile utilizzare Unified Navigation per Console di gestione AWS cercare servizi, visualizzare notifiche, accedere AWS CloudShell, accedere all'account e alle informazioni di fatturazione e personalizzare le impostazioni generali della console. La home page di si Console di gestione AWS chiama. AWS Console Home Da AWS Console Home, puoi gestire le tue AWS applicazioni e accedere a tutte le altre singole console di servizio. Puoi anche personalizzare AWS Console Home per mostrare altre informazioni utili sulle AWS tue risorse utilizzando i widget. Puoi aggiungere, rimuovere e riorganizzare widget come Recentemente visitati, AWS Health e altro.

Argomenti

- [Caratteristiche di Console di gestione AWS](#)
- [Console AWS di servizio individuali in Console di gestione AWS](#)
- [Accedere al Console di gestione AWS](#)
- [Accesso Console di gestione AWS con dispositivi mobili](#)

Caratteristiche di Console di gestione AWS

Le caratteristiche importanti di Console di gestione AWS includono quanto segue:

- Passa alle console di AWS servizio: puoi utilizzare Unified Navigation per accedere alle console di servizio visitate di recente, visualizzare e aggiungere servizi all'elenco dei preferiti, accedere alle impostazioni della console e accedere. Notifiche all'utente AWS
- Cerca AWS servizi e altre AWS informazioni: usa Unified Search per cercare AWS servizi e funzionalità e prodotti sul marketplace. AWS
- Personalizza la console: puoi utilizzare le impostazioni unificate per personalizzare vari aspetti di. Console di gestione AWS Ciò include la lingua, la regione predefinita e altro ancora.
- Esegui comandi CLI: AWS CloudShell è accessibile direttamente dalla console. Puoi usarlo CloudShell per eseguire i comandi AWS CLI sui tuoi servizi preferiti.
- Accedi a tutte le notifiche di AWS eventi: puoi utilizzare il Console di gestione AWS per accedere alle notifiche da Notifiche all'utente AWS e AWS Health.

- Personalizza AWS Console Home: puoi personalizzare completamente la tua AWS Console Home esperienza utilizzando i widget.
- Crea e gestisci AWS applicazioni: gestisci e monitora il costo, lo stato di salute, il livello di sicurezza e le prestazioni delle tue applicazioni utilizzando MyApplications in. AWS Console Home
- Chatta con Amazon Q: puoi ottenere risposte basate sull'assistente di intelligenza artificiale generativa (AI) alle tue Servizio AWS domande direttamente dalla console. Puoi anche metterti in contatto con un agente dal vivo per ricevere ulteriore assistenza.
- Controlla l'accesso agli AWS account nella tua rete: puoi utilizzare Console di gestione AWS Private Access per limitare l'accesso Console di gestione AWS a un insieme specifico di AWS account noti quando il traffico proviene dall'interno della tua rete.

Console AWS di servizio individuali in Console di gestione AWS

Ogni AWS servizio dispone di una propria console di servizio individuale a cui è possibile accedere all' Console di gestione AWS interno di. Le impostazioni scelte in Impostazioni unificate per Console di gestione AWS, come la modalità visiva e la lingua predefinita, vengono applicate a tutte le singole AWS console. AWS [le console di servizio offrono un'ampia gamma di strumenti per il cloud computing, oltre a informazioni sull'account e sulla fatturazione](#). Se desideri saperne di più su un servizio specifico e sulla relativa console, ad esempio Amazon Elastic Compute Cloud, accedi alla sua console utilizzando Unified Search nella barra di Console di gestione AWS navigazione e accedi alla EC2 documentazione di Amazon dal sito Web [AWS Documentation](#).

Quando accedi alla console di un singolo AWS servizio, puoi comunque accedere alle funzionalità di Console di gestione AWS utilizzo di Unified Navigation nella parte superiore della console. Puoi lasciare un feedback per la console di un singolo servizio accedendo a quella console e selezionando Feedback nel piè di pagina della pagina.

Accedere al Console di gestione AWS

È possibile accedere Console di gestione AWS a <https://console.aws.amazon.com/>.

Accesso Console di gestione AWS con dispositivi mobili

[Console di gestione AWS](#) È progettato per funzionare su tablet e altri tipi di dispositivi mobili:

- Lo spazio orizzontale e verticale è ingrandito per una migliore visualizzazione sullo schermo.

- I pulsanti e selettori sono più grandi per una migliore esperienza di tocco.

Per accedere a Console di gestione AWS su un dispositivo mobile, è necessario utilizzare il AWS Console Mobile Application. Questa app è disponibile per Android e iOS. L'applicazione Console Mobile fornisce attività relative ai dispositivi mobili che si accompagnano bene all'esperienza web completa. Ad esempio, puoi visualizzare e gestire facilmente le EC2 istanze Amazon e gli CloudWatch allarmi Amazon esistenti dal tuo telefono. Per ulteriori informazioni, consulta [Cos'è il? AWS Console Mobile Application](#) nella Guida AWS Console Mobile Application per l'utente.

Puoi scaricare l'applicazione Console Mobile da [Amazon Appstore](#), [Google Play](#) e [App Store iOS](#).

Guida introduttiva a un servizio in Console di gestione AWS

La [Console di gestione AWS](#) offre molteplici modi per spostarsi alle singole console dei servizi.

Per aprire una console per un servizio

Esegui una di queste operazioni:

- Nella casella di ricerca sulla barra di navigazione, inserisci il nome parziale o completo del servizio. Alla voce Servizi, scegli il servizio che desideri dall'elenco dei risultati della ricerca. Per ulteriori informazioni, consulta [Ricerca di prodotti, servizi, funzionalità e altro utilizzando la ricerca unificata nel Console di gestione AWS](#).
- Nel widget Recently visited services (Servizi visitati di recente), scegliere il nome di un servizio.
- Nel widget Servizi visitati di recente, scegli Visualizza tutti i AWS servizi. Quindi, nella pagina Tutti i AWS servizi, scegli un nome di servizio.
- Sulla barra di navigazione, scegli Servizi per aprire l'elenco completo dei servizi. Quindi scegli un servizio in Visitati di recente o Tutti i servizi.

Utilizzo della barra Console di gestione AWS di navigazione tramite Unified Navigation

Questo argomento descrive come utilizzare la navigazione unificata. La navigazione unificata si riferisce alla barra di navigazione che funge da intestazione e piè di pagina della console. Puoi utilizzare Unified Navigation per:

- Cerca e accedi a AWS servizi, funzionalità, prodotti e altro ancora.
- Avvia AWS Cloudshell.
- Accedi alle AWS notifiche e agli eventi AWS Health.
- Ottieni supporto da una varietà di fonti di AWS conoscenza.
- Configura il Console di gestione AWS file scegliendo la lingua predefinita, la modalità visiva, la regione e altro ancora.
- Accedi all'account, all'organizzazione, alla quota di servizio e alle informazioni di fatturazione.

Argomenti

- [Accedendo al menu Servizi in Console di gestione AWS](#)
- [Ricerca di prodotti, servizi, funzionalità e altro utilizzando la ricerca unificata nel Console di gestione AWS](#)
- [Avvio AWS CloudShell dalla barra di navigazione in Console di gestione AWS](#)
- [Accesso alle AWS notifiche e agli eventi Health](#)
- [Ottenere supporto](#)
- [Configurazione dell' Console di gestione AWS utilizzo delle impostazioni unificate](#)
- [Accesso all' AWS account, all'organizzazione, alla quota di servizio e alle informazioni di fatturazione nel Console di gestione AWS](#)
- [Accesso a più account](#)
- [AWS Azioni consigliate in Console di gestione AWS](#)

Accedendo al menu Servizi in Console di gestione AWS

Puoi utilizzare il menu Servizi, accanto alla barra di ricerca per accedere ai servizi visitati di recente, visualizzare l'elenco dei Preferiti e visualizzare tutti i AWS servizi. Puoi anche visualizzare i servizi per tipo scegliendo un tipo di servizio, ad esempio Analytics o Application Integration.

La procedura seguente descrive come accedere al menu Servizi.

Per accedere al menu Servizi

1. Accedi alla [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli Servizi (:).
3. (Facoltativo) Scegli Visitati di recente per visualizzare i servizi e le applicazioni con cui hai interagito di recente.
4. (Facoltativo) Scegliete Preferiti per visualizzare l'elenco dei Preferiti.
5. (Facoltativo) Scegliete Tutte le applicazioni per visualizzare le applicazioni MyApplications.
6. (Facoltativo) Scegliete Tutti i servizi per visualizzare un elenco alfabetico di tutti i AWS servizi.
7. (Facoltativo) Scegliete un tipo di servizio per visualizzare AWS i servizi per tipo.

Ricerca di prodotti, servizi, funzionalità e altro utilizzando la ricerca unificata nel Console di gestione AWS

La casella di ricerca nella barra di navigazione fornisce uno strumento di ricerca unificato per trovare AWS servizi e funzionalità, documentazione di servizio, Marketplace AWS prodotti e altro ancora. Basta inserire alcuni caratteri o una domanda per iniziare a generare risultati da tutti i tipi di contenuto disponibili. Ogni parola inserita perfeziona ulteriormente i risultati. I tipi di contenuto disponibili includono:

- Servizi
- Funzionalità
- Documenti
- Blog
- Articoli di conoscenza
- Eventi

- Esercitazioni
- Marketplace
- Resources

Note

Puoi filtrare i risultati della ricerca per mostrare solo le risorse eseguendo una ricerca mirata. Per eseguire una ricerca mirata, inseriscila `/Resources` all'inizio della query nella barra di ricerca e scegli `/Resources` dal menu a discesa. Quindi inserisci il resto della tua ricerca.

Argomenti

- [Ricerca di AWS prodotti nel Console di gestione AWS](#)
- [Perfezionamento della ricerca in Console di gestione AWS](#)
- [Visualizzazione delle funzionalità di un servizio in Console di gestione AWS](#)

Ricerca di AWS prodotti nel Console di gestione AWS

La procedura seguente descrive in dettaglio come cercare AWS prodotti utilizzando lo strumento di ricerca.

Per cercare un servizio, una funzionalità, una documentazione o un Marketplace AWS prodotto

1. Nella casella di ricerca sulla barra di navigazione del [Console di gestione AWS](#), inserisci la tua richiesta.
2. Scegli un link per navigare verso la destinazione desiderata.

Tip

Inoltre, puoi utilizzare la tastiera per passare rapidamente al primo risultato della ricerca. Innanzitutto, premi `Alt+S` (Windows) oppure `Opzione+S` (macOS) per accedere alla barra di ricerca. Quindi, inizia a inserire il termine di ricerca. Quando il risultato desiderato viene visualizzato nella parte superiore dell'elenco, premi `Invio`. Ad esempio, per accedere rapidamente alla console Amazon EC2, digita `ec2` e premi `Invio`.

Perfezionamento della ricerca in Console di gestione AWS

Puoi affinare la ricerca per tipo di contenuto e visualizzare informazioni aggiuntive sui risultati della ricerca.

Per affinare la ricerca a un tipo di contenuto specifico

1. Nella casella di ricerca sulla barra di navigazione di [Console di gestione AWS](#), inserisci la tua richiesta.
2. Scegli uno dei tipi di contenuto accanto ai risultati della ricerca.
3. (Facoltativo) Per visualizzare tutti i risultati per una categoria specifica:
 - Scegli Mostra altro. Si aprirà una nuova scheda con i risultati.
4. (Facoltativo) Per visualizzare informazioni aggiuntive sui risultati della ricerca:
 - a. Nei risultati della ricerca, posiziona il cursore su un risultato di ricerca.
 - b. Visualizza le informazioni aggiuntive disponibili.

Visualizzazione delle funzionalità di un servizio in Console di gestione AWS

È possibile visualizzare le funzionalità di un servizio direttamente dai risultati della ricerca.

Per visualizzare le funzionalità di un servizio

1. Nella casella di ricerca sulla barra di navigazione del [Console di gestione AWS](#), inserisci la tua richiesta.
2. Nei risultati della ricerca, posiziona il cursore su un servizio in Servizi.
3. Scegli uno dei link nelle Funzionalità principali.

Avvio AWS CloudShell dalla barra di navigazione in Console di gestione AWS

AWS CloudShell è una shell preautenticata basata su browser che puoi avviare direttamente dalla barra di navigazione. Console di gestione AWS È possibile eseguire AWS CLI comandi sui servizi utilizzando la shell preferita (Bash o Z shell). PowerShell

È possibile eseguire l'avvio CloudShell Console di gestione AWS utilizzando uno dei due metodi seguenti:

- Scegli l' CloudShell icona nel piè di pagina della console.
- Scegli l' CloudShell icona nella barra di navigazione della console.

Per ulteriori informazioni su questo servizio, consulta la [Guida per l'utente di AWS CloudShell](#).

Per informazioni su Regioni AWS dove AWS CloudShell è disponibile, consulta l'[Elenco dei servizi AWS regionali](#). La selezione della regione della console è sincronizzata con la CloudShell regione. Se non CloudShell è disponibile in una regione selezionata, CloudShell funzionerà nella regione più vicina.

Accesso alle AWS notifiche e agli eventi Health

Puoi accedere ad alcune AWS notifiche e visualizzare gli eventi sanitari dalla barra di navigazione. Puoi anche accedere Notifiche all'utente AWS alla visualizzazione di tutte le AWS notifiche e della AWS Health Dashboard dalla barra di navigazione.

Per ulteriori informazioni, consulta [Cos'è Notifiche all'utente AWS?](#) nella Guida Notifiche all'utente AWS per l'utente e [Cos'è AWS Health?](#) nella Guida per l'AWS Health utente

La procedura seguente descrive come accedere alle informazioni sull' AWS evento.

Per accedere alle informazioni sull' AWS evento

1. Accedi alla [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli l'icona a forma di campana.
3. Visualizza le notifiche e gli eventi sanitari.
4. (Facoltativo) Scegli Visualizza tutte le notifiche per accedere alla Notifiche all'utente console.
5. (Facoltativo) Scegli vedi tutti gli eventi Health per accedere alla AWS Health console.

Ottenere supporto

Puoi ottenere assistenza scegliendo l'icona del punto interrogativo nella barra di navigazione. Dal menu di assistenza, puoi scegliere di:

- Vai alla console di servizio Support Center

- Fatti aiutare da un esperto da AWS IQ
- Visualizza le informazioni curate dagli articoli della community e dal centro di conoscenza su Re:POST AWS
- Vai alla documentazione AWS
- Vai ai AWS corsi di formazione
- Vai al Centro risorse per AWS iniziare
- Lascia un feedback per qualsiasi console di servizio a cui stai attualmente accedendo

Note

Puoi farlo anche selezionando Feedback nel piè di pagina della console. Il titolo della modalità che si apre mostra per quale console stai lasciando un feedback

Puoi anche ricevere assistenza in qualsiasi momento dalla console, connetterti con un agente dal vivo e porre qualsiasi domanda in merito AWS chattando con Q. AWS Per ulteriori informazioni, consulta [???](#).

Configurazione dell' Console di gestione AWS utilizzo delle impostazioni unificate

Questo argomento descrive come configurare l' Console di gestione AWS utilizzo della pagina Impostazioni unificate per impostare impostazioni predefinite applicabili a tutte le console di servizio.

Argomenti

- [Configurazione delle impostazioni unificate in Console di gestione AWS](#)
- [Scegli la tua regione](#)
- [Preferiti in Console di gestione AWS](#)
- [Modifica della password nel Console di gestione AWS](#)
- [Cambiare la lingua del Console di gestione AWS](#)

Configurazione delle impostazioni unificate in Console di gestione AWS

È possibile configurare impostazioni e impostazioni predefinite, come visualizzazione, lingua e regione, dalla pagina Impostazioni unificate Console di gestione AWS . È possibile accedere alle

impostazioni unificate tramite la barra di navigazione in Unified Navigation. La modalità visiva e la lingua predefinita possono essere impostate anche direttamente dalla barra di navigazione. Queste modifiche si applicano a tutte le console di servizio.

Important

Per garantire che le impostazioni, i servizi preferiti e i servizi visitati di recente persistano a livello globale, questi dati vengono archiviati in tutte le aree Regioni AWS, comprese le regioni che sono disabilitate per impostazione predefinita. Queste Regioni sono Africa (Città del Capo), Asia Pacifico (Hong Kong), Asia Pacifico (Hyderabad), Asia Pacifico (Giacarta), Europa (Milano), Europa (Spagna), Europa (Zurigo), Medio Oriente (Bahrein) e Medio Oriente (Emirati Arabi Uniti). È ancora necessario [abilitare manualmente una regione](#) per accedervi e creare e gestire le risorse in tale regione. Se non desideri archiviare tutti questi dati Regioni AWS, scegli Ripristina tutto per cancellare le impostazioni, quindi disattiva la memorizzazione dei servizi visitati di recente nella Gestione delle impostazioni.

Argomenti

- [Accesso alle impostazioni unificate in Console di gestione AWS](#)
- [Reimpostazione delle impostazioni unificate in Console di gestione AWS](#)
- [Modifica delle impostazioni unificate in Console di gestione AWS](#)
- [Modifica della modalità visiva di Console di gestione AWS](#)

Accesso alle impostazioni unificate in Console di gestione AWS

La procedura seguente descrive come accedere alle impostazioni unificate.

Per accedere alle impostazioni unificate

1. Accedi alla [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli l'icona a forma di ingranaggio (#).
3. Per aprire la pagina Impostazioni unificate, scegli Visualizza tutte le impostazioni utente.

Reimpostazione delle impostazioni unificate in Console di gestione AWS

Puoi eliminare tutte le configurazioni delle impostazioni unificate e ripristinare le impostazioni predefinite ripristinando le impostazioni unificate.

Note

Ciò influisce su diverse aree di AWS, inclusi i servizi preferiti nella navigazione e nel menu Servizi, i servizi visitati di recente nei widget Console Home e in AWS Console Mobile Application, e tutte le impostazioni che si applicano ai vari servizi, come la lingua predefinita, la regione predefinita e la modalità visiva.

Per ripristinare tutte le impostazioni unificate

1. Accedi alla [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli l'icona a forma di ingranaggio (#).
3. Apri la pagina delle impostazioni unificate selezionando Visualizza tutte le impostazioni utente.
4. Scegli Ripristina tutto.

Modifica delle impostazioni unificate in Console di gestione AWS

La procedura seguente descrive come modificare le impostazioni preferite.

Per modificare le impostazioni unificate

1. Accedi alla [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli l'icona a forma di ingranaggio (#).
3. Apri la pagina delle impostazioni unificate selezionando Visualizza tutte le impostazioni utente.
4. Scegliere Edit (Modifica) accanto alle impostazioni desiderate:
 - Localizzazione e regione di default:
 - Lingua consente di selezionare la lingua predefinita per il testo della console.
 - Default Region (Regione di default) consente di selezionare una Regione predefinita che si applica ogni volta che si effettua l'accesso. È possibile selezionare una delle Regioni disponibili per il proprio account. È anche possibile selezionare l'ultima Regione utilizzata come Regione predefinita.

Per ulteriori informazioni sul routing della Regione, nella [Console di gestione AWS](#) consulta [Scelta di una Regione](#).

- Visualizzazione:
 - La modalità visiva consente di impostare la console sulla modalità chiara, la modalità scura o la modalità di visualizzazione predefinita del browser.

La modalità scura è una caratteristica beta e potrebbe non essere applicabile a tutte le console di servizio AWS .

- Visualizzazione barra preferiti attiva/disattiva la visualizzazione della barra Preferiti tra il nome completo del servizio con la relativa icona o solo l'icona del servizio.
- La dimensione dell'icona della barra Preferiti alterna la dimensione dell'icona del servizio nella barra Preferiti tra piccole (16x16 pixel) e grandi (24x24 pixel).
- Gestione delle impostazioni:
 - Ricorda i servizi visitati di recente ti consente di scegliere se Console di gestione AWS ricordare i servizi visitati di recente. La disattivazione di questa opzione elimina anche la cronologia dei servizi visitati di recente, quindi non vedrai più i servizi visitati di recente nel menu Servizio o nei AWS Console Mobile Application widget di Console Home.

5. Scegli Save changes (Salva modifiche).

Modifica della modalità visiva di Console di gestione AWS

La modalità visiva imposta la console sulla modalità chiara, sulla modalità scura o sulla modalità di visualizzazione predefinita del browser.

Per modificare la modalità visiva dalla barra di navigazione

1. Accedi alla [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli l'icona a forma di ingranaggio (#).
3. Per la modalità visiva, scegli Chiara per la modalità chiara, Scura per la modalità scura o Predefinita del browser per la modalità di visualizzazione predefinita del browser.

Scegli la tua regione

Per molti servizi, è possibile sceglierne una Regione AWS che specifichi dove vengono gestite le risorse. Le regioni sono insiemi di AWS risorse situate nella stessa area geografica. Non è necessario

scegliere una regione per [Console di gestione AWS](#)o per alcuni servizi, ad esempio AWS Identity and Access Management. Per ulteriori informazioni sulle Regioni AWS, consulta [Managing Regioni AWS](#) (Gestione delle Regioni AWS) nei Riferimenti generali di AWS..

Note

Se hai creato AWS risorse ma non le vedi nella console, è possibile che la console visualizzi risorse provenienti da una regione diversa. Alcune risorse (ad esempio le istanze Amazon EC2) sono specifiche della Regione in cui sono state create.

Argomenti

- [Scegliendo una regione dalla barra di navigazione in Console di gestione AWS](#)
- [Impostazione della regione predefinita in Console di gestione AWS](#)

Scegliendo una regione dalla barra di navigazione in Console di gestione AWS

La procedura seguente descrive in dettaglio come modificare la regione dalla barra di navigazione.

Per scegliere una regione dalla barra di navigazione

1. Accedi alla [Console di gestione AWS](#).
2. Sulla barra di navigazione scegliere il nome della Regione attualmente visualizzata.
3. Scegli una regione a cui passare.

Impostazione della regione predefinita in Console di gestione AWS

La procedura seguente descrive in dettaglio come modificare la regione predefinita dalla pagina Impostazioni unificate.

Per impostare la regione predefinita

1. Nella barra di navigazione, scegli l'icona a forma di ingranaggio (#).
2. Scegli Visualizza tutte le impostazioni utente per accedere alla pagina Impostazioni unificate.
3. Scegliere Edit (Modifica) accanto a Localization and default Region (Localizzazione e regione di default).

4. In Regione predefinita, scegli una regione.

Note

Se non selezioni una Regione di default, la Regione di default sarà l'ultima Regione visitata.

5. Scegliere Save settings (Salva impostazioni).
6. (Facoltativo) Scegliete Vai alla nuova regione predefinita per passare immediatamente alla nuova regione predefinita.

Preferiti in Console di gestione AWS

Per accedere più rapidamente ai servizi e alle applicazioni utilizzati di frequente, è possibile salvare le relative console di servizio in un elenco di Preferiti. È possibile aggiungere e rimuovere i preferiti utilizzando Console di gestione AWS. Quando si aggiunge un servizio o un'applicazione ai Preferiti, questo viene visualizzato nella barra rapida Preferiti.

Argomenti

- [Aggiungere preferiti in Console di gestione AWS](#)
- [Accesso ai preferiti in Console di gestione AWS](#)
- [Rimozione dei preferiti in Console di gestione AWS](#)

Aggiungere preferiti in Console di gestione AWS

È possibile aggiungere servizi e applicazioni ai preferiti dal menu Servizi e dal menu Visitati di recente. Puoi anche aggiungere servizi ai preferiti utilizzando la pagina dei risultati di ricerca nella casella di ricerca. I servizi e le applicazioni che aggiungi ai preferiti vengono visualizzati nella barra rapida Preferiti.

Argomenti

- [Barra rapida Preferiti nella Console di gestione AWS](#)
- [Aggiungere servizi ai preferiti nella Console di gestione AWS](#)
- [Aggiungere applicazioni ai preferiti nella Console di gestione AWS](#)

Barra rapida Preferiti nella Console di gestione AWS

La barra rapida dei preferiti viene visualizzata quando è stato aggiunto almeno un AWS servizio o un'applicazione ai preferiti. La barra rapida dei preferiti si trova dopo la barra di navigazione ed è visibile in tutte le console di AWS servizio, in modo da poter accedere rapidamente ai servizi e alle applicazioni preferiti. È possibile riorganizzare l'ordine dei servizi e delle applicazioni nella barra rapida dei preferiti trascinando un servizio o un'applicazione verso sinistra o destra.

