Guida alle operazioni di base

AWS Management Console

Version 1.0

AWS Management Console: Guida alle operazioni di base

Table of Contents

Qual è il AWS Management Console? 1
Caratteristiche di AWS Management Console 1
Console di AWS servizio individuali 2
Accedere al AWS Management Console 2
Accesso AWS Management Console con dispositivi mobili 2
Nozioni di base su un servizio 4
Navigazione unificata 5
Accesso al menu Servizi 5
Ricerca di prodotti, servizi, funzionalità e altro 6
Ricerca di AWS prodotti 7
Perfezionamento della ricerca 7
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 AWS Management Console 10
Configurazione delle impostazioni unificate 10
Scegli la tua regione 13
Favorites (Preferiti) 15
Modifica della password 19
Cambiare la lingua del AWS Management Console 21
Accesso alle tue informazioni AWS 23
Accesso alle informazioni sull'account 24
Accesso alle informazioni sull'organizzazione 25
Accesso alle informazioni sulle quote di servizio 25
Accesso alle informazioni di fatturazione 25
Accesso a più account 26
AWS Console Home 28
Visualizzazione di tutti i AWS servizi 28
Lavorare con i widget 28
Gestione dei widget 29
Le mie applicazioni 30
Funzionalità di myApplications 31
Servizi correlati 31

Accesso a myApplications ... 32
Prezzi ... 32
Regioni supportate ... 32
Applicazioni ... 33
Risorse ... 40
Dashboard myApplications ... 43
Chattare con Amazon Q ... 48
Inizia a usare Amazon Q ... 48
Domande di esempio ... 48
AWS Management Console Accesso privato ... 49
Console Regioni AWS di servizio e funzionalità supportate ... 49
Panoramica dei controlli di sicurezza di AWS Management Console Private Access ... 55
Restrizioni relative alla AWS Management Console dalla propria rete ... 55
Connettività dalla propria rete a Internet ... 55
Endpoint VPC e configurazione DNS richiesti ... 55
Configurazione DNS ... 56
Endpoint VPC e DNS configurazione per i servizi AWS ... 58
Implementazione delle policy di controllo dei servizi e delle policy degli endpoint VPC ... 59
Policy di controllo dei servizi ... 60
Policy di endpoint VPC ... 60
Implementazione di policy basate su identità e altri tipi di policy ... 62
Chiavi contestuali delle condizioni AWS globali supportate ... 62
Come funziona AWS Management Console Private Access con aws: SourceVpc ... 62
In che modo si riflettono i diversi percorsi di rete CloudTrail ... 64
Prova Private Access AWS Management Console ... 64
Prova la configurazione con Amazon EC2 ... 65
Prova la configurazione con Amazon WorkSpaces ... 79
Test della configurazione VPC con le policy IAM ... 96
Architettura di riferimento ... 97
Markdown in AWS ... 99
Paragrafi, Interlinea e Linee orizzontali ... 99
Intestazioni ... 100
Formattazione del testo ... 100
Link ... 101
Elenchi ... 101
Tabelle e pulsanti (CloudWatch dashboard) ... 101

Risoluzione dei problemi 103
La pagina non si sta caricando correttamente 103
Il mio browser visualizza un errore di «accesso negato» durante la connessione al AWS Management Console 104
Il mio browser mostra errori di timeout durante la connessione a AWS Management Console .. 105
Voglio cambiare la lingua della AWS Management Console ma non riesco a trovare il menu di selezione delle lingue in fondo alla pagina 105
Cronologia dei documenti 106
..... cix

Qual è il AWS Management Console?

AWS Management ConsoleSi 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 AWS Management Console 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 AWS Management Console 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 AWS Management Console
- Console AWS di servizio individuali in AWS Management Console
- Accedere al AWS Management Console
- Accesso AWS Management Console con dispositivi mobili

Caratteristiche di AWS Management Console

Le caratteristiche importanti di AWS Management Console 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. AWS Management Console 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 AWS Management Console 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 AWS Management Console Private Access per limitare l'accesso AWS Management Console a un insieme specifico di AWS account noti quando il traffico proviene dall'interno della tua rete.

Console AWS di servizio individuali in AWS Management Console

Ogni AWS servizio dispone di una propria console di servizio individuale a cui è possibile accedere all' AWS Management Console interno di. Le impostazioni scelte in Impostazioni unificate per AWS Management Console, 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 AWS Management Console 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 AWS Management Console 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 AWS Management Console

È possibile accedere AWS Management Console a https://console.aws.amazon.com/.