Aggiungere servizi ai preferiti nella Console di gestione AWS

Puoi aggiungere servizi ai preferiti dal menu Servizi o dalla pagina dei risultati della ricerca dalla casella di ricerca.

Services menu


Per aggiungere preferiti dal menu Servizi

1. Apri la [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli Servizi (:).
3. (Facoltativo) Aggiungi ai preferiti un servizio visitato di recente:
 - a. In Visitati di recente, posiziona il cursore su un servizio.
 - b. Seleziona la stella accanto al nome del servizio.
4. Scegli Tutti i servizi.
5. Passa il cursore sul servizio scelto.
6. Seleziona la stella accanto al nome del servizio.

Search box

Per aggiungere preferiti dalla casella di ricerca

1. Apri la [Console di gestione AWS](#).
2. Inserisci il nome di un servizio nella casella di ricerca.
3. Nella pagina dei risultati della ricerca, seleziona la stella accanto al nome del servizio.

 Note


Dopo aver aggiunto un servizio ai preferiti, questo viene aggiunto alla barra rapida dei preferiti che segue la barra di navigazione.

Aggiungere applicazioni ai preferiti nella Console di gestione AWS

Puoi aggiungere applicazioni ai preferiti dal menu Servizi.

Per aggiungere preferiti dal menu Servizi

1. Apri la [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli Servizi (:).
3. (Facoltativo) Aggiungi ai preferiti un'applicazione visitata di recente:
 - a. In Visitate di recente, posiziona il cursore su un'applicazione.
 - b. Seleziona la stella accanto al nome dell'applicazione.
4. Selezionare Applications (Applicazioni).
5. Passa il cursore sull'applicazione scelta.
6. Seleziona la stella accanto al nome dell'applicazione.

 Note

Dopo aver aggiunto un'applicazione ai preferiti, questa viene aggiunta alla barra rapida dei preferiti che segue la barra di navigazione.

Accesso ai preferiti in Console di gestione AWS


È possibile accedere ai servizi e alle applicazioni aggiunti ai preferiti dal menu Servizi, dalla barra rapida dei preferiti e dal widget Preferiti.

Services menu

Per accedere ai preferiti dal menu Servizi

1. Apri la [Console di gestione AWS](#).

2. Nella barra di navigazione, scegli Servizi (:).
3. Scegli Preferiti.
4. Visualizza i servizi e le applicazioni che hai aggiunto ai preferiti.
5. (Facoltativo) Visualizza le risorse dell'applicazione:
 - a. Seleziona un'applicazione.
 - b. (Facoltativo) Seleziona una [vista](#).
 - c. Visualizza le tue risorse.
 - d. (Facoltativo) Seleziona un filtro. Puoi filtrare le tue risorse per Proprietà o per Tag. Per ulteriori informazioni, consulta il [riferimento alla sintassi delle query di ricerca per Resource Explorer](#) nella Guida per l'Esploratore di risorse AWS utente.
 - e. (Facoltativo) Seleziona una risorsa per visualizzarla nella console di servizio pertinente.

 Tip

Puoi continuare a sfogliare le risorse da dove avevi interrotto scegliendo Servizi (:). Inoltre, i filtri di ricerca applicati persisteranno.


Favorites quickbar

Per accedere ai preferiti dalla barra rapida dei preferiti

1. Apri la [Console di gestione AWS](#).
2. Visualizza i servizi e le applicazioni nella barra rapida dei preferiti.

Favorites widget

Per accedere ai preferiti dal widget Preferiti

1. Apri la [Console di gestione AWS](#).
2. (Facoltativo) Aggiungi il widget Preferiti se non lo hai:
 - a. Scegli il pulsante + Aggiungi widget nella home page della console.
 - b. Nel menu Aggiungi widget, trascina il widget Preferiti utilizzando l'icona  e posizionalo nella home page della console.

3. Visualizza i servizi e le applicazioni nel widget Preferiti.

Per ulteriori informazioni sui widget, vedere [the section called “Lavorare con i widget”](#).

Rimozione dei preferiti in Console di gestione AWS

È possibile rimuovere servizi e applicazioni dai preferiti utilizzando il menu Servizi. Puoi anche rimuovere i servizi utilizzando la pagina dei risultati di ricerca dalla barra di ricerca.

Services menu

Per rimuovere i preferiti dal menu Servizi

1. Apri la [Console di gestione AWS](#).
2. Sulla barra di navigazione, scegli Services (Servizi).
3. Scegli Preferiti.
4. Deseleziona la stella accanto al servizio o all'applicazione.

Search box

Note

Attualmente, puoi rimuovere i servizi solo utilizzando la pagina dei risultati di ricerca dalla barra di ricerca.

Per rimuovere i preferiti dalla casella di ricerca

1. Apri la [Console di gestione AWS](#).
2. Inserisci il nome di un servizio nella casella di ricerca.
3. Nella pagina dei risultati di ricerca, deseleziona la stella accanto al nome del servizio.

Modifica della password nel Console di gestione AWS

Potresti essere in grado di modificare la password in [Console di gestione AWS](#) base al tipo di utente e alle tue autorizzazioni. L'argomento seguente descrive come modificare la password per ogni tipo di utente.

Argomenti

- [Utenti root in Console di gestione AWS](#)
- [Utenti IAM in Console di gestione AWS](#)
- [Utenti di IAM Identity Center in Console di gestione AWS](#)
- [Identità federate in Console di gestione AWS](#)

Utenti root in Console di gestione AWS

Gli utenti root possono modificare le proprie password direttamente da Console di gestione AWS. Un utente root è il proprietario dell'account con accesso completo a tutti i AWS servizi e le risorse. Sei l'utente root se hai creato l'AWS account e accedi utilizzando l'email e la password dell'utente root. Per ulteriori informazioni, consulta [Utente root](#) nella Guida AWS IAM Identity Center per l'utente.

Per modificare la password come utente root

1. Accedi alla [Console di gestione AWS](#).
2. Sulla barra di navigazione, scegli il nome dell'account.
3. Scegli Security Credentials (Credenziali di sicurezza).
4. Le opzioni visualizzate variano a seconda del Account AWS tipo. Seguire le istruzioni visualizzate nella console per modificare la password.
5. Inserisci la password corrente una volta e la nuova password due volte.

La nuova password deve avere almeno 8 caratteri e deve includere quanto segue:

- Almeno un simbolo
 - Almeno un numero
 - Almeno una lettera maiuscola
 - Almeno una lettera minuscola
6. Scegliere Change Password (Modifica password) o Save changes (Salva le modifiche).

Utenti IAM in Console di gestione AWS

Gli utenti IAM potrebbero essere in grado di modificare la propria password in Console di gestione AWS base alle proprie autorizzazioni. Altrimenti, devono utilizzare un portale di AWS accesso. Un utente IAM è un'identità all'interno del tuo AWS account a cui sono concesse autorizzazioni

personalizzate specifiche. Sei un utente IAM se non hai creato l' AWS account e il tuo amministratore o dipendente dell'help desk ti ha fornito le credenziali di accesso che includono un ID AWS account o un alias dell'account, un nome utente IAM e una password. Per ulteriori informazioni, consulta l'[utente IAM nella Guida per l'utente](#).Accedi ad AWS

Se disponi delle autorizzazioni previste dalla seguente policy: [AWS: Consente agli utenti IAM di modificare la password della propria console nella pagina delle credenziali di sicurezza](#), puoi modificare la password dalla console. Per ulteriori informazioni, consulta [Come un utente IAM cambia la propria password nella Guida](#) per l'AWS Identity and Access Management utente.

Se non disponi delle autorizzazioni necessarie per modificare la password, Console di gestione AWS consulta la sezione [Reimpostazione della password utente nella Guida per AWS IAM Identity Center l'utente](#).AWS IAM Identity Center

Utenti di IAM Identity Center in Console di gestione AWS

AWS IAM Identity Center gli utenti devono modificare la propria password da un portale di AWS accesso. Per ulteriori informazioni, vedere [Reimpostazione della password AWS IAM Identity Center utente](#) nella Guida per l'AWS IAM Identity Center utente.

Un utente IAM Identity Center è un utente il cui AWS account fa parte e AWS Organizations che accede tramite il portale di AWS accesso con un URL univoco. Questi utenti possono essere creati direttamente negli utenti di IAM Identity Center o in Active Directory o in un altro provider di identità esterno. Per ulteriori informazioni, consulta [AWS IAM Identity Center user](#) nella Guida Accedi ad AWS per l'utente.

Identità federate in Console di gestione AWS

Gli utenti con identità federata devono modificare la propria password da un portale di AWS accesso. Per ulteriori informazioni, consulta [Reimpostazione della password AWS IAM Identity Center utente](#) nella Guida per l'AWS IAM Identity Center utente.

Gli utenti di identità federata accedono utilizzando un provider di identità esterno (IdP). Sei un'identità federata se:

- Accedi al tuo AWS account o alle tue risorse con credenziali di terze parti come Login with Amazon, Facebook o Google.
- Utilizza le stesse credenziali per accedere ai sistemi e ai AWS servizi aziendali e utilizza un portale aziendale personalizzato a cui accedere. AWS

Per ulteriori informazioni, consulta [Federated identity](#) nella Guida per l'Accedi ad AWS utente. .

Cambiare la lingua del Console di gestione AWS

L' AWS Console Home esperienza include la pagina delle impostazioni unificate in cui è possibile modificare la lingua predefinita per AWS i servizi in. Console di gestione AWS Puoi anche cambiare rapidamente la lingua predefinita dal menu delle impostazioni della barra di navigazione.

Note

Le seguenti procedure modificano la lingua per tutte le console AWS di servizio, ma non per la AWS documentazione. Per modificare la lingua della documentazione, utilizza il menu delle lingue in altro a destra nella pagina della documentazione.

Argomenti

- [Lingue supportate](#)
- [Modifica della lingua predefinita dalla barra di navigazione in Console di gestione AWS](#)
- [Modifica della lingua predefinita tramite Impostazioni unificate nel Console di gestione AWS](#)

Lingue supportate

Console di gestione AWS Attualmente supporta le seguenti lingue:

- Inglese (Stati Uniti)
- Inglese (Regno Unito)
- Bahasa Indonesia
- Tedesco
- Spagnolo
- Francese
- Giapponese
- Italiano
- Portoghese
- Coreano
- Cinese (semplificato)

- Cinese (tradizionale)
- Turco

Modifica della lingua predefinita dalla barra di navigazione in Console di gestione AWS

La procedura seguente descrive come modificare la lingua predefinita direttamente dalla barra di navigazione.

Per cambiare la lingua predefinita dalla barra di navigazione

1. Accedi alla [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli l'icona a forma di ingranaggio (#).
3. Per Lingua, scegli la lingua Predefinita del browser o la lingua preferita dall'elenco a discesa.


Modifica della lingua predefinita tramite Impostazioni unificate nel Console di gestione AWS

La procedura seguente descrive in dettaglio come modificare la lingua predefinita dalla pagina Impostazioni unificate.

Per cambiare la lingua predefinita in Impostazioni unificate

1. Accedi alla [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli l'icona a forma di ingranaggio (#).
3. Per aprire la pagina Impostazioni unificate, scegli Visualizza tutte le impostazioni utente.
4. In Unified Settings (Impostazioni unificate), scegliere Edit (Modifica) accanto a Localization and default Region (Localizzazione e regione di default).
5. Per selezionare la lingua desiderata per la console, scegli una delle seguenti opzioni:
 - Scegli Impostazione predefinita del browser dall'elenco a discesa, quindi scegli Salva impostazioni.

Il testo della console per tutti i AWS servizi viene visualizzato nella lingua preferita che hai impostato nelle impostazioni del browser.

 Note


L'impostazione predefinita del browser supporta solo le lingue supportate dalla Console di gestione AWS.

- Scegli la lingua preferita dall'elenco a discesa, quindi scegli Salva impostazioni.

Il testo della console per tutti i AWS servizi viene visualizzato nella lingua preferita.

Accesso all' AWS account, all'organizzazione, alla quota di servizio e alle informazioni di fatturazione nel Console di gestione AWS

Se disponi delle autorizzazioni necessarie, puoi accedere alle informazioni sull' AWS account, sulle quote di servizio, sull'organizzazione e sui dati di fatturazione dalla console.

 Note

Fornisce Console di gestione AWS solo l'accesso all'account, all'organizzazione, alla quota di servizio e alle informazioni di fatturazione. Questi servizi dispongono di console separate. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Gestisci il tuo AWS account](#) nella Guida Gestione dell'account AWS di riferimento.
- [Che cos'è AWS Organizations?](#) nella Guida AWS Organizations per l'utente.
- [Che cos'è Service Quotas?](#) nella Guida per l'utente di Service Quotas.
- [Utilizzando la Gestione dei costi e fatturazione AWS home page della AWS](#) Billing User Guide.

 Tip

Puoi anche ottenere ulteriori informazioni su questi argomenti rivolgendoti ad Amazon Q. Per ulteriori informazioni, consulta [Chatta con Amazon Q Developer](#).

Argomenti

- [Accesso alle informazioni sull'account nel Console di gestione AWS](#)

- [Accesso alle informazioni sull'organizzazione nel Console di gestione AWS](#)
- [Accesso alle informazioni sulle quote di servizio in Console di gestione AWS](#)
- [Accesso alle informazioni di fatturazione in Console di gestione AWS](#)

Accesso alle informazioni sull'account nel Console di gestione AWS

Se disponi delle autorizzazioni necessarie, puoi accedere alle informazioni sul tuo AWS account dalla console.

Per accedere alle informazioni del tuo account

1. Accedi alla [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli il nome dell'account.
3. Scegli Account.
4. Visualizza le informazioni del tuo account.

Note

Se desideri chiudere il tuo AWS account, consulta [Chiudere un AWS account](#) nella Guida Gestione dell'account AWS di riferimento.

Accesso alle informazioni sull'organizzazione nel Console di gestione AWS

Se disponi delle autorizzazioni necessarie, puoi accedere alle informazioni sulle tue AWS organizzazioni dalla console.

Per accedere alle informazioni sull'organizzazione

1. Accedi alla [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli il nome dell'account.
3. Scegli Organizations.
4. Visualizza le informazioni sulla tua organizzazione.

Accesso alle informazioni sulle quote di servizio in Console di gestione AWS

Se disponi delle autorizzazioni necessarie, puoi accedere alle informazioni sulle quote di servizio dalla console.

Per accedere alle informazioni sulle quote di servizio

1. Accedi alla [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli il nome dell'account.
3. Scegliere Quote del servizio.
4. Visualizza e gestisci le informazioni sulle quote di servizio.

Accesso alle informazioni di fatturazione in Console di gestione AWS

Se disponi delle autorizzazioni necessarie, puoi accedere alle informazioni sugli AWS addebiti dalla console.

Per accedere ai dati di fatturazione

1. Accedi alla [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli il nome dell'account.
3. Scegli Billing and Cost Management.
4. Utilizza la Gestione dei costi e fatturazione AWS dashboard per trovare un riepilogo e una suddivisione delle tue spese mensili.

Accesso a più account

È possibile accedere contemporaneamente a un massimo di cinque identità diverse in un unico browser Web in Console di gestione AWS. Può trattarsi di qualsiasi combinazione di ruoli root, IAM o federati in account diversi o nello stesso account. Ogni identità a cui accedi apre la propria istanza Console di gestione AWS in una nuova scheda.

Quando abiliti il supporto multiseSSIONE, l'URL della console contiene un sottodominio (ad esempio, <https://000000000000-aaaaaaa.us-east-1.console.aws.amazon.com/console/home?region=us-east-1>). Assicurati di aggiornare i segnalibri e i link della console.

Note

Devi attivare il supporto multiseSSIONE selezionando [Attiva la multiseSSIONE nel menu dell'account in Console di gestione AWS](#), oppure selezionando [Abilita multiseSSIONE su <https://console.aws.amazon.com>](#). Puoi disattivare le sessioni multiseSSIONI in qualsiasi momento selezionando [Disattiva la multiseSSIONE su <https://console.aws.amazon.com/o>](#) cancellando i cookie del browser. L'opt-in è specifico del browser.

Per accedere a più identità

1. Accedi alla [Console di gestione AWS](#).
2. Sulla barra di navigazione, scegli il nome dell'account.
3. Scegli [Aggiungi sessione](#) e scegli [Accedi](#). Si aprirà una nuova scheda per l'accesso.

Note

Per ulteriori informazioni sull'accesso come utente root o IAM, consulta [Accedere alla \[nella\]\(#\) Guida per AWS l'utente di accesso](#). Console di gestione AWS

4. Inserisci le credenziali .
5. Selezionare [Sign in \(Accedi\)](#). Viene Console di gestione AWS caricata in questa scheda come AWS identità scelta.
6. (Facoltativo) Per federare in ruoli aggiuntivi
 - a. Nel portale di AWS IAM Identity Center accesso o nel portale Single Sign-On (SSO), accedi al ruolo aggiuntivo.
 - b. Nel campo Console di gestione AWS scegli il nome del tuo account.
 - c. Visualizza le sessioni aggiuntive che puoi scegliere.

AWS Azioni consigliate in Console di gestione AWS

AWS Le azioni consigliate ti aiutano a lavorare in modo più efficiente Console di gestione AWS fornendo suggerimenti contestuali per il completamento delle attività e l'implementazione delle migliori pratiche. Quando sono disponibili consigli pertinenti, viene visualizzato un pulsante dinamico che puoi utilizzare per agire rapidamente sulla base di questi suggerimenti.

Note

AWS Recommended Actions analizza lo stato delle risorse per fornire suggerimenti ma non elabora i dati degli utenti.

Argomenti

- [Caratteristiche delle azioni AWS consigliate](#)
- [Utilizzo delle azioni consigliate](#)
- [Registrazione delle chiamate API AWS Recommended Actions utilizzando AWS CloudTrail](#)

Caratteristiche delle azioni AWS consigliate

- Consigli sulle azioni da intraprendere: ottieni suggerimenti pertinenti in base allo stato delle risorse, alle best practice e ai modelli di utilizzo comuni
- Azioni con un clic: completa le azioni consigliate direttamente dai messaggi di successo o dalle visualizzazioni delle risorse
- Pannello laterale destro integrato: accedi a un pannello laterale integrato per implementare i suggerimenti senza interrompere il flusso di lavoro
- Supporto multiservizio: ottieni consigli su più servizi AWS

Utilizzo delle azioni consigliate

Per utilizzare le azioni consigliate

1. Accedi a [Console di gestione AWS](#)
2. Cerca il pulsante # Azioni consigliate.

Note

Il pulsante delle azioni consigliate può apparire ovunque nel sito Console di gestione AWS ed è accessibile solo quando le azioni consigliate sono disponibili.

3. Scegli il pulsante per visualizzare le azioni disponibili.
4. Esegui i consigli direttamente o tramite il pannello laterale.

Registrazione delle chiamate API AWS Recommended Actions utilizzando AWS CloudTrail

AWS Recommended Actions è integrato con [AWS CloudTrail](#), un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o un Servizio AWS. CloudTrail acquisisce tutte le chiamate API per le azioni AWS consigliate come eventi. Le chiamate acquisite includono chiamate provenienti da Console di gestione AWS e chiamate di codice alle operazioni dell'API AWS Recommended Actions. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a AWS Recommended Actions, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e ulteriori dettagli.

CloudTrail è attivo nel tuo account Account AWS quando crei l'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione registrati in un. Regione AWS Per ulteriori informazioni, consulta [Lavorare con la cronologia degli CloudTrail eventi](#) nella Guida per l'utente.AWS CloudTrail Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi [CloudTrailLake](#).

AWS Eventi di gestione delle azioni consigliate in CloudTrail

[Gli eventi](#) di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse dell'ambiente Account AWS. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

AWS Recommended Actions registra tutte le operazioni del piano di controllo AWS Recommended Actions come eventi di gestione.

AWS Esempi di eventi Recommended Actions

Un evento rappresenta una singola richiesta proveniente 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.

L'esempio seguente mostra un CloudTrail evento che dimostra l'operazione.

```
{
```

```
"awsRegion": "us-east-2",
"eventCategory": "Management",
"eventID": "3510a29e-8070-4cbc-b6a0-9e11f18e26ec",
"eventName": "ListRecommendedActions",
"eventSource": "action-recommendations.amazonaws.com",
"eventTime": "2025-09-03T03:52:02Z",
"eventType": "AwsApiCall",
"eventVersion": "1.09",
"managementEvent": true,
"readOnly": true,
"recipientAccountId": "123456789098",
"requestID": "ec431c91-0315-413d-bdb6-d282fd4f6d83",
"requestParameters": {
  "context": "*",
  "uxChannel": "EXAMPLE"
},
"responseElements": null,
"sourceIPAddress": "192.0.2.0",
"userAgent": "EXAMPLE",
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AROARZDBH75ZCUYWFSTUS:EXAMPLE",
  "arn": "arn:aws:sts::123456789098:assumed-role/EXAMPLE",
  "accountId": "12345678909",
  "accessKeyId": "ASIAZDBEXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROARZDBHEXAMPLE",
      "arn": "arn:aws:iam::12345678909:role/EXAMPLE",
      "accountId": "12345678909",
      "userName": "EXAMPLE"
    },
    "attributes": {
      "creationDate": "2025-09-03T03:52:00Z",
      "mfaAuthenticated": "false"
    }
  },
  "invokedBy": "action-recommendations.amazonaws.com"
}
```

Per informazioni sul contenuto dei CloudTrail record, consultate il [contenuto dei CloudTrail record](#) nella Guida per l'AWS CloudTrail utente.

Utilizzo AWS Console Home in Console di gestione AWS

Questo argomento descrive come utilizzare AWS Console Home, incluso come personalizzare la home page della console. Console Home è la home page di Console di gestione AWS. Quando accedi per la prima volta alla console, arrivi alla home page della console. Puoi personalizzare la home page della console utilizzando widget e applicazioni. I widget consentono di aggiungere componenti personalizzati che tengono traccia delle informazioni sui AWS servizi e sulle risorse. Le applicazioni consentono di raggruppare AWS risorse e metadati. È possibile gestire le applicazioni utilizzando MyApplications. Puoi anche utilizzare Console Home per visualizzare un elenco di tutti i AWS servizi e chattare con Amazon Q.

Argomenti

- [Visualizzazione di tutti i AWS servizi in AWS Console Home](#)
- [Lavorare con i widget in AWS Console Home](#)
- [In cosa consiste myApplications? AWS Console Home](#)
- [Chattare con Amazon Q Developer in AWS Console Home](#)

Visualizzazione di tutti i AWS servizi in AWS Console Home

È possibile visualizzare un elenco di tutti i AWS servizi e accedere alle relative console da Console Home.

Per accedere a un elenco completo dei AWS servizi

1. Accedi alla [Console di gestione AWS](#).
2. Espandi il menu Home della console scegliendo l'icona a forma di hamburger (☰).
3. Scegli Tutti i servizi.
4. Seleziona un AWS servizio per accedere alla relativa console.

Lavorare con i widget in AWS Console Home

La dashboard di Console Home include widget che visualizzano informazioni importanti sull'AWS ambiente e forniscono collegamenti rapidi ai servizi. Puoi personalizzare la tua esperienza aggiungendo e rimuovendo widget, riorganizzandoli o modificandone le dimensioni.

Gestione dei widget

Puoi gestire i widget aggiungendoli, rimuovendoli, riorganizzandoli e ridimensionandoli. I widget predefiniti possono essere rimossi e aggiunti nuovamente. Puoi anche ripristinare il layout predefinito della console Home e richiedere nuovi widget.

Per aggiungere un widget

1. Scegli il pulsante +Aggiungi widget sul lato destro superiore o inferiore della dashboard Home della console.
2. Scegli l'indicatore di trascinamento, rappresentato da sei punti verticali (:) nella parte superiore sinistra della barra del titolo del widget, quindi trascinalo nella dashboard di Console Home.

Per rimuovere un widget

1. Scegli i puntini di sospensione, rappresentati da tre punti verticali (:) nella parte superiore destra della barra del titolo del widget.
2. Scegli Remove widget (Rimuovi widget).

Per riorganizzare i widget

- Scegli l'indicatore di trascinamento, rappresentato da sei punti verticali (:) nella parte superiore sinistra della barra del titolo del widget, quindi trascina il widget in una nuova posizione nella dashboard Home della console.