Accesso AWS Management Console con dispositivi mobili

AWS Management ConsoleÈ 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 AWS Management Console 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 AWS Management Console

La AWS Management Console 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 AWS Management Console.
- 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 AWS Management Console 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 AWS Management Console 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 AWS Management Console
- Ricerca di prodotti, servizi, funzionalità e altro utilizzando la ricerca unificata nel AWS Management Console
- Avvio AWS CloudShell dalla barra di navigazione in AWS Management Console
- Accesso alle AWS notifiche e agli eventi Health
- Ottenere supporto
- Configurazione dell' AWS Management Console utilizzo delle impostazioni unificate
- Accesso all' AWS account, all'organizzazione, alla quota di servizio e alle informazioni di fatturazione nel AWS Management Console
- Accesso a più account

Accedendo al menu Servizi in AWS Management Console

Puoi utilizzare il menu dei 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 AWS Management Console.
2. Sulla barra di navigazione, scegli Services (Servizi).
3. (Facoltativo) Scegliete Preferiti per visualizzare l'elenco dei Preferiti.
4. (Facoltativo) Scegliete Tutti i servizi per visualizzare un elenco alfabetico di tutti i AWS servizi.
5. (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 AWS Management Console

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
- Tutorial
- Marketplace
- Risorse

> **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 AWS Management Console
- Affinare la ricerca in AWS Management Console
- Visualizzazione delle funzionalità di un servizio in AWS Management Console

Ricerca di AWS prodotti nel AWS Management Console

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 AWS Management Console, 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 EC2 console Amazon, inserisci ec2 e premi Invio.

Affinare la ricerca in AWS Management Console

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 AWS Management Console, 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 AWS Management Console

Puoi visualizzare le funzionalità di un servizio dai risultati della ricerca.

Per visualizzare le funzionalità di un servizio

1. Nella casella di ricerca sulla barra di navigazione del AWS Management Console, 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 AWS Management Console

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

È possibile eseguire l'avvio CloudShell AWS Management Console 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 AWS Management Console.
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' AWS Management Console utilizzo delle impostazioni unificate

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

Argomenti

- Configurazione delle impostazioni unificate in AWS Management Console
- Scegli la tua regione
- Preferiti in AWS Management Console
- Modifica della password nel AWS Management Console
- Cambiare la lingua del AWS Management Console

Configurazione delle impostazioni unificate in AWS Management Console

È possibile configurare impostazioni e impostazioni predefinite, come visualizzazione, lingua e regione, dalla pagina Impostazioni unificate AWS Management Console . 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 AWS Management Console
- Reimpostazione delle impostazioni unificate in AWS Management Console
- Modifica delle impostazioni unificate in AWS Management Console
- Modifica della modalità visiva di AWS Management Console

Accesso alle impostazioni unificate in AWS Management Console

La procedura seguente descrive come accedere alle impostazioni unificate.

Per accedere alle impostazioni unificate

1. Accedi alla AWS Management Console.
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 AWS Management Console

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 AWS Management Console.
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 AWS Management Console

La procedura seguente descrive come modificare le impostazioni preferite.

Per modificare le impostazioni unificate

1. Accedi alla AWS Management Console.
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 AWS Management Consoleconsulta 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 AWS Management Console 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 AWS Management Console

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 AWS Management Console.
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 uno 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 AWS Management Consoleo 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 (come le EC2 istanze Amazon) sono specifiche della regione in cui sono state create.

Argomenti

- Scelta di una regione dalla barra di navigazione in AWS Management Console
- Impostazione della regione predefinita in AWS Management Console

Scelta di una regione dalla barra di navigazione in AWS Management Console

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 AWS Management Console.
2. Sulla barra di navigazione scegliere il nome della Regione attualmente visualizzata.
3. Scegli una regione a cui passare.

Impostazione della regione predefinita in AWS Management Console

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 AWS Management Console

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. AWS Management Console Quando si aggiunge un servizio o un'applicazione ai Preferiti, questo viene visualizzato nella barra rapida Preferiti.

Argomenti

- Aggiungere preferiti in AWS Management Console
- Accesso ai preferiti in AWS Management Console
- Rimozione dei preferiti in AWS Management Console

Aggiungere preferiti in AWS Management Console

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 AWS Management Console
- Aggiungere servizi ai preferiti nella AWS Management Console
- Aggiungere applicazioni ai preferiti nella AWS Management Console

Barra rapida Preferiti nella AWS Management Console

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 AWS Management Console

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 AWS Management Console.
2. Sulla barra di navigazione, scegli Services (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 AWS Management Console.
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 AWS Management Console

Puoi aggiungere applicazioni ai preferiti dal menu Servizi.

Per aggiungere preferiti dal menu Servizi

1. Apri la AWS Management Console.
2. Sulla barra di navigazione, scegli Services (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. Posiziona 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 AWS Management Console

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 AWS Management Console.

2. Sulla barra di navigazione, scegli Services (Servizi).
3. Scegli Preferiti.
4. Visualizza i servizi e le applicazioni che hai aggiunto ai preferiti.

Favorites quickbar

Per accedere ai preferiti dalla barra rapida dei preferiti

1. Apri la AWS Management Console.
2. Visualizza i servizi e le applicazioni nella barra rapida dei preferiti.

Favorites widget

Per accedere ai preferiti dal widget Preferiti

1. Apri la AWS Management Console.
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, vederethe section called “Lavorare con i widget”.

Rimozione dei preferiti in AWS Management Console

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 AWS Management Console.
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 AWS Management Console.
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 AWS Management Console

Potresti essere in grado di modificare la password in AWS Management Consolebase 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 AWS Management Console
- Utenti IAM in AWS Management Console
- Utenti di IAM Identity Center in AWS Management Console
- Identità federate in AWS Management Console

Utenti root in AWS Management Console

Gli utenti root possono modificare le proprie password direttamente da. AWS Management Console 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 AWS Management Console.
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 AWS Management Console

Gli utenti IAM potrebbero essere in grado di modificare la propria password in AWS Management Console 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, AWS Management Console 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 AWS Management Console

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 AWS Management Console

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 AWS Management Console

L' AWS Console Home esperienza include la pagina delle impostazioni unificate in cui è possibile modificare la lingua predefinita per AWS i servizi in. AWS Management Console 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 tramite Impostazioni unificate in AWS Management Console
- Modifica della lingua predefinita dalla barra di navigazione in AWS Management Console

Lingue supportate

AWS Management Console 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 tramite Impostazioni unificate in AWS Management Console

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 AWS Management Console.
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 AWS Management Console.

   - 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.

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

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 AWS Management Console.
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.

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

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 AWS Management Console 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 AWS Billing and Cost Management 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 AWS Management Console
- Accesso alle informazioni sull'organizzazione nel AWS Management Console
- Accesso alle informazioni sulle quote di servizio in AWS Management Console
- Accesso alle informazioni di fatturazione in AWS Management Console

Accesso alle informazioni sull'account nel AWS Management Console

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 AWS Management Console.
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 AWS Management Console

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

Per accedere alle informazioni sull'organizzazione

1. Accedi alla AWS Management Console.
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 AWS Management Console

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 AWS Management Console.
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 AWS Management Console

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

Per accedere ai dati di fatturazione

1. Accedi alla AWS Management Console.
2. Nella barra di navigazione, scegli il nome dell'account.
3. Scegli Billing and Cost Management.
4. Utilizza la AWS Billing and Cost Management 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. AWS Management Console 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 AWS Management Console in una nuova scheda.

Quando abiliti il supporto multisessione, l'URL della console contiene un sottodominio (ad esempio,`https://000000000000-aaaaaaaa.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 AWS Management Console, 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 AWS Management Console.
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. AWS Management Console

4. Inserisci le credenziali .
5. Selezionare Sign in (Accedi). Viene AWS Management Console 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 AWS Management Console scegli il nome del tuo account.

   c. Visualizza le sessioni aggiuntive che puoi scegliere.

Utilizzo AWS Console Home in AWS Management Console

Questo argomento descrive come utilizzare AWS Console Home, incluso come personalizzare la home page della console. Console Home è la home page di AWS Management Console. 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 AWS Management Console.
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. 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 Home della console.

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. Scegli Invia.

> **Note**
>
> Esaminiamo periodicamente i suggerimenti e potremmo aggiungere nuovi widget nei futuri aggiornamenti alla AWS Management Console.