Per ridimensionare un widget

- Seleziona l'icona di ridimensionamento in basso a destra del widget e trascina per ridimensionare il widget.

Se desideri ricominciare con l'organizzazione e la configurazione dei widget, puoi reimpostare la dashboard Home della console al layout predefinito. Questa operazione annullerà le modifiche apportate al layout della dashboard Home della console e ripristinerà tutti i widget nella posizione e nelle dimensioni predefinite.

Per reimpostare la pagina sul layout predefinito

1. Scegli Ripristina il layout predefinito sul lato superiore destro della pagina.
2. Per confermare, scegli Ripristina.

Note

Questa operazione annullerà tutte le modifiche apportate al layout della dashboard Home della console.

Richiesta di un nuovo widget nella dashboard Home della console

1. In basso a sinistra nella dashboard Home della console, scegli Vuoi vedere un altro widget? Diccelo!

Descrivi il widget che desideri vedere aggiunto nella dashboard Home della console.

2. Seleziona Invia.

Note

Esaminiamo periodicamente i suggerimenti e potremmo aggiungere nuovi widget nei futuri aggiornamenti alla Console di gestione AWS.

In cosa consiste myApplications? AWS Console Home

myApplications è un'estensione della Home della console che consente di gestire e monitorare i costi, lo stato, il livello di sicurezza e le prestazioni delle applicazioni su AWS. Le applicazioni consentono di raggruppare risorse e metadati. Puoi accedere a tutte le applicazioni del tuo account, alle metriche chiave di tutte le applicazioni e a una panoramica delle metriche e degli approfondimenti relativi a costi, sicurezza e operazioni da più console di servizio da un'unica visualizzazione in Console di gestione AWS. myApplications include quanto segue:

- Widget delle applicazioni nella pagina Home della console
- myApplications per visualizzare i costi delle risorse delle applicazioni e gli esiti relativi alla sicurezza

- Dashboard myApplications, che fornisce una vista delle principali metriche delle applicazioni, come costi, prestazioni ed esiti relativi alla sicurezza

Argomenti

- [Funzionalità di myApplications](#)
- [Servizi correlati](#)
- [Accesso a myApplications](#)
- [Prezzi](#)
- [Regioni supportate per MyApplications](#)
- [Applicazioni in MyApplications](#)
- [Risorse in MyApplications](#)
- [Dashboard MyApplications in AWS Console Home](#)

Funzionalità di myApplications

- Crea applicazioni: crea nuove applicazioni e organizzane le risorse. Le tue applicazioni vengono visualizzate automaticamente in MyApplications, quindi puoi intervenire nella Console di gestione AWS, APIs, CLI e SDKs L'Infrastructure as code (IaC) viene generata al momento della creazione dell'applicazione ed è accessibile dalla dashboard myApplication. IaC è utilizzabile negli strumenti IaC, inclusi Terraform. AWS CloudFormation
- Accedi alle tue applicazioni: puoi accedere rapidamente a qualsiasi applicazione selezionandola dal widget myApplications.
- Accedi alle tue risorse: puoi visualizzare rapidamente le risorse dell'applicazione dal menu Servizi selezionando l'applicazione. Quando si seleziona una risorsa, si accede direttamente alla console di servizio pertinente. La tua posizione nella tabella delle risorse viene salvata, quindi puoi continuare a navigare in qualsiasi momento dal menu Servizi.
- Confronta le metriche delle applicazioni: utilizza myApplications per confrontare le metriche fondamentali delle applicazioni, come il costo delle risorse applicative e il numero di risultati di sicurezza critici per più applicazioni.
- Monitoraggio e gestione delle applicazioni: valuta lo stato e le prestazioni delle applicazioni utilizzando allarmi, canarini e obiettivi relativi ai livelli di servizio Amazon CloudWatch, ricavati dai risultati e dall' AWS Security Hub CSPM andamento dei costi. AWS Cost Explorer Service

Puoi anche trovare riepiloghi e ottimizzazioni delle metriche di calcolo e gestire la conformità delle risorse e lo stato della configurazione da AWS Systems Manager

Servizi correlati

myApplications utilizza i seguenti servizi:

- AppRegistry
- AppManager
- Amazon CloudWatch
- Amazon EC2
- AWS Lambda
- Esploratore di risorse AWS
- AWS Security Hub CSPM
- Systems Manager
- AWS Service Catalog
- Assegnazione di tag

Accesso a myApplications

È possibile accedere a myApplications dalla [Console di gestione AWS](#) selezionando myApplications nella barra laterale sinistra.

Prezzi

MyApplications on AWS è offerto senza costi aggiuntivi. Non sono previsti costi di configurazione né impegni iniziali. Per l'utilizzo delle risorse e dei servizi sottostanti riepilogati nella dashboard myApplication si continuano ad applicare le tariffe pubblicate per tali risorse.

Regioni supportate per MyApplications

myApplications è disponibile nelle seguenti versioni: Regioni AWS

- Stati Uniti orientali (Ohio)
- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti occidentali (California settentrionale)

- Stati Uniti occidentali (Oregon)
- Asia Pacifico (Mumbai)
- Asia Pacifico (Osaka)
- Asia Pacifico (Seoul)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Tokyo)
- Canada (Centrale)
- Europa (Francoforte)
- Europa (Irlanda)
- Europa (Londra)
- Europe (Paris)
- Europa (Stoccolma)
- Sud America (San Paolo)

Regioni con consenso esplicito

Il consenso per l'utilizzo delle regioni non è attivato per impostazione predefinita. È necessario abilitare manualmente queste regioni per utilizzarle con myApplications. Per ulteriori informazioni su Regioni AWS, vedere [Gestione Regioni AWS](#). Sono supportate le seguenti regioni con consenso esplicito:

- Africa (Città del Capo)
- Asia Pacifico (Hong Kong)
- Asia Pacifico (Hyderabad)
- Asia Pacifico (Giacarta)
- Asia Pacifico (Melbourne)
- Europa (Milano)
- Europa (Spagna)
- Europa (Zurigo)
- Medio Oriente (Bahrein)
- Medio Oriente (Emirati Arabi Uniti)

- Israele (Tel Aviv)

Applicazioni in MyApplications

Le applicazioni consentono di raggruppare risorse e metadati. È possibile gestire le applicazioni creando, effettuando l'onboarding, visualizzandole, modificandole o eliminandole. Puoi anche creare frammenti di codice per aggiungere automaticamente nuove risorse a un'applicazione.

Note

Puoi anche aggiungere applicazioni ai Preferiti in modo da facilitarne l'accesso. Per ulteriori informazioni, consulta [???](#).

Argomenti

- [Creazione di applicazioni in MyApplications](#)
- [Incorpora le applicazioni esistenti in MyApplications AppRegistry](#)
- [Visualizzazione delle applicazioni in MyApplications](#)
- [Modifica delle applicazioni in MyApplications](#)
- [Eliminazione di applicazioni in MyApplications](#)
- [Creazione di frammenti di codice in MyApplications](#)


Creazione di applicazioni in MyApplications

Puoi creare una nuova applicazione o [the section called “Applicazioni di onboarding”](#) crearla prima dell'8 novembre 2023 per iniziare a usare MyApplications. Quando crei una nuova applicazione, puoi aggiungere risorse cercandole e selezionandole o utilizzando tag esistenti.

Come creare una nuova applicazione

1. Accedi alla [Console di gestione AWS](#).
2. Espandi la barra laterale sinistra e scegli MyApplications.
3. Scegli Crea applicazione.
4. Inserisci il nome dell'applicazione.
5. (Facoltativo) Aggiungi una descrizione dell'applicazione.


- (Facoltativo) Aggiungi [tag](#). I tag sono coppie chiave-valore applicate alle risorse per contenere metadati relativi a tali risorse.

 Note

Il tag AWS dell'applicazione viene applicato automaticamente alle applicazioni appena create. Per ulteriori informazioni, consultate [Il tag AWS dell'applicazione](#) nella Guida per l'AWS Service Catalog AppRegistry amministratore.

- (Facoltativo) Aggiungi [gruppi di attributi](#). È possibile utilizzare i gruppi di attributi per archiviare i metadati delle applicazioni.
- Scegli Next (Successivo).
- (Facoltativo) Aggiungi risorse:


Search and select resources

 Note

Per cercare e aggiungere risorse, devi attivare Esploratore di risorse AWS. Per ulteriori informazioni, consulta [Guida introduttiva Esploratore di risorse AWS](#). Tutte le risorse aggiunte sono contrassegnate con il tag AWS dell'applicazione.

Per aggiungere risorse utilizzando la ricerca

- Scegli Cerca e seleziona le risorse.
- Scegli Seleziona risorse.
- (Facoltativo) Scegli una [visualizzazione](#).
- Cerca le tue risorse. Puoi cercare per parola chiave, nome o tipo oppure scegliere un tipo di risorsa.

 Note

Se non riesci a trovare la risorsa che stai cercando, risolvi i problemi con. Esploratore di risorse AWS Per ulteriori informazioni, consulta [Risoluzione dei problemi di ricerca di Resource Explorer](#) nella Guida per l'utente di Resource Explorer.

5. Seleziona la casella di controllo accanto alle risorse che desideri aggiungere.
6. Scegli Aggiungi.
7. Scegli Next (Successivo).
8. Rivedi le scelte effettuate.

Automatically add resources using tags

Quando crei un'applicazione, puoi aggiungere risorse in blocco specificando una coppia chiave-valore di tag esistente. Con questo metodo, applica AWS automaticamente il `awsApplication` tag a tutte le risorse etichettate con la coppia chiave-valore specificata e crea una sincronizzazione dei tag per le risorse dell'applicazione per impostazione predefinita. Con la sincronizzazione dei tag abilitata, tutte le risorse etichettate con la coppia chiave-valore del tag specificata vengono aggiunte automaticamente all'applicazione. Per informazioni sulla risoluzione degli errori di sincronizzazione dei tag, consulta [the section called "Risoluzione degli errori di sincronizzazione dei tag in MyApplications"](#)

Note


L'aggiunta di risorse a un'applicazione utilizzando i tag richiede le autorizzazioni per creare un' AppRegistry applicazione, raggruppare e separare le risorse e etichettare e rimuovere i tag dalle risorse. È possibile aggiungere la politica [ResourceGroupsTaggingAPITagUntagSupportedResources](#) AWS gestita da Resource Groups oppure creare e gestire una politica personalizzata. Le seguenti autorizzazioni devono essere aggiunte alla dichiarazione politica di un utente in IAM:

- `servicecatalog:CreateApplication`
- `resource-groups:GroupResources`
- `resource-groups:UngroupResources`
- `tag:TagResources`
- `tag:UntagResources`

Per aggiungere risorse utilizzando tag esistenti


1. Scegli Aggiungi automaticamente risorse utilizzando i tag.

2. Seleziona una chiave e un valore di tag esistenti:
 - a. Seleziona il ruolo usato per etichettare le risorse. Per ulteriori informazioni, consulta le [autorizzazioni richieste per la sincronizzazione dei tag](#) nella AWS Service Catalog Administrator Guide. AppRegistry
 - b. Seleziona una chiave Tag.
 - c. Seleziona un valore per il tag.
 - d. (Facoltativo) Scegliete Anteprima risorse per vedere in anteprima quali risorse sono etichettate con la coppia chiave-valore del tag.
 - e. Leggi e accetta l'informativa Riconosco che Group Lifecycle Events sarà abilitata alla creazione di un avviso di sincronizzazione dei tag. GLE consente di notare le modifiche AWS alle risorse etichettate con la coppia chiave-valore.
3. Scegli Next (Successivo).
4. Controlla i dettagli dell'applicazione, la coppia chiave-valore del tag selezionata e l'anteprima delle risorse che verranno aggiunte all'applicazione.

 Note

Per impostazione predefinita, la creazione di un'applicazione utilizzando una coppia chiave-valore di tag esistente crea una sincronizzazione tra tag. Dopo la configurazione, tag-sync gestisce inoltre in modo continuo le risorse dell'applicazione, aggiungendo o rimuovendo risorse man mano che vengono etichettate o prive di tag con la coppia chiave-valore specificata. È possibile gestire la sincronizzazione dei tag dalla pagina Gestisci risorse dell'applicazione.

10. Se associ uno CloudFormation stack, seleziona la casella di controllo nella parte inferiore della pagina.

 Note

L'aggiunta di uno CloudFormation stack all'applicazione richiede un aggiornamento dello stack perché tutte le risorse aggiunte all'applicazione sono contrassegnate con il tag dell'applicazione. AWS Le configurazioni manuali eseguite dopo l'ultimo aggiornamento dello stack potrebbero non riflettersi dopo questo aggiornamento. Ciò può causare all'applicazione tempi di inattività o altri problemi. Per ulteriori informazioni, consulta

[Aggiornamento dei comportamenti delle risorse stack](#) nella Guida per l'utente di CloudFormation .

11. Scegli Crea applicazione.

Incorpora le applicazioni esistenti in MyApplications AppRegistry

Puoi effettuare l'onboarding di un' AppRegistry applicazione esistente creata prima dell'8 novembre 2023 per iniziare a usare MyApplications.

Per effettuare l'onboarding di un'applicazione esistente AppRegistry

1. Accedi alla [Console di gestione AWS](#).
2. Nella barra laterale sinistra, scegli myApplications.
3. Usa la barra di ricerca per trovare la tua applicazione.
4. Seleziona l'applicazione.
5. Scegli **application name** Onboard.
6. Se associ uno CloudFormation stack, seleziona la casella di controllo nella casella di avviso.
7. Scegli Onboard dell'applicazione.

Visualizzazione delle applicazioni in MyApplications

Puoi visualizzare le tue applicazioni da MyApplications o dal menu Servizi. Se visualizzi le tue applicazioni da MyApplications, puoi visualizzarle tutte Regioni AWS o in modo specifico Regioni AWS e le relative informazioni pertinenti in una visualizzazione a scheda o tabella.

Note

Puoi anche visualizzare le applicazioni aggiunte ai tuoi Preferiti dal menu Preferiti. Per ulteriori informazioni, consulta [Preferiti in Console di gestione AWS](#).

myApplications

Per visualizzare le applicazioni in MyApplications

1. Apri la [Console di gestione AWS](#).

2. Nella barra laterale sinistra, scegli myApplications.
3. In Regioni, seleziona Regione attuale o Regioni supportate.
4. Per trovare un'applicazione specifica, inserisci il nome, le parole chiave o la descrizione nella barra di ricerca.
5. (Facoltativo) La visualizzazione predefinita è la visualizzazione a schede. Per personalizzare la pagina della tua applicazione:
 - a. Scegli l'icona a forma di ingranaggio.
 - b. (Facoltativo) Seleziona le dimensioni della pagina.
 - c. (Facoltativo) Scegli la visualizzazione a schede o a tabelle.
 - d. (Facoltativo) Seleziona le dimensioni della pagina.
 - e. (Facoltativo) Se utilizzi la visualizzazione a tabelle, seleziona le proprietà per la visualizzazione a tabelle.
 - f. (Facoltativo) Attiva le proprietà dell'applicazione visibili e seleziona l'ordine di visualizzazione.
 - g. Scegli Conferma.

Services menu

Per visualizzare le applicazioni dal menu Servizi

1. Apri la [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli Servizi (:).
3. Scegli Tutte le applicazioni.
4. Seleziona un'applicazione.
5. (Facoltativo) Selezionate una [vista](#).
6. (Facoltativo) Seleziona un filtro. Puoi filtrare le tue risorse per Proprietà o per Tag. Per ulteriori informazioni, consulta il [riferimento alla sintassi delle query di ricerca per Resource Explorer](#) nella Guida per l'Esploratore di risorse AWS utente.
7. (Facoltativo) Seleziona una risorsa per visualizzarla nella console di servizio pertinente.

 Tip


Puoi continuare a sfogliare le risorse da dove avevi interrotto scegliendo Servizi (:). Inoltre, i filtri di ricerca applicati persisteranno.

Modifica delle applicazioni in MyApplications

La modifica dell'applicazione si apre AppRegistry in modo da poterne aggiornare la descrizione. Puoi anche usarla AppRegistry per modificare i tag e i gruppi di attributi dell'applicazione.

Per modificare un'applicazione

1. Apri la [Console di gestione AWS](#).
2. Nella barra laterale sinistra della console, scegli myApplications.
3. Seleziona l'applicazione da modificare.
4. Nella dashboard MyApplication, scegli Azioni, quindi scegli Modifica applicazione.
5. In Modifica applicazione, apporta le modifiche desiderate alla descrizione, ai tag e ai gruppi di attributi dell'applicazione.


 Note

Per ulteriori informazioni sulla gestione dei tag e dei gruppi di attributi, vedere [Gestione dei tag](#) e [Modifica dei gruppi di attributi](#) nella Guida per l'AWS Service Catalog AppRegistry amministratore.

6. Scegliere Aggiorna.

Eliminazione di applicazioni in MyApplications

È possibile eliminare le applicazioni che non sono più necessarie. Prima di eliminare un'applicazione, assicuratevi di rimuovere tutte le condivisioni di risorse e i gruppi di attributi associati che non sono stati creati da un AWS servizio.

 Note

L'eliminazione di un'applicazione non ha alcun impatto sulle risorse. Le risorse contrassegnate con il tag AWS dell'applicazione rimarranno contrassegnate.

Per eliminare un'applicazione

1. Apri la [Console di gestione AWS](#).
2. Nella barra laterale sinistra della console, scegli myApplications.
3. Seleziona l'applicazione da eliminare.
4. Nella dashboard myApplications, scegli Azioni.
5. Scegli Elimina applicazione.
6. Conferma l'eliminazione, quindi scegli Elimina.

Creazione di frammenti di codice in MyApplications

myApplications crea frammenti di codice per tutte le applicazioni. È possibile utilizzare frammenti di codice per aggiungere automaticamente risorse appena create a un'applicazione utilizzando gli strumenti Infrastructure as Code (IaC). Tutte le risorse aggiunte sono contrassegnate con il tag AWS dell'applicazione per associarle all'applicazione.

Per creare un frammento di codice per l'applicazione

1. Apri la [Console di gestione AWS](#).
2. Nella barra laterale sinistra della console, scegli myApplications.
3. Cerca e seleziona un'applicazione.
4. Scegli Azioni.
5. Scegli Ottieni frammento di codice.
6. Seleziona un tipo di frammento di codice.
7. Scegli Copia per copiare il codice negli appunti.
8. Copia il codice nello strumento IaC.

Risorse in MyApplications

In AWS, una risorsa è un'entità con cui puoi lavorare. Gli esempi includono un'istanza Amazon EC2, uno AWS CloudFormation stack o un bucket Amazon S3. Puoi gestire le tue risorse in MyApplications aggiungendole e rimuovendole dalle applicazioni.

Argomenti

- [Aggiungere risorse in MyApplications](#)
- [Rimozione di risorse in MyApplications](#)
- [Visualizzazione delle risorse in MyApplications](#)

Aggiungere risorse in MyApplications

Aggiungendo risorse alle applicazioni sei in grado di raggrupparle e di gestirne la sicurezza, le prestazioni e la conformità. È possibile aggiungere risorse alle applicazioni esistenti cercandole e selezionandole oppure utilizzando tag esistenti ed eseguendo una sincronizzazione dei tag.

Search and select resources

Per cercare e selezionare risorse

1. Apri la [Console di gestione AWS](#).
2. Nella barra laterale sinistra della console, scegli myApplications.
3. Cerca e seleziona un'applicazione.
4. Scegli Gestisci risorse.
5. Scegli Aggiungi risorse.
6. (Facoltativo) Scegli una [visualizzazione](#).
7. Cerca le tue risorse. Puoi cercare per parola chiave, nome o tipo oppure scegliere un tipo di risorsa.

Note

Se non riesci a trovare la risorsa che stai cercando, risolvi i problemi con. Esploratore di risorse AWS Per ulteriori informazioni, consulta [Risoluzione dei problemi di ricerca di Resource Explorer](#) nella Guida per l'utente di Resource Explorer.

8. Seleziona la casella di controllo accanto alle risorse che desideri aggiungere.
9. Scegli Aggiungi.

Automatically add resources using tags

Quando crei un'applicazione, puoi aggiungere risorse in blocco specificando una coppia chiave-valore di tag esistente. Con questo metodo, applica AWS automaticamente il `awsApplication` tag a tutte le risorse e crea una sincronizzazione dei tag per le risorse dell'applicazione per impostazione predefinita. Con tag-sync abilitato, tutte le risorse etichettate con la coppia chiave-valore del tag specificata vengono aggiunte automaticamente all'applicazione.

Per aggiungere risorse utilizzando tag esistenti

1. Apri la [Console di gestione AWS](#).
2. Nella barra laterale sinistra della console, scegli myApplications.
3. Scegli Gestisci risorse.
4. Scegli Crea sincronizzazione dei tag.
5. Seleziona una chiave e un valore di tag esistenti:
 - a. Seleziona il ruolo usato per etichettare le risorse. Per ulteriori informazioni, vedere [Autorizzazioni richieste per l'attività di sincronizzazione dei tag](#) nella AWS Service Catalog Administrator Guide. AppRegistry
 - b. Seleziona una chiave Tag.
 - c. Seleziona un valore per il tag.
 - d. Leggi e accetta l'informativa Riconosco che Group Lifecycle Events sarà abilitata alla creazione di un avviso di sincronizzazione dei tag. GLE consente di notare le modifiche AWS alle risorse etichettate con la coppia chiave-valore.
6. Scegli Crea sincronizzazione dei tag.

Risoluzione degli errori di sincronizzazione dei tag in MyApplications

Questa sezione descrive gli errori più comuni di sincronizzazione dei tag e come risolverli. Dopo aver tentato di risolvere l'errore, puoi riprovare l'operazione di sincronizzazione dei tag non riuscita.

- **Autorizzazioni insufficienti:** non disponi delle autorizzazioni minime richieste per avviare, aggiornare o annullare la sincronizzazione dei tag. Per ulteriori informazioni, consulta le autorizzazioni richieste

[per la sincronizzazione dei tag](#). Dopo esserti assicurato che il ruolo specificato per eseguire la sincronizzazione dei tag disponga delle autorizzazioni minime richieste, riprova l'operazione di sincronizzazione dei tag non riuscita.

- Esiste già: per questa applicazione esiste già un'attività con questa coppia chiave-valore del tag. Un'applicazione può supportare più di una sincronizzazione dei tag, ma ogni sincronizzazione dei tag deve avere una coppia chiave-valore di tag diversa. Dopo aver specificato una diversa coppia chiave-valore del tag, ritenta l'operazione di sincronizzazione tag non riuscita.
- Limite massimo raggiunto: hai raggiunto il limite massimo di 100 attività di sincronizzazione dei tag per account, in tutte le applicazioni.

Rimozione di risorse in MyApplications

È possibile rimuovere le risorse per dissociarle dall'applicazione.

Per rimuovere risorse

1. Apri la [Console di gestione AWS](#).
2. Nella barra laterale sinistra della console, scegli myApplications.
3. Cerca e seleziona un'applicazione.
4. Scegli Gestisci risorse.
5. (Facoltativo) Scegli una [visualizzazione](#).
6. Cerca le tue risorse. Puoi cercare per parola chiave, nome o tipo oppure scegliere un tipo di risorsa.

Note

Se non riesci a trovare la risorsa che stai cercando, risolvi i problemi con. Esploratore di risorse AWS Per ulteriori informazioni, consulta [Risoluzione dei problemi di ricerca di Resource Explorer](#) nella Guida per l'utente di Resource Explorer.

7. Scegli Rimuovi.
8. Conferma di voler rimuovere la risorsa selezionando Rimuovi risorse.

Visualizzazione delle risorse in MyApplications

È possibile visualizzare le risorse dell'applicazione da MyApplications e dal menu Servizi.

myApplications

Per visualizzare le risorse in MyApplications

1. Apri la [Console di gestione AWS](#).
2. Espandi la barra laterale sinistra e scegli MyApplications.
3. Seleziona un'applicazione.
4. Nel widget Risorse, visualizza le tue risorse.