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 AWS Management Console. 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 AWS Management Console, 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.
- 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 dei livelli di servizio derivanti da Amazon CloudWatch, risultati e tendenze dei costi. AWS Security Hub 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
- Systems Manager
- AWS Service Catalog
- Assegnazione di tag

Accesso a myApplications

È possibile accedere a myApplications dalla AWS Management Console 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 Pacific (Osaka)
- Asia Pacific (Seul)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Tokyo)

- Canada (Centrale)
- Europa (Francoforte)
- Europa (Irlanda)
- Europe (London)
- 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 Pacific (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 i tag esistenti.

Creazione di una nuova applicazione

1. Accedi alla AWS Management Console.
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.
6. (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.

7. (Facoltativo) Aggiungi gruppi di attributi. È possibile utilizzare i gruppi di attributi per archiviare i metadati delle applicazioni.
8. Scegli Next (Successivo).
9. (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

   1. Scegli Cerca e seleziona le risorse.
   2. Scegli Seleziona risorse.
   3. (Facoltativo) Scegli una visualizzazione.
   4. 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 di policy di un utente in IAM:
>
> - `servicecatalog:CreateApplication`
> - `resource-groups:GroupResources`
> - `resource-groups:UngroupResources`
> - `tag:TagResources`
> - `tag:UntagResources`

Per aggiungere risorse utilizzando i 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 AWS CloudFormation stack, seleziona la casella di controllo nella parte inferiore della pagina.

> **Note**
>
> L'aggiunta di uno AWS 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 AWS 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 AWS Management Console.
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

È possibile visualizzare le applicazioni in tutte le regioni o in regioni specifiche e le relative informazioni in una visualizzazione a schede o a tabelle.

Per visualizzare le applicazioni

1. Nella barra laterale sinistra, scegli myApplications.
2. In Regioni, seleziona Regione attuale o Regioni supportate.
3. Per trovare un'applicazione specifica, inserisci il nome, le parole chiave o la descrizione nella barra di ricerca.
4. (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.

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 AWS Management Console.
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. Scegli 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 AWS Management Console.
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 AWS Management Console.
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' EC2 istanza Amazon, 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

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 AWS Management Console.
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 i tag esistenti

1. Apri la AWS Management Console.
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 di tag. Un'applicazione può supportare più di una sincronizzazione tag, ma ogni sincronizzazione tag deve avere una coppia chiave-valore diversa. Dopo aver specificato una coppia chiave-valore diversa per il tag, riprova l'operazione di sincronizzazione dei tag non riuscita.

- Limite massimo raggiunto: hai raggiunto il 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 AWS Management Console.
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.

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 delle metriche delle prestazioni delle risorse Amazon CloudWatch per l'utilizzo della CPU delle EC2 istanze Amazon e le chiamate Lambda.

Configurazione del widget Calcolo

Per compilare i dati nel widget Compute, configura almeno un' EC2 istanza Amazon 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. FOr 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.

Configurazione del widget AWS di sicurezza

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

AWS Security Hub 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, abilitalo 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 EC2 istanze Amazon per la tua applicazione configurando AWS Systems Manager 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 (SLOs) e parametri del livello di servizio dell'applicazione
- 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 AWS Management Console, 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?`

AWS Management Console Accesso privato

AWS Management Console Private Access è una funzionalità di sicurezza avanzata per controllare l'accesso a AWS Management Console. 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 AWS Management Console 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 AWS Management Console rete e da account consentiti.

Argomenti

- Console di servizio e funzionalità Regioni AWS supportate per Private Access
- Panoramica dei controlli di sicurezza di AWS Management Console 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 AWS Management Console
- Architettura di riferimento

Console di servizio e funzionalità Regioni AWS supportate per Private Access

AWS Management Console Private Access supporta solo un sottoinsieme di regioni e AWS servizi. Le console di servizio non supportate saranno inattive nella AWS Management Console. Inoltre, alcune AWS Management Console funzionalità potrebbero essere disabilitate quando si utilizza AWS Management Console Private Access, 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)
- US West (Oregon)
- Asia Pacific (Hyderabad)
- Asia Pacifico (Mumbai)
- Asia Pacifico (Seoul)
- Asia Pacifico (Osaka-Locale)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Malesia)
- Asia Pacifico (Tailandia)
- Asia Pacifico (Tokyo)
- Canada (Centrale)
- Europa (Francoforte)
- Europa (Irlanda)
- Europe (London)
- 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