Services menu

Per visualizzare le applicazioni dal menu Servizi

1. Apri la [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli Servizi (:).
3. Scegli Tutte le applicazioni.
4. Seleziona un'applicazione.
5. (Facoltativo) Selezionate una [vista](#).
6. (Facoltativo) Seleziona un filtro. Puoi filtrare le tue risorse per Proprietà o per Tag. Per ulteriori informazioni, consulta il [riferimento alla sintassi delle query di ricerca per Resource Explorer](#) nella Guida per l'Esploratore di risorse AWS utente.
7. (Facoltativo) Seleziona una risorsa per visualizzarla nella console di servizio pertinente.

Tip

Puoi continuare a sfogliare le risorse da dove avevi interrotto scegliendo Servizi (:). Inoltre, i filtri di ricerca applicati persisteranno.

Dashboard MyApplications in AWS Console Home

Ogni applicazione creata o integrata ha la propria dashboard myApplications. La dashboard MyApplications contiene widget relativi a costi, sicurezza e operatività che consentono di ottenere informazioni dettagliate da più servizi. AWS È anche possibile aggiungere un widget ai preferiti, riordinarlo, rimuoverlo o ridimensionarlo. Per ulteriori informazioni, consulta [Lavorare con i widget in AWS Console Home](#).

Argomenti

- [Widget Configurazione della dashboard dell'applicazione](#)
- [Widget Riepilogo dell'applicazione](#)
- [Widget Calcolo](#)
- [Widget Costi e utilizzo](#)
- [AWS Widget di sicurezza](#)
- [AWS Widget di resilienza](#)
- [Widget Risorse](#)
- [DevOps widget](#)
- [Widget Monitoraggio e operazioni](#)
- [Widget Tag](#)

Widget Configurazione della dashboard dell'applicazione

Questo widget contiene un elenco di attività introduttive suggerite che puoi utilizzare per aiutarti a configurare la gestione delle Servizi AWS risorse dell'applicazione.

Widget Riepilogo dell'applicazione

Questo widget mostra il nome, la descrizione e il [tag applicazione AWS](#) della tua applicazione. È possibile accedere e copiare il tag dell'applicazione in Infrastructure as Code (IAC) per aggiungere manualmente tag alle risorse.

Widget Calcolo

Questo widget mostra informazioni e metriche relative alle risorse di calcolo che aggiungi all'applicazione. Ad esempio, il totale degli allarmi e il totale dei tipi di risorse di calcolo. Il widget mostra anche i grafici di tendenza dei parametri relativi alle prestazioni delle risorse Amazon CloudWatch per l'utilizzo della CPU delle istanze Amazon EC2 e le chiamate Lambda.

Configurazione del widget Calcolo

Per popolare i dati nel widget Calcolo, configura almeno un'istanza Amazon EC2 o una funzione Lambda per la tua applicazione. Per ulteriori informazioni, consulta la [Documentazione di Amazon Elastic Compute Cloud](#) e [Nozioni di base su Lambda](#) nella Guida per gli sviluppatori di AWS Lambda

Widget Costi e utilizzo

Questo widget mostra i dati AWS sui costi e sull'utilizzo delle risorse dell'applicazione. È possibile utilizzare questi dati per confrontare i costi mensili e visualizzare le ripartizioni dei costi per Servizio AWS. Questo widget riepiloga solo i costi delle risorse contrassegnate con il tag AWS dell'applicazione, escluse tasse, commissioni e altri costi condivisi non direttamente associati a una risorsa. I costi mostrati non sono combinati e aggiornati almeno una volta ogni 24 ore. Per ulteriori informazioni, consulta [la sezione Analisi dei costi Esploratore di risorse AWS](#) nella Guida per l'AWS Cost Management utente.

Configurazione del widget Costi e utilizzo

Per configurare il widget Costo e utilizzo, abilitalo AWS Cost Explorer Service per l'applicazione e l'account. Questo servizio è offerto senza costi aggiuntivi e non prevede costi di configurazione o impegni iniziali. Per ulteriori informazioni, consulta [Utilizzo dell'Esploratore dei costi](#) nella Guida per l'utente di AWS Cost Management .

AWS Widget di sicurezza

Questo widget mostra i risultati di sicurezza di AWS Security for your application. AWS Security fornisce una visione completa dei risultati di sicurezza per l'applicazione in AWS. È possibile accedere ai risultati prioritari recenti in base alla gravità, monitorarne il livello di sicurezza, accedere ai risultati recenti critici o di gravità elevata e ottenere approfondimenti utili per i passaggi successivi. Per ulteriori informazioni, consulta [AWS Security Hub CSPM](#).

Configurazione del widget AWS Sicurezza

Per configurare il widget AWS di sicurezza, configuralo AWS Security Hub CSPM per l'applicazione e l'account. Per ulteriori informazioni, vedi [Cos'è AWS Security Hub CSPM?](#) nella Guida AWS Security Hub CSPM per l'utente. Per informazioni sui prezzi, consulta [Versione di prova gratuita e prezzi di AWS Security Hub CSPM](#) nella Guida per l'utente di AWS Security Hub CSPM .

AWS Security Hub CSPM richiede la configurazione di AWS Config Recording. Questo servizio fornisce una visualizzazione dettagliata delle risorse associate all' AWS account. Per ulteriori informazioni, consulta [AWS Systems Manager](#) nella Guida per l'utente di AWS Systems Manager .

AWS Widget di resilienza

Questo widget mostra i dettagli sulla resilienza di AWS Resilience Hub per le tue applicazioni. Dopo aver avviato una valutazione, AWS Resiliency Hub analizza lo stato di resilienza delle applicazioni

valutando le relative risorse rispetto a una politica di resilienza predefinita. Puoi accedere a metriche come il punteggio di resilienza, le violazioni delle politiche, le variazioni delle politiche, la deriva delle risorse e la cronologia dei tuoi punteggi di resilienza. Le tue applicazioni vengono valutate quotidianamente per un tracciamento avanzato, ma puoi disabilitarlo in qualsiasi momento. Per ulteriori informazioni, consulta [AWS Resilience Hub](#). Per informazioni sui prezzi, consulta [Prezzi di AWS Resilience Hub](#).

Configurazione del widget Resiliency AWS

Per configurare il widget AWS Resilienza, aggiungi un'applicazione. Per ulteriori informazioni, consulta [Cos'è AWS Resilience Hub?](#) nella Guida AWS Resilience Hub per l'utente.

Widget Risorse

Questo widget utilizza AWS Resource Explorer per mostrare le risorse che hai aggiunto all'applicazione all'interno di una vista. Puoi anche utilizzare questo widget per cercare o filtrare le tue risorse utilizzando metadati di risorse come nomi, tag e IDs. Per ulteriori informazioni, consulta [AWS Resource Explorer](#).

Configurazione del widget Risorse

Per configurare il widget delle risorse, effettua l'accesso con Resource Explorer. Per ulteriori informazioni, consulta [Guida introduttiva a Resource Explorer](#) nella Guida per l'utente di AWS Resource Explorer.

DevOps widget

Questo widget mostra informazioni relative alle operazioni che permettono di valutare la conformità dell'applicazione e di effettuare interventi correttivi. Questi approfondimenti includono:

- Gestione del parco istanze
- Gestione dello stato
- Gestione delle patch
- Configurazione e OpsItems gestione

Configurazione del widget DevOps

Per configurare il DevOps widget, abilita AWS Systems Manager OpsCenter per l'applicazione e l'account. Per ulteriori informazioni, vedere Guida [introduttiva a Systems Manager Explorer e](#)

[OpsCenter](#) nella Guida AWS Systems Manager per l'utente. L'abilitazione OpsCenter consente di configurare AWS Config e AWS Systems Manager Explorer far Amazon CloudWatch sì che i relativi eventi vengano creati automaticamente OpsItems in base a regole ed eventi di uso comune. Per ulteriori informazioni, consulta [Configurazione OpsCenter nella Guida per l'AWS Systems Manager utente](#).

È possibile configurare le istanze per l'esecuzione degli agenti Systems Manager e applicare le autorizzazioni per abilitare la scansione delle patch. Per ulteriori informazioni, consulta [AWS Systems Manager Quick Setup](#) nella Guida per l'utente di AWS Systems Manager .

Puoi anche configurare il patching automatico delle istanze Amazon EC2 per la tua applicazione AWS Systems Manager configurando Patch Manager. Per maggiori informazioni, consulta [Utilizzo delle policy di patch di Quick Setup](#) nella Guida per l'utente di AWS Systems Manager .

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

Widget Monitoraggio e operazioni

Questo widget mostra:

- Allarmi e avvisi per le risorse associate all'applicazione
- Obiettivi e parametri del livello di servizio dell'applicazione () SLOs
- Metriche dei segnali AWS applicativi disponibili

Configurazione del widget Monitoraggio e operazioni

Per configurare il widget Monitoraggio e operazioni, crea CloudWatch allarmi e canarini nel tuo account. AWS Per ulteriori informazioni, consulta [Using Amazon CloudWatch alarms](#) e [Creating a canary](#) nella Amazon CloudWatch User Guide. Per i prezzi di CloudWatch Alarm e Synthetic Canary, consulta [rispettivamente CloudWatch i prezzi di Amazon](#) e il [blog AWS Cloud Operations and Migrations](#).

Per ulteriori informazioni su CloudWatch Application Signals, consulta [Enable Amazon CloudWatch Application Signals](#) nella Amazon CloudWatch User Guide.

Widget Tag

Questo widget mostra tutti i tag associati all'applicazione. È possibile utilizzare questo widget per tracciare e gestire i metadati delle applicazioni (criticità, ambiente, centro di costo). Per ulteriori

informazioni, consulta [Cosa sono i tag?](#) nel AWS white paper sulle migliori pratiche per l'etichettatura AWS delle risorse.

Chattare con Amazon Q Developer in AWS Console Home

Amazon Q Developer è un assistente conversazionale generativo basato sull'intelligenza artificiale (AI) che può aiutarti a comprendere, creare, estendere e utilizzare le applicazioni. AWS Puoi porre ad Amazon Q qualsiasi domanda in merito AWS, incluse domande sull' AWS architettura, le AWS risorse, le best practice, la documentazione e altro ancora. Puoi anche creare casi di supporto e ricevere assistenza da un agente reale. Per ulteriori informazioni, consulta [Cos'è Amazon Q?](#) nella Amazon Q Developer User Guide.

Inizia a usare Amazon Q

Puoi iniziare a chattare con Amazon Q nei siti Web di AWS documentazione Console di gestione AWS, nei siti AWS Web o nell'applicazione AWS Console Mobile scegliendo l'icona esagonale di Amazon Q. Per ulteriori informazioni, consulta [Get started with Amazon Q Developer](#) User Guide nella Amazon Q Developer User Guide.

Domande di esempio

Di seguito sono riportati alcuni esempi di domande che puoi porre ad Amazon Q:

- How do I get billing support?
- How do I create an EC2 instance?
- How do I troubleshoot a "Failed to load" error?
- How do I close an AWS account?
- Can you connect me with a person?

Console di gestione AWS Accesso privato

Console di gestione AWS Private Access è una funzionalità di sicurezza avanzata per controllare l'accesso a Console di gestione AWS. Console Private Access è utile quando si desidera impedire agli utenti di accedere a utenti imprevisti Account AWS dall'interno della rete. Con questa funzionalità, è possibile limitare l'accesso Console di gestione AWS solo a un gruppo specifico di utenti noti Account AWS quando il traffico proviene dall'interno della rete. Console Private Access è utile anche quando si desidera garantire che tutte le chiamate in arrivo Servizi AWS provengano dall'interno della Console di gestione AWS rete e da account consentiti.

Argomenti

- [Console di servizio e funzionalità Regioni AWS supportate per Private Access](#)
- [Panoramica dei controlli di sicurezza di Console di gestione AWS Private Access](#)
- [Endpoint VPC e configurazione DNS richiesti](#)
- [Implementazione delle policy di controllo dei servizi e delle policy degli endpoint VPC](#)
- [Implementazione di policy basate su identità e altri tipi di policy](#)
- [Prova Private Access Console di gestione AWS](#)
- [Architettura di riferimento](#)

Console di servizio e funzionalità Regioni AWS supportate per Private Access

Console di gestione AWS Private Access supporta solo un sottoinsieme di regioni e AWS servizi. Le console di servizio non supportate saranno inattive nella Console di gestione AWS. Inoltre, alcune Console di gestione AWS funzionalità potrebbero essere disabilitate quando si utilizza l'accesso Console di gestione AWS privato, ad esempio la selezione della [regione predefinita](#) in Impostazioni unificate.

Sono supportate le seguenti regioni e console di servizio.

Regioni supportate

- Stati Uniti orientali (Ohio)
- Stati Uniti orientali (Virginia settentrionale)

- Stati Uniti occidentali (California settentrionale)
- Stati Uniti occidentali (Oregon)
- Asia Pacifico (Hyderabad)
- Asia Pacifico (Mumbai)
- Asia Pacifico (Seoul)
- Asia Pacifico (Osaka)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Malesia)
- Asia Pacifico (Thailandia)
- Asia Pacifico (Tokyo)
- Canada (Centrale)
- Europa (Francoforte)
- Europa (Irlanda)
- Europa (Londra)
- Europe (Paris)
- Europa (Stoccolma)
- Sud America (San Paolo)
- Africa (Città del Capo)
- Asia Pacifico (Hong Kong)
- Asia Pacifico (Giacarta)
- Asia Pacifico (Melbourne)
- Canada occidentale (Calgary)
- Messico (centrale)
- Europa (Milano)
- Europa (Spagna)
- Europa (Zurigo)
- Medio Oriente (Bahrein)

- Medio Oriente (Emirati Arabi Uniti)
- Israele (Tel Aviv)

Console di servizio supportate

- Gateway Amazon API
- AWS App Mesh
- AWS Application Migration Service
- AWS Artifact
- Amazon Athena
- AWS Audit Manager
- AWS Auto Scaling
- AWS Batch
- AWS Billing Conductor
- Gestione dei costi e fatturazione AWS
- Budget AWS
- AWS Certificate Manager
- AWS Cloud Map
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon CodeGuru
- AWS CodePipeline
- Amazon Comprehend
- Amazon Comprehend Medical

- [AWS Compute Optimizer](#)
- [AWS Console Home](#)
- [AWS Control Tower](#)
- [Amazon DataZone](#)
- [AWS Database Migration Service](#)
- [AWS DataSync](#)
- [AWS DeepRacer](#)
- [AWS Direct Connect](#)
- [AWS Directory Service](#)
- [Amazon DocumentDB](#)
- [Amazon DynamoDB](#)
- [Amazon EC2](#)
- [Amazon EC2 Global View](#)
- [EC2 Image Builder](#)
- [Amazon EC2 Instance Connect](#)
- [Amazon Elastic Container Registry](#)
- [Amazon Elastic Container Service](#)
- [AWS Elastic Disaster Recovery](#)
- [Amazon Elastic File System](#)
- [Amazon Elastic Kubernetes Service](#)
- [Elastic Load Balancing](#)
- [Amazon ElastiCache](#)
- [Amazon EMR](#)
- [Amazon EventBridge](#)
- [AWS Firewall Manager](#)
- [GameLift Server Amazon](#)
- [AWS Glue](#)
- [AWS Global Accelerator](#)
- [AWS Glue DataBrew](#)

- AWS Ground Station
- Amazon GuardDuty
- AWS IAM Identity Center
- AWS Identity and Access Management
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- Amazon Kendra
- AWS Key Management Service
- Amazon Kinesis
- Servizio gestito da Amazon per Apache Flink
- Amazon Data Firehose
- Flusso di dati Amazon Kinesis
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Grafana gestito da Amazon
- Amazon Macie
- Amazon Managed Streaming per Apache Kafka
- Amazon Managed Workflows for Apache Airflow (MWAA)
- Suggerimenti di strategia dell'Hub di migrazione AWS
- Amazon MQ
- Strumento di analisi degli accessi alla rete
- AWS Network Firewall
- AWS Network Manager
- OpenSearch Servizio Amazon
- AWS Organizations
- AWS Autorità di certificazione privata
- Pannello di controllo della sanità pubblica

- Amazon Rekognition
- Amazon Relational Database Service
- AWS Resource Access Manager
- AWS Resource Groups e Tag Editor
- Amazon Route 53 Resolver
- Amazon Route 53 Resolver Firewall DNS
- Amazon S3 su Outposts
- Amazon SageMaker
- SageMaker Runtime di Amazon
- Dati sintetici Amazon SageMaker AI
- Gestione dei segreti AWS
- AWS Service Catalog
- AWS Security Hub CSPM
- Service Quotas
- AWS Signer
- Amazon Simple Email Service
- Amazon SNS
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS SQL Workbench
- AWS Step Functions
- Gateway di archiviazione AWS
- Supporto
- AWS Systems Manager
- Amazon Timestream
- AWS Transfer Family
- AWS Trusted Advisor
- Impostazioni unificate
- Gestione indirizzi IP Amazon VPC

- Amazon Virtual Private Cloud
- Amazon WorkSpaces Thin client

Panoramica dei controlli di sicurezza di Console di gestione AWS Private Access

Restrizioni relative all'account Console di gestione AWS dalla tua rete

Console di gestione AWS L'accesso privato è utile negli scenari in cui si desidera limitare l'accesso alla rete solo a un gruppo specifico di utenti noti Account AWS all'interno dell'organizzazione. Console di gestione AWS In questo modo, è possibile impedire agli utenti di accedere ad Account AWS non previsti dall'interno della propria rete. È possibile implementare questi controlli utilizzando la policy degli endpoint VPC della Console di gestione AWS . Per ulteriori informazioni, consulta [Implementazione delle policy di controllo dei servizi e delle policy degli endpoint VPC](#).

Connettività dalla propria rete a Internet

La connettività Internet dalla rete è ancora necessaria per accedere alle risorse utilizzate da Console di gestione AWS, come i contenuti statici (CSSJavaScript, immagini) e a tutte le risorse Servizi AWS non abilitate da [AWS PrivateLink](#). Per un elenco dei domini di primo livello utilizzati da Console di gestione AWS, consulta. [Risoluzione dei problemi](#)

Note

Attualmente, Console di gestione AWS Private Access non supporta endpoint `comestatus.aws.amazon.com`, `health.aws.amazon.com` e `docs.aws.amazon.com`. Dovrai instradare questi domini verso la rete Internet pubblica.

Endpoint VPC e configurazione DNS richiesti

Console di gestione AWS Private Access richiede i seguenti due endpoint VPC per regione. *region*Sostituiscilo con le informazioni sulla tua regione.

1. `com.amazonaws.region.console` per Console di gestione AWS
2. `com.amazonaws.region.signin` per Accedi ad AWS

Note

Effettua sempre il provisioning dell'infrastruttura e della connettività di rete nella regione Stati Uniti orientali (Virginia settentrionale) (us-east-1), indipendentemente dalle altre regioni utilizzate con la Console di gestione AWS. Puoi utilizzare AWS Transit Gateway per configurare la connettività tra Stati Uniti orientali (Virginia settentrionale) e qualsiasi altra regione. Per ulteriori informazioni sull'utilizzo di VPC Transit Gateway, consulta [Nozioni di base sui gateway di transito](#) nella Guida per il gateway di transito di Amazon VPC. Puoi anche usare il peering di Amazon VPC. Per ulteriori informazioni, consulta [Che cos'è il peering di VPC?](#) nella Guida al peering di Amazon VPC. Per confrontare queste opzioni, consulta le opzioni di connettività di [Amazon VPC-to-Amazon VPC nel white paper sulle opzioni di connettività](#) di Amazon Virtual Private Cloud.

Argomenti

- [DNSconfigurazione per e Console di gestione AWS Accedi ad AWS](#)
- [Endpoint VPC e DNS configurazione per AWS i servizi in Console di gestione AWS](#)

DNSconfigurazione per e Console di gestione AWS Accedi ad AWS

Per instradare il traffico di rete verso i rispettivi endpoint VPC, configurare i record DNS nella rete da cui gli utenti accederanno alla Console di gestione AWS. Questi record DNS indirizzeranno il traffico dei browser degli utenti verso gli endpoint VPC creati.

Puoi creare una singola zona ospitata. Tuttavia, gli endpoint come `health.aws.amazon.com` e `docs.aws.amazon.com` non saranno accessibili perché non hanno endpoint VPC. Dovrai instradare questi domini verso la rete Internet pubblica. Ti consigliamo di creare due zone ospitate private per regione, una per `signin.aws.amazon.com` e una per `console.aws.amazon.com` con i seguenti record CNAME:

- Accedi
 - `region.signin.aws.amazon.com` che punta all'endpoint Accedi ad AWS VPC nella zona di accesso dove si trova la regione desiderata DNS *region*
 - `signin.aws.amazon.com` che punta all'endpoint VPC di AWS accesso negli Stati Uniti orientali (Virginia settentrionale) (us-east-1)
- Console

- `region.console.aws.amazon.com` che punta all'endpoint Console di gestione AWS VPC nella zona della console dove si trova la regione desiderata DNS `region`
- `*.region.console.aws.amazon.com` che punta all'endpoint Console di gestione AWS VPC nella zona della console dove si trova la regione desiderata DNS `region`
- `*.region.console.aws.amazon.com` che punta all'endpoint VPC nella zona della console Console di gestione AWS DNS
- Record CNAME senza regioni solo per la Regione Stati Uniti orientali (Virginia settentrionale). Configura sempre la regione Stati Uniti orientali (Virginia settentrionale).
 - `signin.aws.amazon.com` che punta all'endpoint Accedi ad AWS VPC negli Stati Uniti orientali (Virginia settentrionale) (`us-east-1`)
 - `*.console.aws.amazon.com` che punta all'endpoint Console di gestione AWS VPC negli Stati Uniti orientali (Virginia settentrionale) (`us-east-1`)

Per istruzioni sulla creazione di un record CNAME, consulta [Working with records](#) (Utilizzo dei record nella Guida per gli sviluppatori di Amazon Route 53).

Alcune AWS console, tra cui Amazon S3, utilizzano modelli diversi per DNS i loro nomi. Di seguito sono riportati due esempi:

- `support.console.aws.amazon.com`
- `s3.console.aws.amazon.com`

Per poter indirizzare questo traffico verso il tuo endpoint Console di gestione AWS VPC, devi aggiungere quei nomi singolarmente. Per un'esperienza completamente privata, ti consigliamo di configurare il routing per tutti gli endpoint. Tuttavia, questo non è necessario per utilizzare Console di gestione AWS Private Access.

I seguenti json file contengono l'elenco completo Servizio AWS degli endpoint e della console da configurare per regione. Usare il campo `PrivateIpv4DnsNames` sotto l'endpoint `com.amazonaws.region.console` per i nomi DNS.

- <https://configuration.private-access.console.amazonaws.com/us-east-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/us-east-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/us-west-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json>

- <https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-central-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/il-central-1.config.json>

Note

Questo elenco viene aggiornato ogni mese man mano che aggiungiamo ulteriori endpoint all'ambito di Accesso privato alla Console di gestione AWS . Per mantenere aggiornate le zone ospitate private, estrarre periodicamente l'elenco di file precedente.

Se usi Route 53 per configurare il tuo, vai su `v2/hostedzones#` per verificare la DNS configurazione. <https://console.aws.amazon.com/route53/> DNS Per ogni zona ospitata privata in Route 53, verificare che siano presenti i seguenti set di record.

- `console.aws.amazon.com`
- `signin.aws.amazon.com`
- `*. region.console.aws.amazon.com`
- `region.console.aws.amazon.com`
- `*. region.console.aws.amazon.com`
- `signin.aws.amazon.com`
- `region.signin.aws.amazon.com`
- Record aggiuntivi presenti nei file JSON elencati in precedenza

Endpoint VPC e DNS configurazione per AWS i servizi in Console di gestione AWS

Le Console di gestione AWS chiamate vengono effettuate Servizi AWS tramite una combinazione di

richieste dirette del browser e richieste inviate tramite proxy dai server Web. Per indirizzare questo

traffico verso il tuo endpoint Console di gestione AWS VPC, devi aggiungere l'endpoint VPC e configurarlo per ogni servizio dipendente. DNS AWS

I seguenti json file elencano i file AWS PrivateLink Servizi AWS supportati disponibili per l'uso. Se un servizio non si integra con AWS PrivateLink, non è incluso in questi file.

- <https://configuration.private-access.console.amazonaws.com/us-east-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/us-east-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/us-west-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-central-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/il-central-1.config.json>

Utilizzare il campo `ServiceName` per l'endpoint VPC del servizio corrispondente da aggiungere al proprio VPC.

Note

Aggiorniamo questo elenco ogni mese man mano che aggiungiamo il supporto per Private Access a più console di servizio. Console di gestione AWS Per rimanere aggiornati, estrarre periodicamente l'elenco precedente di file e aggiornare gli endpoint VPC.

Implementazione delle policy di controllo dei servizi e delle policy degli endpoint VPC

Puoi utilizzare le policy di controllo del servizio (SCPs) e le policy degli endpoint VPC per Console di gestione AWS Private Access per limitare il set di account autorizzati a utilizzare il VPC all'interno del Console di gestione AWS tuo VPC e delle sue reti locali connesse.

Argomenti

- [Utilizzo di Console di gestione AWS Private Access con le politiche di controllo del servizio AWS Organizations](#)
- [Consenti Console di gestione AWS l'utilizzo solo per gli account e le organizzazioni previsti \(identità affidabili\)](#)

Utilizzo di Console di gestione AWS Private Access con le politiche di controllo del servizio AWS Organizations

Se la tua AWS organizzazione utilizza una policy di controllo dei servizi (SCP) che consente servizi specifici, devi aggiungerla `signin:*` alle azioni consentite. Questa autorizzazione è necessaria perché l'accesso all' Console di gestione AWS endpoint VPC ad accesso privato esegue un'autorizzazione IAM che SCP blocca senza l'autorizzazione. Ad esempio, la seguente politica di controllo dei servizi consente di utilizzare Amazon EC2 e CloudWatch i servizi nell'organizzazione, anche quando vi si accede tramite un endpoint di accesso Console di gestione AWS privato.

```
{
  "Effect": "Allow",
  "Action": [
    "signin:*",
    "ec2:*",
    "cloudwatch:*",
    ... Other services allowed
  ],
  "Resource": "*"
}
```

Per ulteriori informazioni in merito SCPs, consulta [Service control policies \(SCPs\) nella Guida](#) per l'AWS Organizations utente.

Consenti Console di gestione AWS l'utilizzo solo per gli account e le organizzazioni previsti (identità affidabili)

Console di gestione AWS e Accedi ad AWS supportano una policy degli endpoint VPC che controlla in modo specifico l'identità dell'account che ha effettuato l'accesso.

A differenza di altre policy degli endpoint VPC, la policy viene esaminata prima dell'autenticazione. Di conseguenza, controlla specificamente l'accesso e l'uso solo della sessione autenticata e non le azioni specifiche del servizio intraprese AWS dalla sessione. Ad esempio, quando la sessione accede a una console di AWS servizio, come la console Amazon EC2, queste policy sugli endpoint VPC non verranno valutate rispetto alle azioni di Amazon EC2 intraprese per visualizzare quella pagina. Piuttosto, puoi utilizzare le policy IAM associate all'IAM Principal che ha effettuato l'accesso per controllarne l'autorizzazione alle azioni di servizio. AWS

Note

Le policy degli endpoint VPC per gli endpoint VPC e gli endpoint Console di gestione AWS SignIn VPC supportano solo un sottoinsieme limitato di formulazioni di policy. Ogni Principal e Resource devono essere impostati su * e Action dovrebbe essere * o signin:*. È possibile controllare l'accesso agli endpoint VPC utilizzando aws:PrincipalOrgId e le chiavi di condizione aws:PrincipalAccount.

Le seguenti politiche sono consigliate sia per gli endpoint Console che SignIn VPC.

Questa politica degli endpoint VPC consente l'accesso all' Account AWS AWS organizzazione specificata e blocca l'accesso a qualsiasi altro account.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
```

```
    "StringEquals": {
      "aws:PrincipalOrgId": "o-xxxxxxxxxxxx"
    }
  }
}
]
```

Questa policy sugli endpoint VPC limita l'accesso a un elenco di account specifici Account AWS e blocca l'accesso a qualsiasi altro account.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": [ "111122223333", "222233334444" ]
        }
      }
    }
  ]
}
```

Le policy che limitano Account AWS un'organizzazione sugli endpoint VPC Console di gestione AWS e di accesso vengono valutate al momento dell'accesso e periodicamente rivalutate per le sessioni esistenti.

Implementazione di policy basate su identità e altri tipi di policy

Puoi gestire l'accesso AWS creando policy e collegandole alle identità o alle risorse IAM (utenti, gruppi di utenti o ruoli). AWS Questa pagina descrive come funzionano le policy se utilizzate insieme a Console di gestione AWS Private Access.

Chiavi contestuali delle condizioni AWS globali supportate

Console di gestione AWS Private Access non supporta `aws:SourceVpce` le chiavi di contesto a condizione `aws:VpcSourceIp` AWS globale. È possibile invece utilizzare nelle proprie policy la condizione IAM `aws:SourceVpc`, quando si utilizza l'accesso privato alla Console di gestione AWS.

Come funziona Console di gestione AWS Private Access con `aws:SourceVpc`

Questa sezione descrive i vari percorsi di rete a cui Console di gestione AWS possono accedere le richieste generate da te Servizi AWS. In generale, le console di AWS servizio vengono implementate con una combinazione di richieste dirette del browser e richieste inviate tramite proxy dai server Console di gestione AWS Web a. Servizi AWS Queste implementazioni sono soggette a modifica senza preavviso. Se i tuoi requisiti di sicurezza includono l'accesso all' Servizi AWS utilizzo degli endpoint VPC, ti consigliamo di configurare gli endpoint VPC per tutti i servizi che intendi utilizzare da VPC, direttamente o tramite Private Access. Console di gestione AWS Inoltre, è necessario utilizzare la condizione `aws:SourceVpc` IAM nelle policy anziché `aws:SourceVpce` valori specifici con la funzionalità Private Access. Console di gestione AWS Questa sezione fornisce dettagli su come funzionano i diversi percorsi di rete.

Dopo aver effettuato l'accesso Console di gestione AWS, un utente effettua le richieste Servizi AWS tramite una combinazione di richieste dirette del browser e richieste che vengono inoltrate dai server Console di gestione AWS Web ai AWS server. Ad esempio, le richieste di dati CloudWatch grafici vengono effettuate direttamente dal browser. Alcune richieste AWS di console di servizio, come Amazon S3, vengono invece inoltrate dal server Web ad Amazon S3.

Per le richieste dirette del browser, l'utilizzo di Console di gestione AWS Private Access non cambia nulla. Come in precedenza, la richiesta raggiunge il servizio tramite il percorso di rete che il VPC ha configurato per raggiungere `monitoring.region.amazonaws.com`. Se il VPC è configurato con un endpoint VPC `percom.amazonaws.region.monitoring`, la richiesta arriverà attraverso CloudWatch quell'endpoint VPC. CloudWatch Se non esiste un endpoint VPC per CloudWatch, la richiesta arriverà CloudWatch al suo endpoint pubblico, tramite un Internet Gateway sul VPC. Le richieste che arrivano CloudWatch tramite l'endpoint CloudWatch VPC avranno le condizioni IAM `aws:SourceVpc` e saranno `aws:SourceVpce` impostate sui rispettivi valori. Quelle che lo raggiungeranno CloudWatch tramite l'endpoint pubblico avranno `aws:SourceIp` impostato l'indirizzo IP di origine della richiesta. Per ulteriori informazioni su queste chiavi di condizione IAM, consulta la sezione [Global condition keys](#) (Chiavi di condizione globali) nella Guida per l'utente IAM.

Per le richieste inviate tramite proxy dal server Console di gestione AWS Web, ad esempio la richiesta effettuata dalla console Amazon S3 per elencare i bucket quando si visita la console Amazon S3, il percorso di rete è diverso. Queste richieste non vengono avviate dal proprio VPC e quindi non utilizzano l'endpoint VPC che si potrebbe aver configurato sul proprio VPC per quel servizio. Anche se in questo caso si dispone di un endpoint VPC per Amazon S3, la richiesta della sessione ad Amazon S3 di elencare i bucket non utilizza l'endpoint VPC di Amazon S3. Tuttavia, quando utilizzi Console di gestione AWS Private Access con servizi supportati, queste richieste (ad esempio, ad Amazon S3) includeranno la chiave di `aws:SourceVpc` condizione nel contesto della richiesta. La chiave di `aws:SourceVpc` condizione verrà impostata sull'ID VPC in cui vengono distribuiti gli endpoint di accesso Console di gestione AWS privato per l'accesso e la console. Pertanto, se si utilizzano restrizioni `aws:SourceVpc` nelle policy basate sull'identità, è necessario aggiungere l'ID VPC del VPC che ospita gli endpoint di accesso e di accesso privato alla Console di gestione AWS. La `aws:SourceVpc` condizione verrà impostata sul rispettivo endpoint IDs VPC di accesso o console.

Note

Se desideri che gli utenti continuino ad accedere alle console di servizio non supportate da Accesso privato alla Console di gestione AWS, devi includere un elenco di indirizzi di rete pubblici previsti (ad esempio l'intervallo di rete on-premise) utilizzando la chiave di condizione `aws:SourceIP` nelle policy basate sull'identità degli utenti.

In che modo si riflettono i diversi percorsi di rete CloudTrail

I diversi percorsi di rete utilizzati dalle richieste generate dall'utente Console di gestione AWS si riflettono nella cronologia CloudTrail degli eventi.

Per le richieste dirette tramite browser, l'utilizzo di Console di gestione AWS Private Access non cambia nulla. CloudTrail gli eventi includeranno dettagli sulla connessione, come l'ID dell'endpoint VPC utilizzato per effettuare la chiamata all'API del servizio.

Per le richieste inviate tramite proxy dal server Console di gestione AWS Web, CloudTrail gli eventi non includeranno alcun dettaglio relativo al VPC. Tuttavia, le richieste iniziali necessarie per Accedi ad AWS stabilire la sessione del browser, ad esempio il tipo di `AwsConsoleSignIn` evento, includeranno l'ID dell'endpoint Accedi ad AWS VPC nei dettagli dell'evento.

Prova Private Access Console di gestione AWS

Questa sezione descrive come configurare e testare Console di gestione AWS Private Access in un nuovo account.

Console di gestione AWS Private Access è una funzionalità di sicurezza avanzata e richiede conoscenze preliminari sulla rete e sulla configurazione VPCs. Questo argomento descrive come provare Accesso privato alla Console di gestione AWS senza un'infrastruttura completa.

Argomenti

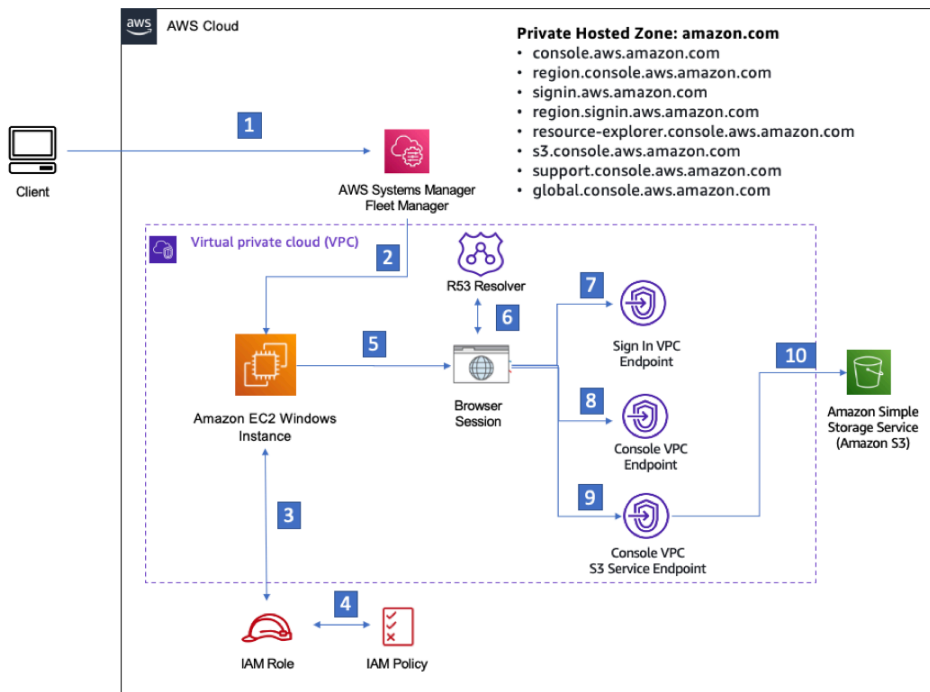
- [Test della configurazione con Amazon EC2](#)
- [Configurazione di prova con Amazon WorkSpaces](#)
- [Test della configurazione VPC con le policy IAM](#)

Test della configurazione con Amazon EC2

[Amazon Elastic Compute Cloud](#) (Amazon EC2) fornisce capacità di calcolo scalabile nel cloud di Amazon Web Services. Puoi utilizzare Amazon EC2 per avviare il numero di server virtuali necessari, configurare la sicurezza e i servizi di rete, nonché gestire l'archiviazione. In questa configurazione viene utilizzato [Fleet Manager](#), una funzionalità di AWS Systems Manager, per connettersi alle istanze Windows di Amazon EC2 utilizzando il protocollo RDP (Remote Desktop Protocol).

Questa guida illustra un ambiente di test per configurare e provare una connessione Console di gestione AWS Private Access ad Amazon Simple Storage Service da un'istanza Amazon EC2. Questo tutorial serve CloudFormation a creare e configurare la configurazione di rete che verrà utilizzata da Amazon EC2 per visualizzare questa funzionalità.

Il diagramma seguente descrive il flusso di lavoro per l'utilizzo di Amazon EC2 per accedere a una configurazione di Accesso privato alla Console di gestione AWS . Mostra come un utente è connesso ad Amazon S3 mediante un endpoint privato.



- 1 Client connects to the Fleet manager using Key pair.
- 2 Authenticated session connection to Windows Server using the Remote Desktop Protocol (RDP).
- 3 EC2 instance confirms credentials for IAM role in use as instance profile.
- 4 EC2 instance profile role permissions check.
- 5 Initiate browser session in EC2 instance.
- 6 Route53 resolver with endpoint address.
- 7 Private Sign in endpoint.
- 8 Private Console endpoint.
- 9 S3 service private endpoint.
- 10 Connected to S3 service via private endpoint.

Copia il seguente CloudFormation modello e salvalo in un file che utilizzerai nella fase tre della procedura Per configurare una rete.

Note

Questo CloudFormation modello utilizza configurazioni che attualmente non sono supportate nella regione di Israele (Tel Aviv).

Console di gestione AWS Modello Amazon CloudFormation EC2 per ambiente di accesso privato

Description: |
 AWS Management Console Private Access.
 Parameters:
 VpcCIDR:
 Type: String
 Default: 172.16.0.0/16
 Description: CIDR range for VPC
 Ec2KeyPair:
 Type: AWS::EC2::KeyPair::KeyName

Description: The EC2 KeyPair to use to connect to the Windows instance

PublicSubnet1CIDR:

Type: String

Default: 172.16.1.0/24

Description: CIDR range for Public Subnet A

PublicSubnet2CIDR:

Type: String

Default: 172.16.0.0/24

Description: CIDR range for Public Subnet B

PublicSubnet3CIDR:

Type: String

Default: 172.16.2.0/24

Description: CIDR range for Public Subnet C

PrivateSubnet1CIDR:

Type: String

Default: 172.16.4.0/24

Description: CIDR range for Private Subnet A

PrivateSubnet2CIDR:

Type: String

Default: 172.16.5.0/24

Description: CIDR range for Private Subnet B

PrivateSubnet3CIDR:

Type: String

Default: 172.16.3.0/24

Description: CIDR range for Private Subnet C

LatestWindowsAmiId:

Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'

Default: '/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-Base'

InstanceTypeParameter:

Type: String

Default: 't3.medium'

Resources:

#####

```
# VPC AND SUBNETS
#####

AppVPC:
  Type: 'AWS::EC2::VPC'
  Properties:
    CidrBlock: !Ref VpcCIDR
    InstanceTenancy: default
    EnableDnsSupport: true
    EnableDnsHostnames: true

PublicSubnetA:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet1CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone:
      Fn::Select:
        - 0
        - Fn::GetAZs: ""

PublicSubnetB:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet2CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone:
      Fn::Select:
        - 1
        - Fn::GetAZs: ""

PublicSubnetC:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet3CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone:
      Fn::Select:
        - 2
        - Fn::GetAZs: ""
```

```
PrivateSubnetA:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PrivateSubnet1CIDR
    AvailabilityZone:
      Fn::Select:
        - 0
        - Fn::GetAZs: ""

PrivateSubnetB:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PrivateSubnet2CIDR
    AvailabilityZone:
      Fn::Select:
        - 1
        - Fn::GetAZs: ""

PrivateSubnetC:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PrivateSubnet3CIDR
    AvailabilityZone:
      Fn::Select:
        - 2
        - Fn::GetAZs: ""

InternetGateway:
  Type: AWS::EC2::InternetGateway

InternetGatewayAttachment:
  Type: AWS::EC2::VPCEGatewayAttachment
  Properties:
    InternetGatewayId: !Ref InternetGateway
    VpcId: !Ref AppVPC

NatGatewayEIP:
  Type: AWS::EC2::EIP
  DependsOn: InternetGatewayAttachment

NatGateway:
```

```
Type: AWS::EC2::NatGateway
Properties:
  AllocationId: !GetAtt NatGatewayEIP.AllocationId
  SubnetId: !Ref PublicSubnetA
```

```
#####
```

```
# Route Tables
```

```
#####
```

```
PrivateRouteTable:
  Type: 'AWS::EC2::RouteTable'
  Properties:
    VpcId: !Ref AppVPC
```

```
DefaultPrivateRoute:
  Type: AWS::EC2::Route
  Properties:
    RouteTableId: !Ref PrivateRouteTable
    DestinationCidrBlock: 0.0.0.0/0
    NatGatewayId: !Ref NatGateway
```

```
PrivateSubnetRouteTableAssociation1:
  Type: 'AWS::EC2::SubnetRouteTableAssociation'
  Properties:
    RouteTableId: !Ref PrivateRouteTable
    SubnetId: !Ref PrivateSubnetA
```

```
PrivateSubnetRouteTableAssociation2:
  Type: 'AWS::EC2::SubnetRouteTableAssociation'
  Properties:
    RouteTableId: !Ref PrivateRouteTable
    SubnetId: !Ref PrivateSubnetB
```

```
PrivateSubnetRouteTableAssociation3:
  Type: 'AWS::EC2::SubnetRouteTableAssociation'
  Properties:
    RouteTableId: !Ref PrivateRouteTable
    SubnetId: !Ref PrivateSubnetC
```

```
PublicRouteTable:
  Type: AWS::EC2::RouteTable
  Properties:
    VpcId: !Ref AppVPC
```

```
DefaultPublicRoute:
  Type: AWS::EC2::Route
  DependsOn: InternetGatewayAttachment
  Properties:
    RouteTableId: !Ref PublicRouteTable
    DestinationCidrBlock: 0.0.0.0/0
    GatewayId: !Ref InternetGateway

PublicSubnetARouteTableAssociation1:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    RouteTableId: !Ref PublicRouteTable
    SubnetId: !Ref PublicSubnetA

PublicSubnetBRouteTableAssociation2:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    RouteTableId: !Ref PublicRouteTable
    SubnetId: !Ref PublicSubnetB

PublicSubnetBRouteTableAssociation3:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    RouteTableId: !Ref PublicRouteTable
    SubnetId: !Ref PublicSubnetC

#####
# SECURITY GROUPS
#####

VPCEndpointSecurityGroup:
  Type: 'AWS::EC2::SecurityGroup'
  Properties:
    GroupDescription: Allow TLS for VPC Endpoint
    VpcId: !Ref AppVPC
    SecurityGroupIngress:
      - IpProtocol: tcp
        FromPort: 443
        ToPort: 443
        CidrIp: !GetAtt AppVPC.CidrBlock

EC2SecurityGroup:
  Type: 'AWS::EC2::SecurityGroup'
```

Properties:

GroupDescription: Default EC2 Instance SG
VpcId: !Ref AppVPC

#####

VPC ENDPOINTS

#####

VPCEndpointGatewayS3:

Type: 'AWS::EC2::VPCEndpoint'

Properties:

ServiceName: !Sub 'com.amazonaws.\${AWS::Region}.s3'
VpcEndpointType: Gateway
VpcId: !Ref AppVPC
RouteTableIds:
- !Ref PrivateRouteTable

VPCEndpointInterfaceSSM:

Type: 'AWS::EC2::VPCEndpoint'

Properties:

VpcEndpointType: Interface
PrivateDnsEnabled: false
SubnetIds:
- !Ref PrivateSubnetA
- !Ref PrivateSubnetB
SecurityGroupIds:
- !Ref VPCEndpointSecurityGroup
ServiceName: !Sub 'com.amazonaws.\${AWS::Region}.ssm'
VpcId: !Ref AppVPC

VPCEndpointInterfaceEc2messages:

Type: 'AWS::EC2::VPCEndpoint'

Properties:

VpcEndpointType: Interface
PrivateDnsEnabled: false
SubnetIds:
- !Ref PrivateSubnetA
- !Ref PrivateSubnetB
- !Ref PrivateSubnetC
SecurityGroupIds:
- !Ref VPCEndpointSecurityGroup
ServiceName: !Sub 'com.amazonaws.\${AWS::Region}.ec2messages'
VpcId: !Ref AppVPC

```
VPCEndpointInterfaceSsmmessages:
  Type: 'AWS::EC2::VPCEndpoint'
  Properties:
    VpcEndpointType: Interface
    PrivateDnsEnabled: false
    SubnetIds:
      - !Ref PrivateSubnetA
      - !Ref PrivateSubnetB
      - !Ref PrivateSubnetC
    SecurityGroupIds:
      - !Ref VPCEndpointSecurityGroup
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssmmessages'
    VpcId: !Ref AppVPC
```

```
VPCEndpointInterfaceSignin:
  Type: 'AWS::EC2::VPCEndpoint'
  Properties:
    VpcEndpointType: Interface
    PrivateDnsEnabled: false
    SubnetIds:
      - !Ref PrivateSubnetA
      - !Ref PrivateSubnetB
      - !Ref PrivateSubnetC
    SecurityGroupIds:
      - !Ref VPCEndpointSecurityGroup
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
    VpcId: !Ref AppVPC
```

```
VPCEndpointInterfaceConsole:
  Type: 'AWS::EC2::VPCEndpoint'
  Properties:
    VpcEndpointType: Interface
    PrivateDnsEnabled: false
    SubnetIds:
      - !Ref PrivateSubnetA
      - !Ref PrivateSubnetB
      - !Ref PrivateSubnetC
    SecurityGroupIds:
      - !Ref VPCEndpointSecurityGroup
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
    VpcId: !Ref AppVPC
```

```
#####
```

```
# ROUTE53 RESOURCES
```

```
#####
```

```
ConsoleHostedZone:
```

```
Type: "AWS::Route53::HostedZone"
```

```
Properties:
```

```
HostedZoneConfig:
```

```
Comment: 'Console VPC Endpoint Hosted Zone'
```

```
Name: 'console.aws.amazon.com'
```

```
VPCs:
```

```
-
```

```
VPCId: !Ref AppVPC
```

```
VPCRegion: !Ref "AWS::Region"
```

```
ConsoleRecordGlobal:
```

```
Type: AWS::Route53::RecordSet
```

```
Properties:
```

```
HostedZoneId: !Ref 'ConsoleHostedZone'
```

```
Name: 'console.aws.amazon.com'
```

```
AliasTarget:
```

```
DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt  
VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt  
VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
Type: A
```

```
GlobalConsoleRecord:
```

```
Type: AWS::Route53::RecordSet
```

```
Properties:
```

```
HostedZoneId: !Ref 'ConsoleHostedZone'
```

```
Name: 'global.console.aws.amazon.com'
```

```
AliasTarget:
```

```
DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt  
VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt  
VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
Type: A
```

```
ConsoleS3ProxyRecordGlobal:
```

```
Type: AWS::Route53::RecordSet
```

```
Properties:
```

```
HostedZoneId: !Ref 'ConsoleHostedZone'
```

```
Name: 's3.console.aws.amazon.com'
```

```
AliasTarget:
```

```
    DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    Type: A

ConsoleSupportProxyRecordGlobal:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: "support.console.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

ExplorerProxyRecordGlobal:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: "resource-explorer.console.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

WidgetProxyRecord:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: "*.widget.console.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ["1", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
      HostedZoneId: !Select ["0", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
      Type: A

ConsoleRecordRegional:
  Type: AWS::Route53::RecordSet
```

Properties:

HostedZoneId: !Ref 'ConsoleHostedZone'

Name: !Sub "\${AWS::Region}.console.aws.amazon.com"

AliasTarget:

DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt VPCEndpointInterfaceConsole.DnsEntries]]]

HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt VPCEndpointInterfaceConsole.DnsEntries]]]

Type: A

ConsoleRecordRegionalMultiSession:

Type: AWS::Route53::RecordSet

Properties:

HostedZoneId: !Ref 'ConsoleHostedZone'

Name: !Sub ".*\${AWS::Region}.console.aws.amazon.com"

AliasTarget:

DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt VPCEndpointInterfaceConsole.DnsEntries]]]

HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt VPCEndpointInterfaceConsole.DnsEntries]]]

Type: A

SigninHostedZone:

Type: "AWS::Route53::HostedZone"

Properties:**HostedZoneConfig:**

Comment: 'Signin VPC Endpoint Hosted Zone'

Name: 'signin.aws.amazon.com'

VPCs:

-

VPCId: !Ref AppVPC

VPCRegion: !Ref "AWS::Region"

SigninRecordGlobal:

Type: AWS::Route53::RecordSet

Properties:

HostedZoneId: !Ref 'SigninHostedZone'

Name: 'signin.aws.amazon.com'

AliasTarget:

DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt VPCEndpointInterfaceSignin.DnsEntries]]]

HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt VPCEndpointInterfaceSignin.DnsEntries]]]

Type: A

```

SigninRecordRegional:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'SigninHostedZone'
    Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
    Type: A

```

```

#####
# EC2 INSTANCE
#####

```

```

Ec2InstanceRole:
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
      Version: 2012-10-17
      Statement:
        -
          Effect: Allow
          Principal:
            Service:
              - ec2.amazonaws.com
          Action:
            - sts:AssumeRole
    Path: /
    ManagedPolicyArns:
      - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

```

```

Ec2InstanceProfile:
  Type: AWS::IAM::InstanceProfile
  Properties:
    Path: /
    Roles:
      - !Ref Ec2InstanceRole

```

```

EC2WinInstance:
  Type: 'AWS::EC2::Instance'
  Properties:

```

```
ImageId: !Ref LatestWindowsAmiId
IamInstanceProfile: !Ref Ec2InstanceProfile
KeyName: !Ref Ec2KeyPair
InstanceType:
  Ref: InstanceTypeParameter
SubnetId: !Ref PrivateSubnetA
SecurityGroupIds:
  - Ref: EC2SecurityGroup
BlockDeviceMappings:
  - DeviceName: /dev/sda1
    Ebs:
      VolumeSize: 50
Tags:
  - Key: "Name"
    Value: "Console VPCE test instance"
```

Configurazione di una rete

1. Accedere all'account di gestione dell'organizzazione e aprire la [console CloudFormation](#).
2. Seleziona Crea stack.
3. Scegliere Con nuove risorse (standard). Carica il file CloudFormation modello che hai creato in precedenza e scegli Avanti.
4. Inserire un nome per lo stack, ad esempio **PrivateConsoleNetworkForS3**, quindi scegliere Successivo.
5. Per VPC e sottoreti, inserire gli intervalli IP CIDR preferiti o utilizzare i valori predefiniti forniti. Se utilizzi i valori predefiniti, verifica che non si sovrappongano alle risorse VPC esistenti nel tuo Account AWS
6. Per il KeyPair parametro Ec2, selezionane una tra le coppie di chiavi Amazon EC2 esistenti nel tuo account. Se non si dispone di una coppia di chiavi Amazon EC2 esistente, è necessario creare una prima di passare alla fase successiva. Per ulteriori informazioni, consulta [Create a key pair using Amazon EC2 nella Amazon EC2 User Guide](#).
7. Seleziona Crea stack.
8. Dopo aver creato lo stack, scegliere la scheda Risorse per visualizzare le risorse che sono state create.

Eseguire la connessione all'istanza Amazon EC2

1. Accedere all'account di gestione dell'organizzazione e aprire la [console Amazon EC2](#).
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Nella pagina Istanze, seleziona l'istanza di test Console VPCE creata dal modello. CloudFormation Quindi scegliere Connetti.

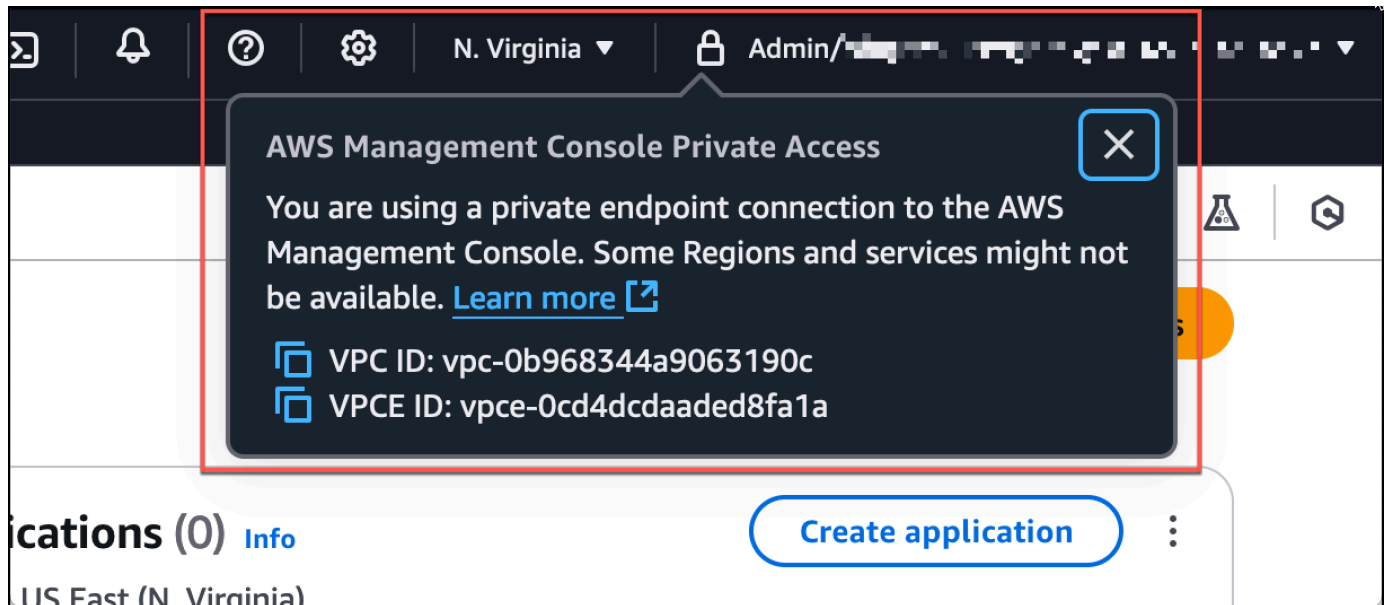
Note

Questo esempio utilizza Fleet Manager, una funzionalità di AWS Systems Manager Explorer, per connettersi a Windows Server. Potrebbero essere necessari alcuni minuti prima che la connessione possa essere avviata.

4. Nella pagina Connetti all'istanza, scegliere client RDP, quindi Connettiti tramite Fleet Manager.
5. Scegliere Desktop remoto di Fleet Manager.
6. Per ottenere la password amministrativa per l'istanza Amazon EC2 e accedere al desktop di Windows tramite l'interfaccia Web, utilizza la chiave privata associata alla coppia di chiavi Amazon EC2 utilizzata durante CloudFormation la creazione del modello.
7. Dall'istanza Amazon EC2 per Windows, apri il file Console di gestione AWS nel browser.
8. Dopo aver effettuato l'accesso con AWS le tue credenziali, apri la console [Amazon S3](#) e verifica di essere connesso Console di gestione AWS tramite Private Access.

Per testare la configurazione di Console di gestione AWS Private Access

1. Accedere all'account di gestione dell'organizzazione e aprire la [console Amazon S3](#).
2. Scegliere l'icona di blocco privato nella barra di navigazione per visualizzare l'endpoint VPC in uso. La schermata seguente mostra la posizione dell'icona di blocco privato e le informazioni sul VPC.



Configurazione di prova con Amazon WorkSpaces

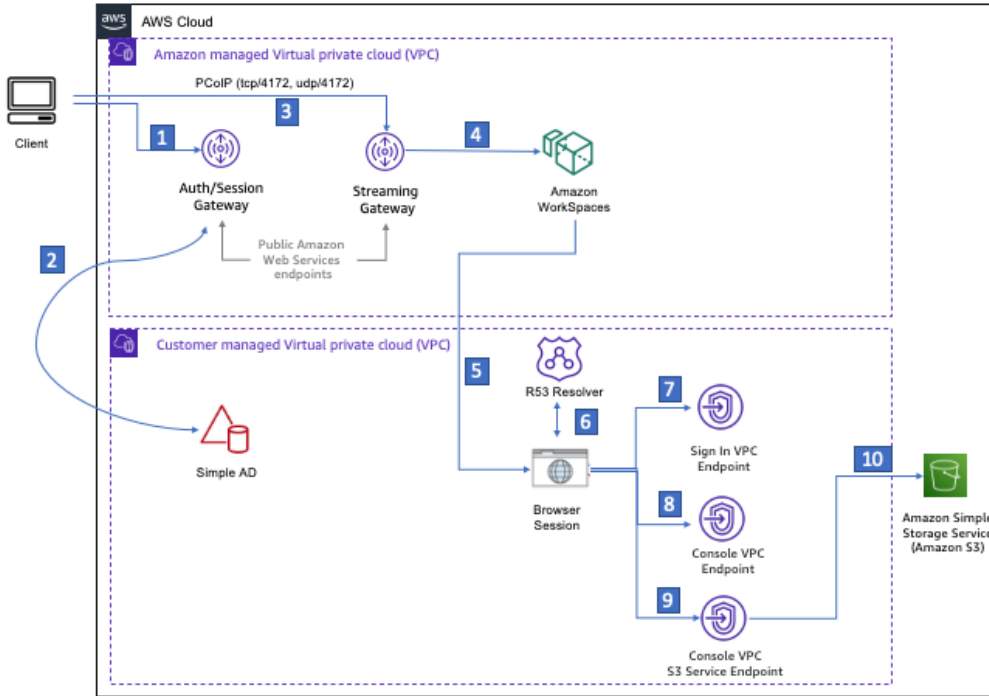
Amazon WorkSpaces consente di fornire desktop virtuali basati su cloud Windows, Amazon Linux o Ubuntu Linux per i tuoi utenti, noti come WorkSpaces. È possibile aggiungere o rimuovere rapidamente utenti man mano che le proprie esigenze cambiano. Gli utenti possono accedere ai propri desktop virtuali da più dispositivi o browser Web. Per ulteriori informazioni WorkSpaces, consulta la [Amazon WorkSpaces Administration Guide](#).

L'esempio in questa sezione descrive un ambiente di test in cui un ambiente utente utilizza un browser Web in esecuzione su un WorkSpace per accedere a Console di gestione AWS Private Access. Poi, l'utente visita la console di Amazon Simple Storage Service. Questo WorkSpace ha lo scopo di simulare l'esperienza di un utente aziendale con un laptop su una rete connessa a VPC, accedendovi dal Console di gestione AWS proprio browser.

Questo tutorial serve AWS CloudFormation a creare e configurare la configurazione della rete e una Simple Active Directory da utilizzare WorkSpaces insieme alle istruzioni dettagliate per configurare e utilizzare il WorkSpace Console di gestione AWS

Il diagramma seguente descrive il flusso di lavoro per l'utilizzo di una configurazione WorkSpace di test di Console di gestione AWS Private Access. Mostra la relazione tra un client WorkSpace, un VPC gestito da Amazon e un VPC gestito dal cliente.

- Private Hosted Zone: amazon.com**
- console.aws.amazon.com
 - region.console.aws.amazon.com
 - signin.aws.amazon.com
 - region.signin.aws.amazon.com
 - resource-explorer.console.aws.amazon.com
 - s3.console.aws.amazon.com
 - support.console.aws.amazon.com
 - global.console.aws.amazon.com



- 1 Login information sent to authentication gateway
- 2 Authentication against Simple AD
- 3 Streaming Traffic to Streaming gateway
- 4 Each Workspace is connected to two networks simultaneously, Amazon-managed VPC for streaming traffic and Customer managed VPC handling all other traffic.
- 5 Initiate browser session
- 6 Route53 resolver with endpoint address.
- 7 Private Sign in endpoint
- 8 Private Console endpoint
- 9 S3 service private endpoint
- 10 Connected to S3 service via private endpoint

Copia il seguente CloudFormation modello e salvalo in un file che utilizzerai nel passaggio 3 della procedura per configurare una rete.

Console di gestione AWS CloudFormation Modello di ambiente Private Access

Description: |
AWS Management Console Private Access.

Parameters:

VpcCIDR:

Type: String

Default: 172.16.0.0/16

Description: CIDR range for VPC

PublicSubnet1CIDR:

Type: String

Default: 172.16.1.0/24

```
Description: CIDR range for Public Subnet A

PublicSubnet2CIDR:
  Type: String
  Default: 172.16.0.0/24
  Description: CIDR range for Public Subnet B

PrivateSubnet1CIDR:
  Type: String
  Default: 172.16.4.0/24
  Description: CIDR range for Private Subnet A

PrivateSubnet2CIDR:
  Type: String
  Default: 172.16.5.0/24
  Description: CIDR range for Private Subnet B

DSAdminPasswordResourceName:
  Type: String
  Default: ADAdminSecret
  Description: Password for directory services admin

# Amazon WorkSpaces is available in a subset of the Availability Zones for each
# supported Region.
# https://docs.aws.amazon.com/workspaces/latest/adminguide/azs-workspaces.html
Mappings:
  RegionMap:
    us-east-1:
      az1: use1-az2
      az2: use1-az4
      az3: use1-az6
    us-west-2:
      az1: usw2-az1
      az2: usw2-az2
      az3: usw2-az3
    ap-south-1:
      az1: aps1-az1
      az2: aps1-az2
      az3: aps1-az3
    ap-northeast-2:
      az1: apne2-az1
      az2: apne2-az3
    ap-southeast-1:
      az1: apse1-az1
```

```
    az2: apse1-az2
ap-southeast-2:
    az1: apse2-az1
    az2: apse2-az3
ap-northeast-1:
    az1: apne1-az1
    az2: apne1-az4
ca-central-1:
    az1: cac1-az1
    az2: cac1-az2
eu-central-1:
    az1: euc1-az2
    az2: euc1-az3
eu-west-1:
    az1: euw1-az1
    az2: euw1-az2
eu-west-2:
    az1: euw2-az2
    az2: euw2-az3
sa-east-1:
    az1: sae1-az1
    az2: sae1-az3
```

Resources:

```
iamLambdaExecutionRole:
```

```
  Type: AWS::IAM::Role
```

```
  Properties:
```

```
    AssumeRolePolicyDocument:
```

```
      Version: 2012-10-17
```

```
      Statement:
```

```
        - Effect: Allow
```

```
          Principal:
```

```
            Service:
```

```
              - lambda.amazonaws.com
```

```
          Action:
```

```
            - 'sts:AssumeRole'
```

```
    ManagedPolicyArns:
```

```
      - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
```

```
    Policies:
```

```
      - PolicyName: describe-ec2-az
```

```
        PolicyDocument:
```

```
          Version: "2012-10-17"
```

```
          Statement:
```

```

    - Effect: Allow
      Action:
        - 'ec2:DescribeAvailabilityZones'
      Resource: '*'
    MaxSessionDuration: 3600
    Path: /service-role/

fnZoneIdtoZoneName:
  Type: AWS::Lambda::Function
  Properties:
    Runtime: python3.8
    Handler: index.lambda_handler
    Code:
      ZipFile: |
        import boto3
        import cfnresponse

        def zoneId_to_zoneName(event, context):
            responseData = {}
            ec2 = boto3.client('ec2')
            describe_az = ec2.describe_availability_zones()
            for az in describe_az['AvailabilityZones']:
                if event['ResourceProperties']['ZoneId'] == az['ZoneId']:
                    responseData['ZoneName'] = az['ZoneName']
                    cfnresponse.send(event, context, cfnresponse.SUCCESS,
responseData, str(az['ZoneId']))

            def no_op(event, context):
                print(event)
                responseData = {}
                cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
str(event['RequestId']))

            def lambda_handler(event, context):
                if event['RequestType'] == ('Create' or 'Update'):
                    zoneId_to_zoneName(event, context)
                else:
                    no_op(event, context)
    Role: !GetAtt iamLambdaExecutionRole.Arn

getAZ1:
  Type: "Custom::zone-id-zone-name"
  Properties:
    ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn

```

```
    ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az1 ]
getAZ2:
  Type: "Custom::zone-id-zone-name"
  Properties:
    ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
    ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az2 ]
```

```
#####
```

```
# VPC AND SUBNETS
```

```
#####
```

```
AppVPC:
  Type: 'AWS::EC2::VPC'
  Properties:
    CidrBlock: !Ref VpcCIDR
    InstanceTenancy: default
    EnableDnsSupport: true
    EnableDnsHostnames: true
```

```
PublicSubnetA:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet1CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone: !GetAtt getAZ1.ZoneName
```

```
PublicSubnetB:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet2CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone: !GetAtt getAZ2.ZoneName
```

```
PrivateSubnetA:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PrivateSubnet1CIDR
    AvailabilityZone: !GetAtt getAZ1.ZoneName
```

```
PrivateSubnetB:
  Type: 'AWS::EC2::Subnet'
```

Properties:

```
VpcId: !Ref AppVPC
CidrBlock: !Ref PrivateSubnet2CIDR
AvailabilityZone: !GetAtt getAZ2.ZoneName
```

InternetGateway:

```
Type: AWS::EC2::InternetGateway
```

InternetGatewayAttachment:

```
Type: AWS::EC2::VPCGatewayAttachment
Properties:
  InternetGatewayId: !Ref InternetGateway
  VpcId: !Ref AppVPC
```

NatGatewayEIP:

```
Type: AWS::EC2::EIP
DependsOn: InternetGatewayAttachment
```

NatGateway:

```
Type: AWS::EC2::NatGateway
Properties:
  AllocationId: !GetAtt NatGatewayEIP.AllocationId
  SubnetId: !Ref PublicSubnetA
```

```
#####
```

Route Tables

```
#####
```

PrivateRouteTable:

```
Type: 'AWS::EC2::RouteTable'
Properties:
  VpcId: !Ref AppVPC
```

DefaultPrivateRoute:

```
Type: AWS::EC2::Route
Properties:
  RouteTableId: !Ref PrivateRouteTable
  DestinationCidrBlock: 0.0.0.0/0
  NatGatewayId: !Ref NatGateway
```

PrivateSubnetRouteTableAssociation1:

```
Type: 'AWS::EC2::SubnetRouteTableAssociation'
Properties:
  RouteTableId: !Ref PrivateRouteTable
```

```
SubnetId: !Ref PrivateSubnetA
```

```
PrivateSubnetRouteTableAssociation2:
```

```
  Type: 'AWS::EC2::SubnetRouteTableAssociation'
```

```
  Properties:
```

```
    RouteTableId: !Ref PrivateRouteTable
```

```
    SubnetId: !Ref PrivateSubnetB
```

```
PublicRouteTable:
```

```
  Type: AWS::EC2::RouteTable
```

```
  Properties:
```

```
    VpcId: !Ref AppVPC
```

```
DefaultPublicRoute:
```

```
  Type: AWS::EC2::Route
```

```
  DependsOn: InternetGatewayAttachment
```

```
  Properties:
```

```
    RouteTableId: !Ref PublicRouteTable
```

```
    DestinationCidrBlock: 0.0.0.0/0
```

```
    GatewayId: !Ref InternetGateway
```

```
PublicSubnetARouteTableAssociation1:
```

```
  Type: AWS::EC2::SubnetRouteTableAssociation
```

```
  Properties:
```

```
    RouteTableId: !Ref PublicRouteTable
```

```
    SubnetId: !Ref PublicSubnetA
```

```
PublicSubnetBRouteTableAssociation2:
```

```
  Type: AWS::EC2::SubnetRouteTableAssociation
```

```
  Properties:
```

```
    RouteTableId: !Ref PublicRouteTable
```

```
    SubnetId: !Ref PublicSubnetB
```

```
#####
```

```
# SECURITY GROUPS
```

```
#####
```

```
VPCEndpointSecurityGroup:
```

```
  Type: 'AWS::EC2::SecurityGroup'
```

```
  Properties:
```

```
    GroupDescription: Allow TLS for VPC Endpoint
```

```
    VpcId: !Ref AppVPC
```

```
    SecurityGroupIngress:
```

```
- IpProtocol: tcp
  FromPort: 443
  ToPort: 443
  CidrIp: !GetAtt AppVPC.CidrBlock
```

```
#####
```

```
# VPC ENDPOINTS
```

```
#####
```

```
VPCEndpointGatewayS3:
```

```
  Type: 'AWS::EC2::VPCEndpoint'
```

```
  Properties:
```

```
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
```

```
    VpcEndpointType: Gateway
```

```
    VpcId: !Ref AppVPC
```

```
    RouteTableIds:
```

```
      - !Ref PrivateRouteTable
```

```
VPCEndpointInterfaceSignin:
```

```
  Type: 'AWS::EC2::VPCEndpoint'
```

```
  Properties:
```

```
    VpcEndpointType: Interface
```

```
    PrivateDnsEnabled: false
```

```
    SubnetIds:
```

```
      - !Ref PrivateSubnetA
```

```
      - !Ref PrivateSubnetB
```

```
    SecurityGroupIds:
```

```
      - !Ref VPCEndpointSecurityGroup
```

```
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
```

```
    VpcId: !Ref AppVPC
```

```
VPCEndpointInterfaceConsole:
```

```
  Type: 'AWS::EC2::VPCEndpoint'
```

```
  Properties:
```

```
    VpcEndpointType: Interface
```

```
    PrivateDnsEnabled: false
```

```
    SubnetIds:
```

```
      - !Ref PrivateSubnetA
```

```
      - !Ref PrivateSubnetB
```

```
    SecurityGroupIds:
```

```
      - !Ref VPCEndpointSecurityGroup
```

```
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
```

```
    VpcId: !Ref AppVPC
```

```
#####  
# ROUTE53 RESOURCES  
#####
```

ConsoleHostedZone:

Type: "AWS::Route53::HostedZone"

Properties:**HostedZoneConfig:**

Comment: 'Console VPC Endpoint Hosted Zone'

Name: 'console.aws.amazon.com'

VPCs:

-

VPCId: !Ref AppVPC

VPCRegion: !Ref "AWS::Region"

ConsoleRecordGlobal:

Type: AWS::Route53::RecordSet

Properties:

HostedZoneId: !Ref 'ConsoleHostedZone'

Name: 'console.aws.amazon.com'

AliasTarget:

DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]

HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]

Type: A

GlobalConsoleRecord:

Type: AWS::Route53::RecordSet

Properties:

HostedZoneId: !Ref 'ConsoleHostedZone'

Name: 'global.console.aws.amazon.com'

AliasTarget:

DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]

HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]

Type: A

ConsoleS3ProxyRecordGlobal:

Type: AWS::Route53::RecordSet

Properties:

HostedZoneId: !Ref 'ConsoleHostedZone'

Name: 's3.console.aws.amazon.com'

```
AliasTarget:
  DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
  HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
  Type: A

ConsoleSupportProxyRecordGlobal:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: "support.console.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

ExplorerProxyRecordGlobal:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: "resource-explorer.console.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

WidgetProxyRecord:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref "ConsoleHostedZone"
    Name: "*.widget.console.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ["1", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
      HostedZoneId: !Select ["0", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
      Type: A

ConsoleRecordRegional:
```

```
Type: AWS::Route53::RecordSet
Properties:
  HostedZoneId: !Ref 'ConsoleHostedZone'
  Name: !Sub "${AWS::Region}.console.aws.amazon.com"
  AliasTarget:
    DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
  Type: A

ConsoleRecordRegionalMultiSession:
Type: AWS::Route53::RecordSet
Properties:
  HostedZoneId: !Ref 'ConsoleHostedZone'
  Name: !Sub ".*${AWS::Region}.console.aws.amazon.com"
  AliasTarget:
    DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
  Type: A

SigninHostedZone:
Type: "AWS::Route53::HostedZone"
Properties:
  HostedZoneConfig:
    Comment: 'Signin VPC Endpoint Hosted Zone'
    Name: 'signin.aws.amazon.com'
  VPCs:
    -
      VPCId: !Ref AppVPC
      VPCRegion: !Ref "AWS::Region"

SigninRecordGlobal:
Type: AWS::Route53::RecordSet
Properties:
  HostedZoneId: !Ref 'SigninHostedZone'
  Name: 'signin.aws.amazon.com'
  AliasTarget:
    DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
    HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
```

Type: A

SigninRecordRegional:

Type: AWS::Route53::RecordSet

Properties:

HostedZoneId: !Ref 'SigninHostedZone'

Name: !Sub "\${AWS::Region}.signin.aws.amazon.com"

AliasTarget:

DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]

HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]

Type: A

#####

WORKSPACE RESOURCES

#####

ADAdminSecret:

Type: AWS::SecretsManager::Secret

Properties:

Name: !Ref DSAdminPasswordResourceName

Description: "Password for directory services admin"

GenerateSecretString:

SecretStringTemplate: '{"username": "Admin"}'

GenerateStringKey: password

PasswordLength: 30

ExcludeCharacters: '@/\'

WorkspaceSimpleDirectory:

Type: AWS::DirectoryService::SimpleAD

DependsOn: AppVPC

Properties:

Name: "corp.awsconsole.com"

Password: '{{resolve:secretsmanager:ADAdminSecret:SecretString:password}}'

Size: "Small"

VpcSettings:

SubnetIds:

- Ref: PrivateSubnetA

- Ref: PrivateSubnetB

VpcId:

Ref: AppVPC

Outputs:**PrivateSubnetA:**

Description: Private Subnet A

Value: !Ref PrivateSubnetA

PrivateSubnetB:

Description: Private Subnet B

Value: !Ref PrivateSubnetB

WorkspaceSimpleDirectory:


Description: Directory to be used for Workspaces

Value: !Ref WorkspaceSimpleDirectory

WorkspacesAdminPassword:

Description : "The ARN of the Workspaces admin's password. Navigate to the Secrets Manager in the AWS Console to view the value."

Value: !Ref ADAdminSecret

 **Note**

Questa configurazione test è progettata per essere eseguita nella regione Stati Uniti orientali (Virginia settentrionale) (us-east-1).

Configurazione di una rete

1. Accedere all'account di gestione dell'organizzazione e aprire la [console CloudFormation](#).
2. Seleziona Crea stack.
3. Scegliere Con nuove risorse (standard). Carica il file CloudFormation modello che hai creato in precedenza e scegli Avanti.
4. Inserire un nome per lo stack, ad esempio **PrivateConsoleNetworkForS3**, quindi scegliere Successivo.
5. Per VPC e sottoreti, inserire gli intervalli IP CIDR preferiti o utilizzare i valori predefiniti forniti. Se utilizzi i valori predefiniti, verifica che non si sovrappongano alle risorse VPC esistenti nel tuo Account AWS
6. Seleziona Crea stack.
7. Dopo aver creato lo stack, scegliere la scheda Risorse per visualizzare le risorse che sono state create.

- Scegliere la scheda Output per visualizzare i valori per le sottoreti private e la Workspace Simple Directory. Prendi nota di questi valori, poiché li utilizzerai nel passaggio quattro della prossima procedura per la creazione e la configurazione di un. WorkSpace

La schermata seguente mostra la visualizzazione della scheda Outputs che mostra i valori per le sottoreti private e per la Workspace Simple Directory.

The screenshot shows the AWS CloudFormation console interface for a stack named "PrivateConsoleNetworkForS3". The "Outputs" tab is selected, displaying a table of stack outputs. The table has columns for Key, Value, Description, and Export name. There are four outputs listed:

Key	Value	Description	Export name
PrivateSubnetA	subnet-0aea1291fe9eb1b47	Private Subnet A	-
PrivateSubnetB	subnet-04f6adc31f08a09b6	Private Subnet B	-
WorkspacesAdminPassword	arn:aws:secretsmanager:us-east-1:851725487077:secret:ADAdminSecret-GAwM8i	The ARN of the Workspaces admin's password. Navigate to the Secrets Manager in the AWS Console to view the value.	-
WorkspaceSimpleDirectory	d-9067f40091	Directory to be used for Workspaces	-

Dopo aver creato la rete, utilizzate le seguenti procedure per creare e accedere a un WorkSpace.

Per creare un WorkSpace

- Apri la [WorkSpaces console](#).
- Nel riquadro di navigazione, seleziona Directory.
- Nella pagina Directory, verificare che lo stato della directory sia Attivo. La schermata seguente mostra una pagina Directory con una directory attiva.

Directory ID	Workspace Type	Directory name	Organization n...	Identity source	Status
d-9067f40091	Personal	corp.awsconsole.com	d-9067f40091	AWS Directory Service	Registered

4. Per utilizzare una cartella in WorkSpaces, è necessario registrarla. Nel riquadro di navigazione, scegli WorkSpaces, quindi scegli Crea WorkSpaces.
5. In Seleziona una directory, scegliere la directory creata da CloudFormation nella procedura precedente. Dal menu Operazioni scegliere Registra.
6. Per la selezione delle sottoreti, selezionare le due sottoreti annotate nella fase nove della procedura precedente.
7. Selezionare Abilita le autorizzazioni self-service, quindi scegliere Registra.
8. Dopo aver registrato la directory, continua a creare il WorkSpace. Selezionare la directory registrata, quindi scegliere Successivo.
9. Nella pagina Crea utenti, scegliere Crea utente aggiuntivo. Inserisci il tuo nome e la tua email per consentirti di utilizzare il WorkSpace. Verifica che l'indirizzo e-mail sia valido poiché le informazioni di WorkSpace accesso vengono inviate a questo indirizzo e-mail.
10. Scegli Next (Successivo).
11. Nella pagina Identifica utenti, selezionare l'utente creato nella fase nove, quindi scegliere Successivo.
12. Nella pagina Seleziona bundle, scegliere Standard con Amazon Linux 2, quindi scegliere Successivo.
13. Usare le impostazioni predefinite per la modalità di esecuzione e la personalizzazione dell'utente e scegliere Crea Workspace. Lo Pending stato WorkSpace inizia e passa a quello successivo Available entro circa 20 minuti.
14. Quando sarà WorkSpace disponibile, riceverai un'e-mail con le istruzioni per accedervi all'indirizzo e-mail fornito nel passaggio nove.

Dopo aver effettuato l'accesso al tuo WorkSpace, puoi verificare di accedervi utilizzando il tuo accesso Console di gestione AWS privato.

Per accedere a WorkSpace

1. Aprire l'e-mail ricevuta nella fase 14 della procedura precedente.

2. Nell'e-mail, scegli il link univoco fornito per configurare il tuo profilo e scaricare il WorkSpaces client.
3. Impostazione della password.
4. Scaricare il client preferito.
5. Installare e avviare il client. Inserire il codice di registrazione fornito nell'e-mail, quindi scegliere Registra.
6. Accedi ad Amazon WorkSpaces utilizzando le credenziali che hai creato nella fase tre.

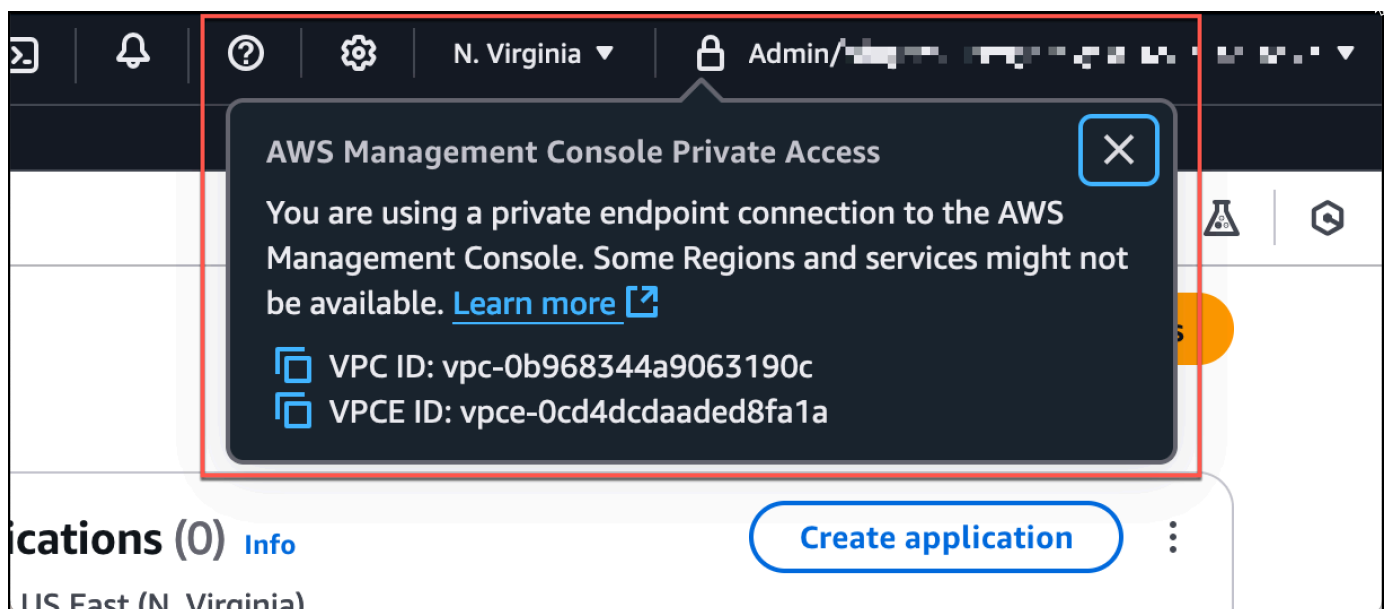
Per testare la configurazione di Console di gestione AWS Private Access

1. Dal tuo Workspace, apri il browser. Quindi, vai alla [Console di gestione AWS](#) e accedi utilizzando le tue credenziali.

Note

Se utilizzi Firefox come browser, verifica che l'opzione Abilita DNS su HTTPS sia disattivata nelle impostazioni del browser.

2. Apri la [console Amazon S3](#) dove puoi verificare di essere connesso tramite Console di gestione AWS Private Access.
3. Scegli l'icona di blocco privato nella barra di navigazione per visualizzare il VPC e l'endpoint VPC in uso. La schermata seguente mostra la posizione dell'icona di blocco privato e le informazioni sul VPC.



Test della configurazione VPC con le policy IAM

Puoi testare ulteriormente il tuo VPC che hai configurato con Amazon EC2 WorkSpaces o implementando policy IAM che limitano l'accesso.

La policy seguente nega l'accesso ad Amazon S3 a meno che non si utilizzi il VPC specificato.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "S3:*",
      "Resource": "*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "aws:SourceVpc": "vpc-12345678"
        },
        "Bool": {
          "aws:ViaAwsService": "false"
        }
      }
    }
  ]
}
```

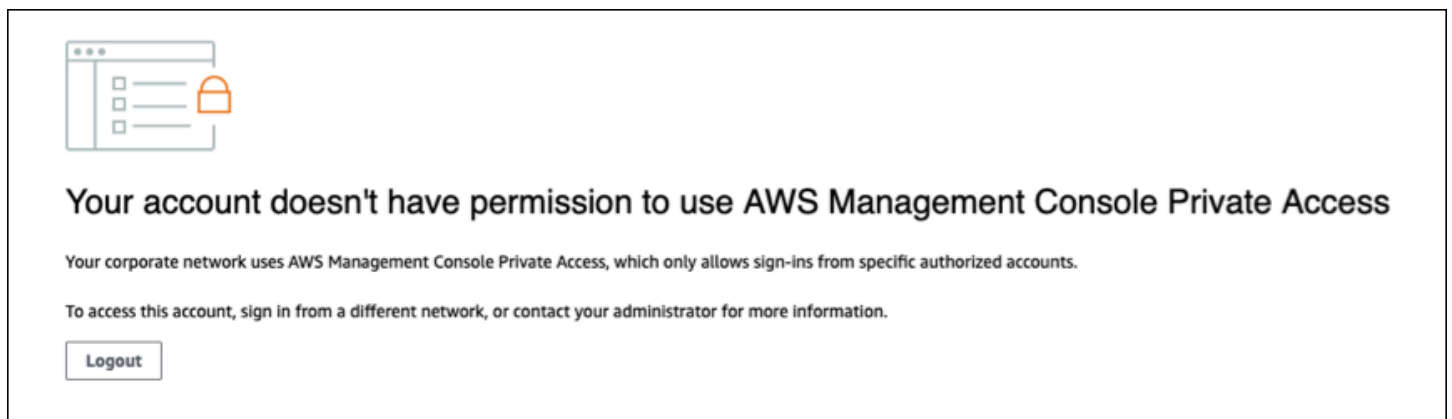
La seguente policy limita l'accesso a determinati utenti Account AWS IDs utilizzando una policy di accesso Console di gestione AWS privato per l'endpoint di accesso.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
```

```
"Resource": "*",
"Condition": {
  "StringEquals": {
    "aws:PrincipalAccount": [
      "AWSAccountID"
    ]
  }
}
```

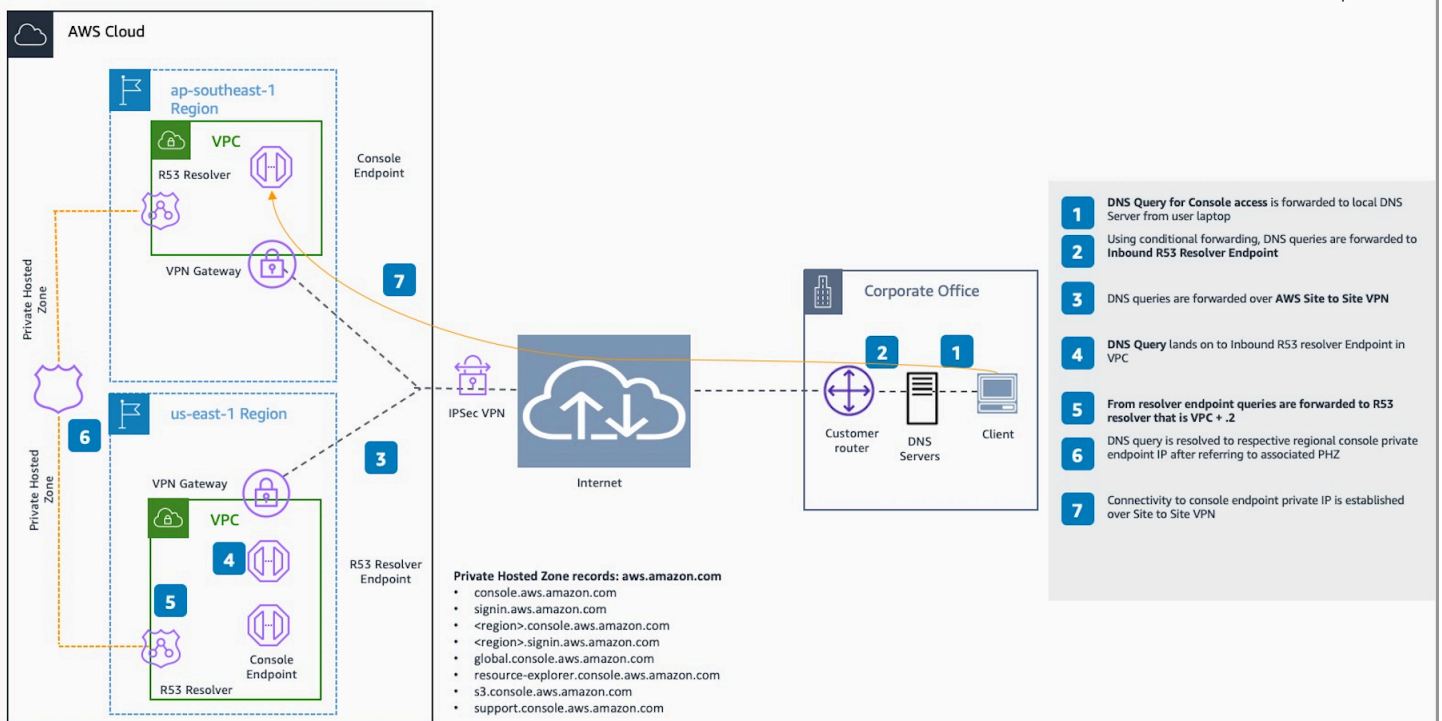
Se ci si connette con un'identità che non appartiene al proprio account, viene visualizzata la seguente pagina di errore.



Architettura di riferimento

Per connetterti privatamente a Console di gestione AWS Private Access da una rete locale, puoi sfruttare l'opzione di connessione AWS Site-to-Site VPN a AWS Virtual Private Gateway (VGW). AWS Site-to-Site VPN consente l'accesso alla rete remota dal VPC creando una connessione e configurando il routing per far passare il traffico attraverso la connessione. Per ulteriori informazioni, consulta [Cos'è la AWS VPN da sito a sito nella Guida per l'utente](#) della VPN. AWS Site-to-Site AWS Virtual Private Gateway (VGW) è un servizio regionale ad alta disponibilità che funge da gateway tra un VPC e la rete locale.

AWS Site-to-Site VPN a AWS Virtual Private Gateway (VGW)



Un componente essenziale in questo progetto di architettura di riferimento è, in particolare Amazon Route 53 Resolver, il resolver in entrata. Quando lo configuri nel VPC in cui vengono creati gli endpoint di accesso Console di gestione AWS privato, gli endpoint resolver (interfacce di rete) vengono creati nelle sottoreti specificate. I loro indirizzi IP possono quindi essere indicati in server di inoltro condizionali sui server DNS on-premise, per consentire le query dei record in una zona ospitata privata. Quando i client locali si connettono a, vengono indirizzati ai dispositivi Private Access privati degli endpoint Console di gestione AWS Private Access. Console di gestione AWS IPs

Prima di configurare la connessione all'endpoint di accesso Console di gestione AWS privato, completa i passaggi relativi ai prerequisiti per configurare gli endpoint di accesso Console di gestione AWS privato in tutte le regioni in cui desideri accedere e nella Console di gestione AWS regione Stati Uniti orientali (Virginia settentrionale) e configurare la zona ospitata privata.

AWS Personalizzazione dell'esperienza utente (UXC)

AWS La personalizzazione dell'esperienza utente consente di personalizzare le AWS interfacce per soddisfare esigenze specifiche e migliorare l'efficienza. UXC offre attualmente una funzione di personalizzazione del colore degli account per gli amministratori degli account. Questa funzionalità consente agli amministratori di impostare un colore per un account in base al raggruppamento richiesto. Ad esempio, un amministratore può assegnare il rosso a tutti gli account di produzione, il giallo a tutti gli account di test e il verde a tutti gli account sviluppatore. I vantaggi della personalizzazione del colore dell'account includono:

- Identifica rapidamente e visivamente i tipi di account
- Riduzione del rischio di modifiche agli account errati
- Raggruppa account simili (produzione, test, sviluppo)

Accesso alla personalizzazione dell'esperienza utente

Puoi accedere a UXC dalla pagina del tuo account in Console di gestione AWS Per ulteriori informazioni sull'accesso a questa pagina, vedere. [???](#)

Guida introduttiva alla personalizzazione AWS dell'esperienza utente

Gli amministratori possono impostare i colori per diversi AWS account. I colori degli account facilitano la distinzione tra gli account a cui hai attualmente effettuato l'accesso. Le organizzazioni possono utilizzare il colore degli account per distinguere tra diversi tipi di account, ad esempio, è possibile utilizzare il verde per gli account di sviluppo, il giallo per gli account di test e il rosso per gli account di produzione.

Note

Le funzionalità essenziali per Console di gestione AWS, come la personalizzazione AWS dell'esperienza utente e Amazon Q AWS CloudShell, richiedono autorizzazioni IAM appropriate. AWS le politiche gestite forniscono un modo conveniente per concedere queste autorizzazioni agli utenti e ai ruoli utilizzati all'interno di Console di gestione AWS Le seguenti politiche gestite sono disponibili per l'uso:

- `AWSManagementConsoleBasicUserAccess`
 - Per utenti non amministrativi
 - Fornisce l'accesso alle funzionalità di base della console
- `AWSManagementConsoleAdministratorAccess`
 - Per utenti amministrativi
 - Fornisce l'accesso a Console di gestione AWS funzionalità essenziali
 - Consente agli amministratori di configurarli e personalizzarli Console di gestione AWS per altre identità

Per ulteriori informazioni, consulta [???](#).

Per impostare il colore di un account

1. Accedi alla [Console di gestione AWS](#).
2. Nella barra di navigazione, scegli il nome dell'account.
3. Scegli Account.
4. Nelle impostazioni di visualizzazione dell'account, scegli un colore.
5. Scegliere Aggiorna.

Documentazione di riferimento delle API

Lo AWS User Experience Customization API Reference fornisce descrizioni, parametri di richiesta API e la risposta JSON per ciascuna delle azioni dell'API di personalizzazione AWS dell'esperienza utente.

Argomenti

- [Azioni](#)
- [Errori comuni](#)

Azioni

Sono supportate le operazioni seguenti:

- [???](#)
- [???](#)
- [???](#)

GetAccountColor

Ottiene il colore associato all'account.

Sintassi della richiesta

```
GET /v1/account-color HTTP/1.1
```

La richiesta non utilizza parametri URI né include un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
  "color": "string"
}
```

Elementi di risposta

color

Il colore associato all'account.

Tipo: String

Valori validi: nessuno | rosa | viola | blu scuro | blu chiaro | verde | giallo | arancione | rosso

Errori

Per informazioni sugli errori comuni a tutte le azioni, consulta Errori comuni.

AccessDeniedException

L'utente non dispone di accesso sufficiente per eseguire questa azione.

Codice di stato HTTP: 403

InternalServerError

Errore imprevisto durante l'elaborazione della richiesta.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Questa eccezione viene generata quando la convalida dell'evento di notifica non supera.

Codice di stato HTTP: 400

DeleteAccountColor

Elimina l'impostazione del colore dell'account.

Sintassi della richiesta

```
DELETE /v1/account-color HTTP/1.1
```

Parametri della richiesta

Questa operazione non utilizza parametri richiesta.

Corpo della richiesta

Questa operazione non ha un corpo della richiesta.

Corpo della risposta

Questa operazione non restituisce un corpo della risposta.

Errori

Per informazioni sugli errori comuni a tutte le azioni, consulta [Errori comuni](#).

AccessDeniedException

L'utente non dispone di accesso sufficiente per eseguire questa azione.

Codice di stato HTTP: 403

InternalServerError

Errore imprevisto durante l'elaborazione della richiesta.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Questa eccezione viene generata quando la convalida dell'evento di notifica non supera.

Codice di stato HTTP: 400

PutAccountColor

Imposta il colore associato a un account.

Sintassi della richiesta

```
PUT /v1/account-color HTTP/1.1
```

Corpo della richiesta

```
Content-type: application/json
```

```
{  
  "color": "string"  
}
```

Sintassi della risposta

```
HTTP/1.1 200
```

```
Content-type: application/json
```

```
{  
  "color": "string"  
}
```

Elementi di risposta

color

Il colore associato all'account.

Tipo: String

Valori validi: nessuno | rosa | viola | blu scuro | blu chiaro | verde | giallo | arancione | rosso

Errori

Per informazioni sugli errori comuni a tutte le azioni, consulta [Errori comuni](#).

AccessDeniedException

L'utente non dispone di accesso sufficiente per eseguire questa azione.

Codice di stato HTTP: 403

InternalServerError

Errore imprevisto durante l'elaborazione della richiesta.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata rifiutata a causa della limitazione della richiesta.

Codice di stato HTTP: 429

ValidationException

Questa eccezione viene generata quando la convalida dell'evento di notifica non supera.

Codice di stato HTTP: 400

Errori comuni

I seguenti errori sono comuni alle azioni API di tutti i AWS servizi. Per gli errori specifici di un'azione API, consulta la documentazione relativa all'azione.

AccessDeniedException

Non hai accesso sufficiente per eseguire questa azione.

Codice di stato HTTP: 403

Per ulteriori informazioni, consulta [Risoluzione degli errori di accesso negato](#).

ExpiredTokenException

Il token di sicurezza incluso nella richiesta è scaduto.

Codice di stato HTTP: 403

IncompleteSignature

La firma della richiesta non è conforme agli AWS standard.

Codice di stato HTTP: 403

InternalFailure

L'elaborazione della richiesta non è riuscita a causa di un errore, un'eccezione o un guasto interno sconosciuto.

Codice di stato HTTP: 500

MalformedHttpRequestException

Ci sono problemi con la richiesta a livello HTTP. Ad esempio, non possiamo decomprimere il corpo in base all'algoritmo di decompressione specificato dalla codifica del contenuto.

Codice di stato HTTP: 400

NotAuthorized

Non sei autorizzato a eseguire questa azione.

Codice di stato HTTP: 401

OptInRequired

L'ID della chiave di AWS accesso richiede un abbonamento al servizio.

Codice di stato HTTP: 403

RequestAbortedException

La richiesta è stata interrotta prima dell'invio di una risposta (ad esempio, il client ha chiuso la connessione).

Codice di stato HTTP: 400

RequestEntityTooLargeException

Ci sono problemi con la richiesta a livello HTTP. L'entità della richiesta è troppo grande.

Codice di stato HTTP: 413

RequestExpired

La richiesta ha raggiunto il servizio più di 15 minuti dopo la data indicata sulla richiesta o più di 15 minuti dopo la data di scadenza della richiesta (ad esempio nel caso di pre-firmata URLs), oppure la data indicata sulla richiesta è tra più di 15 minuti.

Codice di stato HTTP: 400

RequestTimeoutException

Ci sono problemi con la richiesta a livello HTTP. È scaduto il tempo di lettura della richiesta.

Codice di stato HTTP: 408

ServiceUnavailable

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 503

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

UnrecognizedClientException

Il certificato X.509 o AWS l'ID della chiave di accesso fornito non esiste nei nostri archivi.

Codice di stato HTTP: 403

UnknownOperationException

L'azione o l'operazione richiesta non è valida. Verifica che l'operazione sia digitata correttamente.

Codice di stato HTTP: 404

ValidationError

L'input non soddisfa i vincoli specificati da un AWS servizio.

Codice di stato HTTP: 400

Registrazione delle chiamate AWS all'API di personalizzazione dell'esperienza utente utilizzando AWS CloudTrail

AWS La personalizzazione dell'esperienza utente è integrata con [AWS CloudTrail](#), un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o un. Servizio AWS CloudTrail acquisisce tutte le chiamate API per UXC come eventi. Le chiamate acquisite includono chiamate dalla console UXC e chiamate di codice alle operazioni dell'API UXC. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta che è stata effettuata a UXC, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e ulteriori dettagli.

CloudTrail è attivo nel tuo account Account AWS quando crei l'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione registrati in un. Regione AWS Per ulteriori informazioni, consulta [Lavorare con la cronologia degli CloudTrail eventi](#) nella Guida per l'utente.AWS CloudTrail Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Per una registrazione continua degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi [CloudTrailLake](#).

Eventi di gestione UXC in CloudTrail

[Gli eventi di gestione](#) forniscono informazioni sulle operazioni di gestione eseguite sulle risorse dell'ambiente. Account AWS Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

AWS User Experience Customization registra tutte le operazioni del piano di controllo UXC come eventi di gestione. [Per un elenco delle operazioni del piano di controllo AWS User Experience](#)

[Customization a cui UXC accede CloudTrail, consulta lo User Experience Customization API Reference.AWS](#)

Esempi di eventi UXC

Un evento rappresenta una singola richiesta proveniente 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.

L'esempio seguente mostra un CloudTrail evento che dimostra l'operazione.

```
{
  "eventVersion" : "1.09",
  "userIdentity" : {
    "type" : "AssumedRole",
    "principalId" : "AIDACKCEVSQ6C2EXAMPLE:jdoe",
    "arn" : "arn:aws:sts::111122223333:assumed-role/user/jdoe",
    "accountId" : "111122223333",
    "accessKeyId" : "AKIAIOSFODNN7EXAMPLE",
    "sessionContext" : {
      "sessionIssuer" : {
        "type" : "Role",
        "principalId" : "AIDACKCEVSQ6C2EXAMPLE",
        "arn" : "arn:aws:iam::111122223333:role/user",
        "accountId" : "111122223333",
        "userName" : "jdoe"
      },
      "webIdFederationData" : { },
      "attributes" : {
        "creationDate" : "2022-12-09T23:48:51Z",
        "mfaAuthenticated" : "false"
      }
    }
  },
  "eventTime" : "2022-12-09T23:50:03Z",
  "eventSource" : "uxc.amazonaws.com",
  "eventName" : "GetAccountColor",
  "awsRegion" : "us-east-2",
  "sourceIPAddress" : "10.24.34.3",
  "userAgent" : "PostmanRuntime/7.43.4",
  "requestParameters" : null,
  "responseElements" : null,
```

```
"requestID" : "543db7ab-b4b2-11e9-8925-d139e92a1fe8",  
"eventID" : "5b2805a5-3e06-4437-a7a2-b5fdb5cbb4e2",  
"readOnly" : true,  
"eventType" : "AwsApiCall",  
"managementEvent" : true,  
"recipientAccountId" : "111122223333",  
"eventCategory" : "Management"  
}
```

Per informazioni sul contenuto dei CloudTrail record, consultate il [contenuto dei CloudTrail record](#) nella Guida per l'AWS CloudTrail utente.

AWS politiche gestite per Console di gestione AWS

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. Le politiche 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 le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. È più probabile che aggiorni una policy AWS gestita quando nel Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

AWS politica gestita: AWSManagementConsoleBasicUserAccess

È possibile associare la policy `AWSManagementConsoleBasicUserAccess` a utenti, gruppi e ruoli.

Questa politica concede le autorizzazioni necessarie per gli utenti non amministrativi di Console di gestione AWS. Ciò include funzionalità come l'individuazione delle risorse, le notifiche, l'accesso alla shell basato sul browser e la navigazione personalizzata.

Dettagli delle autorizzazioni

Queste `AWSManagementConsoleBasicUserAccess` sono raggruppate nei seguenti set di autorizzazioni:

- `cloudshell`— Consente ai principali l'accesso completo alle AWS CloudShell funzionalità, tra cui la creazione dell'ambiente, la gestione delle sessioni e l'esecuzione dei comandi.

- `ec2`— Consente ai mandanti di descrivere le regioni abilitate per l'account in [Unified Navigation](#).
- `notifications`— Consente ai presidi di ottenere eventi da. Notifiche all'utente AWS
- `q`— Consente ai presidi di chattare con Amazon Q Developer.
- `resource-explorer-2`— Consente ai dirigenti di cercare e scoprire AWS risorse utilizzando [Unified Search](#).
- `uxc`— Consente ai dirigenti di leggere le impostazioni di personalizzazione AWS dell'esperienza utente.
- `action-recommendations`— Consente ai presidi di ricevere consigli contestuali sulle azioni da intraprendere.
- `account`— Consente ai responsabili di recuperare informazioni sull'account specificato, inclusi il nome dell'account, l'ID dell'account e la data e l'ora di creazione dell'account.

Per vedere le autorizzazioni per questa policy, consulta [AWSManagementConsoleBasicUserAccess](#) nella Guida di riferimento sulle policy gestite da AWS .

AWS politica gestita: AWSManagementConsoleAdministratorAccess

È possibile associare la policy `AWSManagementConsoleAdministratorAccess` a utenti, gruppi e ruoli.

Questa politica garantisce l'accesso completo alla configurazione e alla personalizzazione di Console di gestione AWS. Consente agli amministratori di impostare i colori degli account, abilitare le notifiche agli utenti e configurare l'individuazione delle risorse. Include anche le autorizzazioni derivanti dalla politica `AWSManagementConsoleBasicUserAccess` gestita, essenziali per gli utenti non amministrativi di Console di gestione AWS

Dettagli delle autorizzazioni

Queste `AWSManagementConsoleAdministratorAccess` sono raggruppate nei seguenti set di autorizzazioni:

- `cloudshell`— Consente ai principali l'accesso completo alle AWS CloudShell funzionalità, tra cui la creazione dell'ambiente, la gestione delle sessioni e l'esecuzione dei comandi.
- `ec2`— Consente ai mandanti di descrivere le regioni abilitate per l'account in [Unified](#) Navigation.
- `notifications`— Consente ai responsabili di accedere e aggiornare le configurazioni delle notifiche, gli eventi e lo stato di attivazione delle funzionalità.
- `q`— Consente ai responsabili di chattare con Amazon Q Developer per il supporto assistito dall'intelligenza artificiale.
- `resource-explorer-2`— [Consente ai dirigenti di cercare e scoprire AWS risorse utilizzando Unified Search.](#)
- `uxc`— Consente ai responsabili l'accesso completo alle impostazioni di personalizzazione AWS dell'esperienza utente.
- `action-recommendations`— Consente ai presidi di ricevere consigli contestuali sulle azioni da intraprendere.
- `account`— Consente ai responsabili di recuperare informazioni sull'account specificato, inclusi il nome dell'account, l'ID dell'account e la data e l'ora di creazione dell'account.

Per vedere le autorizzazioni per questa policy, consulta

[AWSManagementConsoleAdministratorAccess](#) nella Guida di riferimento sulle policy gestite da AWS

Console di gestione AWS aggiornamenti alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite Console di gestione AWS da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei Console di gestione AWS documenti.

Modifica	Descrizione	Data
AWSManagementConso leBasicUserAccess — Politica aggiornata	Politica aggiornata per aggiungere autorizzazioni per consentire agli utenti di visualizzare le informazi	9 dicembre 2025

Modifica	Descrizione	Data
	oni sull'account e ricevere consigli sulle azioni durante la navigazione nel. Console di gestione AWS	
AWSManagementConso leAdministratorAccess — Politica aggiornata	Politica aggiornata per aggiungere autorizzazioni per consentire agli utenti di visualizzare le informazioni sull'account e ricevere consigli sulle azioni durante la navigazione nel. Console di gestione AWS	9 dicembre 2025
AWSManagementConso leBasicUserAccess : nuova policy	È stata aggiunta una nuova politica AWS gestita che concede le autorizzazioni necessarie per la Console di gestione AWS navigazione di base, la visualizzazione dei colori dell'account e l'individuazione delle risorse.	14 agosto 2025
AWSManagementConso leAdministratorAccess : nuova policy	È stata aggiunta una nuova politica AWS gestita che fornisce l'accesso completo per configurare e personalizzare. Console di gestione AWS	14 agosto 2025
Console di gestione AWS ha iniziato a tenere traccia delle modifiche	Console di gestione AWS ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	14 agosto 2025

Utilizzo di Markdown nella console

Alcuni servizi Console di gestione AWS, come Amazon CloudWatch, supportano l'uso di [Markdown](#) in determinati campi. Questo argomento spiega i tipi di formattazione Markdown supportati nella console.

Indice

- [Paragrafi, Interlinea e Linee orizzontali](#)
- [Intestazioni](#)
- [Formattazione del testo](#)
- [Link](#)
- [Elenchi](#)
- [Tabelle e pulsanti \(CloudWatch dashboard\)](#)

Paragrafi, Interlinea e Linee orizzontali

I paragrafi sono separati da una riga vuota. Per assicurarsi che la riga vuota tra i paragrafi venga visualizzata quando viene convertita in HTML, aggiungere una nuova riga con uno spazio unificatore () e una riga vuota. Ripetere questa coppia di righe per inserire più righe vuote una dopo l'altra, come nell'esempio seguente:

```
&nbsp;
&nbsp;
```

Per creare una regola orizzontale che separa i paragrafi, aggiungere una nuova riga con tre trattini in una riga: ---

```
Previous paragraph.
---
Next paragraph.
```

Per creare un blocco di testo con testo a spaziatura fissa, aggiungere una riga con tre virgolette (`). Inserire il testo da visualizzare nel testo a spaziatura fissa. Quindi, aggiungere un'altra nuova riga

con tre apici inversi. L'esempio seguente mostra il testo che verrà formattato come testo a spaziatura fissa quando viene visualizzato:

```
```\nThis appears in a text box with a background shading.\nThe text is in monospace.\n```
```

## Intestazioni

Per creare intestazioni, usa il cancelletto (#). Un solo cancelletto e uno spazio indicano un'intestazione di livello principale. Due cancelletti creano un'intestazione di secondo livello e tre cancelletti creano un'intestazione di terzo livello. Gli esempi seguenti mostrano un'intestazione di livello principale, di secondo livello e di terzo livello:

```
Top-level heading
```

```
Second-level heading
```

```
Third-level heading
```

## Formattazione del testo

Per formattare il testo come corsivo, farlo precedere e seguire da un solo carattere di sottolineatura ( \_ ) o da un asterisco (\*).

```
This text appears in italics.
```

Per formattare il testo come grassetto, farlo precedere e seguire da due trattini bassi o da due asterischi per lato.

```
This text appears in bold.
```

Per formattare il testo come barrato, farlo precedere e seguire da due tilde per lato (~).

```
~~This text appears in strikethrough.~~
```

## Link

Per aggiungere un collegamento ipertestuale di testo, inserire il testo del collegamento tra parentesi quadre ([ ]), seguito dall'URL completo tra parentesi (( )), come nel seguente esempio:

```
Choose [link_text](http://my.example.com).
```

## Elenchi

Per formattare righe come parte di un elenco puntato, aggiungerle su righe separate che iniziano con un singolo asterisco (\*) e quindi uno spazio, come nell'esempio seguente:

```
Here is a bulleted list:
* Ant
* Bug
* Caterpillar
```

Per formattare righe come parte di un elenco numerato, aggiungerle su righe separate che iniziano con un numero, un punto (.) e uno spazio, come nell'esempio seguente:

```
Here is a numbered list:
1. Do the first step
2. Do the next step
3. Do the final step
```

## Tabelle e pulsanti (CloudWatch dashboard)

CloudWatch i widget di testo delle dashboard supportano le tabelle e i pulsanti Markdown.

Per creare una tabella, separare le colonne con le barre verticali (|) e le righe utilizzando nuove linee. Per rendere la prima riga una riga di intestazione, inserire una riga tra la riga di intestazione e la prima riga di valori. Quindi aggiungere almeno tre trattini (-) per ogni colonna nella tabella. Separazione delle colonne mediante barre verticali. L'esempio seguente mostra il Markdown per una tabella con due colonne, una riga di intestazione e due righe di dati:

```
Table | Header
----|-----
Amazon Web Services | AWS
```

1 | 2

Il testo Markdown dell'esempio precedente crea la tabella seguente:

Tabella	Header
Amazon Web Services	AWS
1	2

In un widget di testo della CloudWatch dashboard, puoi anche formattare un collegamento ipertestuale in modo che appaia come pulsante. Per creare un pulsante, usa `[button:Button text]`, seguito dall'URL completo tra parentesi (( )), come nel seguente esempio:

```
[button:Go to AWS](http://my.example.com)
[button:primary:This button stands out even more](http://my.example.com)
```

# Risoluzione dei problemi

Consulta questa sezione per trovare soluzioni ai problemi più comuni con Console di gestione AWS.

Puoi anche diagnosticare e risolvere gli errori più comuni per alcuni servizi AWS utilizzando Amazon Q Developer. Per ulteriori informazioni, consulta [Diagnosticare gli errori comuni nella console con Amazon Q Developer](#) nella Amazon Q Developer User Guide.

## Argomenti

- [La pagina non si sta caricando correttamente](#)
- [Il mio browser visualizza un errore di «accesso negato» durante la connessione al Console di gestione AWS](#)
- [Il mio browser mostra errori di timeout durante la connessione a Console di gestione AWS](#)
- [Vorrei cambiare la lingua di Console di gestione AWS ma non riesco a trovare il menu di selezione della lingua in fondo alla pagina](#)

## La pagina non si sta caricando correttamente

- Se questo problema si verifica solo occasionalmente, controlla la tua connessione Internet. Prova a connetterti tramite una rete diversa, con o senza una VPN, oppure prova a utilizzare un browser Web diverso.
- Se tutti gli utenti interessati fanno parte dello stesso team, potrebbe trattarsi di un'estensione del browser per la privacy o di un problema con il firewall di sicurezza. Le estensioni del browser per la privacy e i firewall di sicurezza possono bloccare l'accesso ai domini utilizzati da Console di gestione AWS. Prova a disattivare queste estensioni o a modificare le impostazioni del firewall. Per verificare i problemi di connessione, apri gli strumenti di sviluppo del browser ([Chrome](#), [Firefox](#)) e controlla gli errori nella scheda Console. Console di gestione AWS Utilizza i suffissi dei domini, incluso il seguente elenco. L'elenco non è completo e può essere modificato nel corso del tempo. I suffissi di questi domini non vengono utilizzati esclusivamente da AWS.
  - .a2z.com
  - .amazon.com
  - .amazonaws.com
  - .aws
  - .aws.com

- .aws.dev
- .awscloud.com
- .awsplayer.com
- .awsstatic.com
- .cloudfront.net
- .live-video.net

#### Warning

Dal 31 luglio 2022, AWS non supporta più Internet Explorer 11. Ti consigliamo di utilizzarlo Console di gestione AWS con altri browser supportati. Per ulteriori informazioni, consulta il [News Blog AWS](#).

## Il mio browser visualizza un errore di «accesso negato» durante la connessione al Console di gestione AWS

Le modifiche recenti apportate alla console potrebbero influire sull'accesso se vengono soddisfatte tutte le seguenti condizioni:

- Si accede Console di gestione AWS da una rete configurata per raggiungere gli endpoint AWS del servizio tramite endpoint VPC.
- Puoi limitare l'accesso ai AWS servizi utilizzando `aws:SourceIp` la chiave di condizione `aws:SourceVpc` globale nelle tue policy IAM.

Ti consigliamo di esaminare le politiche IAM che contengono la chiave di condizione `aws:SourceIp` o `aws:SourceVpc` globale. Applicate entrambe `aws:SourceIp` e `aws:SourceVpc` dove applicabile.

Alcune Console di gestione AWS funzionalità utilizzano domini dual-stack che supportano sia le connessioni che le connessioni. IPv4 IPv6 Se la tua policy IAM limita l'accesso utilizzando `aws:SourceIp` solo blocchi IPv4 CIDR, le richieste potrebbero fallire quando il sistema operativo preferisce IPv6 le connessioni (o viceversa). Per evitare che ciò accada, includi entrambi IPv4 i blocchi IPv6 CIDR nelle tue condizioni. `aws:SourceIp` Per ulteriori informazioni, consulta [aws:SourceIp](#) nella Guida per l'AWS Identity and Access Management utente.

Puoi anche utilizzare la funzionalità di accesso Console di gestione AWS privato per accedere Console di gestione AWS tramite un endpoint VPC e `aws:SourceVpc` utilizzare le condizioni nelle tue politiche. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Console di gestione AWS Accesso privato](#)
- [the section called “Come funziona Console di gestione AWS Private Access con aws: SourceVpc”](#)
- [the section called “Chiavi contestuali delle condizioni AWS globali supportate”](#)

## Il mio browser mostra errori di timeout durante la connessione a Console di gestione AWS

Se si verifica un'interruzione del servizio come impostazione predefinita Regione AWS, il browser potrebbe visualizzare un errore 504 Gateway Timeout quando si tenta di connettersi a Console di gestione AWS. Per accedere Console di gestione AWS da una regione diversa, specifica un endpoint regionale alternativo nell'URL. Ad esempio, se c'è un'interruzione nella Regione `us-west-1` (California settentrionale), per accedere alla Regione `us-west-2` (Oregon) utilizza il seguente modello:

```
https://region.console.aws.amazon.com
```

Per ulteriori informazioni, consulta [Console di gestione AWS service endpoints](#) (Endpoint del servizio della console) nei Riferimenti generali di AWS.

Per visualizzare lo stato di tutti Servizi AWS, incluso il Console di gestione AWS, vedi [Dashboard AWS Health](#)

## Vorrei cambiare la lingua di Console di gestione AWS ma non riesco a trovare il menu di selezione della lingua in fondo alla pagina

Il menu di selezione delle lingue è stato spostato nella nuova pagina delle Impostazioni unificate. Per cambiare la lingua di Console di gestione AWS, [vai alla pagina Impostazioni unificate](#), quindi scegli la lingua per la console.

Per ulteriori informazioni, consulta [Modifica della lingua della Console di gestione AWS](#).

# Cronologia dei documenti

Nella tabella seguente sono descritte le modifiche importanti apportate alla Guida alle operazioni di base della Console di gestione AWS , a partire da marzo 2021.

Modifica	Descrizione	Data
Pagina aggiunta	Nuova pagina aggiunta per spiegare le azioni consigliate. Per ulteriori informazioni, consulta <a href="#">???</a> .	15 ottobre 2025
Nuove politiche AWS gestite	Sono state aggiunte due nuove politiche per l'ambito delle autorizzazioni per l'utilizzo, la configurazione e la personalizzazione di. Console di gestione AWS <ul style="list-style-type: none"><li>• <a href="#">AWSManagementConsoleBasicUserAccess</a></li><li>• <a href="#">AWSManagementConsoleAdministratorAccess</a></li></ul>	14 agosto 2025
<a href="#">Personalizzazioni dell'esperienza utente (UXC)</a>	Nuovo servizio disponibile.	14 agosto 2025
Pagina aggiornata	Ora puoi visualizzare le tue applicazioni in MyApplications dal menu Servizi. Per ulteriori informazioni, consulta <a href="#">???</a> .	29 luglio 2025
Pagina aggiunta	Nuova pagina aggiunta per spiegare la funzionalità multisesione. Per ulteriori informazioni, consulta <a href="#">???</a> .	6 dicembre 2024

Modifica	Descrizione	Data
Pagina aggiornata	Modifica della pagina della password aggiornata. Per ulteriori informazioni, consulta <a href="#">???</a> .	18 giugno 2024
Nuove pagine aggiunte	Nuove pagine aggiunte per descrivere come accedere al menu Servizi e alle notifiche AWS degli eventi. Per ulteriori informazioni, consultare <a href="#">???</a> e <a href="#">???</a> .	18 giugno 2024
Pagina aggiornata	Che cos'è il Console di gestione AWS? pagina aggiornata. Per ulteriori informazioni, consulta <a href="#">???</a> .	18 giugno 2024
Richiedi assistenza	È stata aggiunta una nuova pagina per descrivere come ottenere assistenza. Per ulteriori informazioni, consulta <a href="#">???</a> .	18 giugno 2024
Navigazione unificata e AWS Console Home	Nuove pagine aggiunte per descrivere come utilizzare la console. Per ulteriori informazioni, consultare <a href="#">???</a> e <a href="#">???</a> .	18 giugno 2024
Chatta con Amazon Q	Una nuova pagina di impostazioni che spiega in che modo gli utenti possono porre AWS domande ad Amazon Q Developer. Per ulteriori informazioni, consulta <a href="#">Chatta con Amazon Q Developer</a> .	29 maggio 2024

Modifica	Descrizione	Data
myApplications	Una nuova pagina che presenta MyApplications. Per ulteriori informazioni, consulta <a href="#">What is MyApplications? AWS</a> .	29 novembre 2023
Configurazione delle impostazioni unificate	Una nuova pagina delle impostazioni per la configurazione delle impostazioni e dei valori di default applicabili all'utente corrente, inclusi lingua e Regione. Per ulteriori informazioni, consulta <a href="#">Configurazione delle impostazioni unificate</a> .	6 aprile 2022
Nuova AWS Console Home interfaccia utente	Nuova AWS Console Home interfaccia utente, che include widget per la visualizzazione di importanti informazioni sull'utilizzo e collegamenti ai AWS servizi. Per ulteriori informazioni, consulta <a href="#">Utilizzo dei widget</a> .	25 febbraio 2022
Modifica della lingua della console	Scegliere una lingua diversa per la Console di gestione AWS. Per ulteriori informazioni, consulta <a href="#">Modifica della lingua della Console di gestione AWS</a> .	1 aprile 2021

Modifica	Descrizione	Data
Avvio CloudShell	Apri AWS CloudShell da Console di gestione AWS ed esegui i AWS comandi CLI. Per ulteriori informazioni, consulta <a href="#">AWS CloudShell Launching</a> .	22 marzo 2021

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.