- Amazon API Gateway
- AWS App Mesh
- AWS Application Migration Service
- AWS Artifact
- Amazon Athena
- AWS Audit Manager
- AWS Auto Scaling
- AWS Batch
- AWS Billing Conductor
- AWS Billing and Cost Management
- 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
- Visione EC2 globale di Amazon
- 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
- Sistema di bilanciamento del carico elastico
- 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 Private Certificate Authority
- 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
- Amazon SageMaker Runtime
- Dati sintetici Amazon SageMaker AI
- AWS Secrets Manager
- AWS Service Catalog
- AWS Security Hub
- Service Quotas (Quote di Servizio)
- AWS Signer
- Amazon Simple Email Service
- Amazon SNS
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Storage Gateway
- Supporto
- AWS Systems Manager
- Amazon Timestream
- AWS Transfer Family
- AWS Trusted Advisor
- Impostazioni unificate
- Amazon VPC IP Address Manager

- Amazon Virtual Private Cloud
- Amazon WorkSpaces Thin client

Panoramica dei controlli di sicurezza di AWS Management Console Private Access

Restrizioni relative alla AWS Management Console dalla propria rete

AWS Management Console 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. AWS Management Console 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 AWS Management Console . 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 AWS Management Console, 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 AWS Management Console, consulta. Risoluzione dei problemi

> **Note**
>
> Attualmente, AWS Management Console 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

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

1. com.amazonaws. *region*.console per AWS Management Console
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 AWS Management Console. 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 AWS Management ConsoleAccedi ad AWS
- Endpoint VPC e DNS configurazione per AWS i servizi in AWS Management Console

DNSconfigurazione per e AWS Management ConsoleAccedi 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 AWS Management Console. 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 AWS Management Console VPC nella zona della console dove si trova la regione desiderata DNS *region*
- *. *region*.console.aws.amazon.com che punta all'endpoint AWS Management Console VPC nella zona della console dove si trova la regione desiderata DNS *region*
- console.aws.amazon.com che punta all'endpoint AWS Management Console VPC negli Stati Uniti orientali (Virginia settentrionale) (us-east-1)
- *.console.aws.amazon.com che punta all'endpoint AWS Management Console 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 AWS Management Console 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 AWS Management Console 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 AWS Management Console . 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
- *.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 AWS Management Console

Le AWS Management Console 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 AWS Management Console 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. AWS Management Console 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 AWS Management Console Private Access per limitare il set di account autorizzati a utilizzare il VPC all'interno del AWS Management Console tuo VPC e delle sue reti locali connesse.

Argomenti

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

Utilizzo di AWS Management Console 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' AWS Management Console 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 AWS Management Console privato.

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

Per ulteriori informazioni in merito SCPs, consulta le politiche di controllo del servizio (SCPs) nella Guida per l'AWS Organizations utente.

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

AWS Management Console 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 EC2 console Amazon, queste policy sugli endpoint VPC non verranno valutate rispetto alle azioni di EC2 Amazon 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 AWS Management Console 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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgId": "o-xxxxxxxxxxx"
        }
      }
    }
  ]
}
```

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

```
{
```

```
  "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 AWS Management Console 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 AWS Management Console Private Access.

Chiavi contestuali delle condizioni AWS globali supportate

AWS Management Console 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 AWS Management Console .

Come funziona AWS Management Console Private Access con aws: SourceVpc

Questa sezione descrive i vari percorsi di rete a cui AWS Management Console 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 AWS

Management Console 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. AWS Management Console Inoltre, è necessario utilizzare la condizione `aws:SourceVpc` IAM nelle policy anziché `aws:SourceVpce` valori specifici con la funzionalità Private Access. AWS Management Console Questa sezione fornisce dettagli su come funzionano i diversi percorsi di rete.

Dopo aver effettuato l'accesso AWS Management Console, un utente effettua le richieste Servizi AWS tramite una combinazione di richieste dirette del browser e richieste che vengono inoltrate dai server AWS Management Console 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 AWS Management Console 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 AWS Management Console 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 AWS Management Console 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 AWS Management Console 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 AWS

Management Console . La `aws:SourceVpce` 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 AWS Management Console , 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 AWS Management Console si riflettono nella cronologia CloudTrail degli eventi.

Per le richieste dirette tramite browser, l'utilizzo di AWS Management Console 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 AWS Management Console 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 AWS Management Console

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

AWS Management Console 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 AWS Management Console senza un'infrastruttura completa.

Argomenti

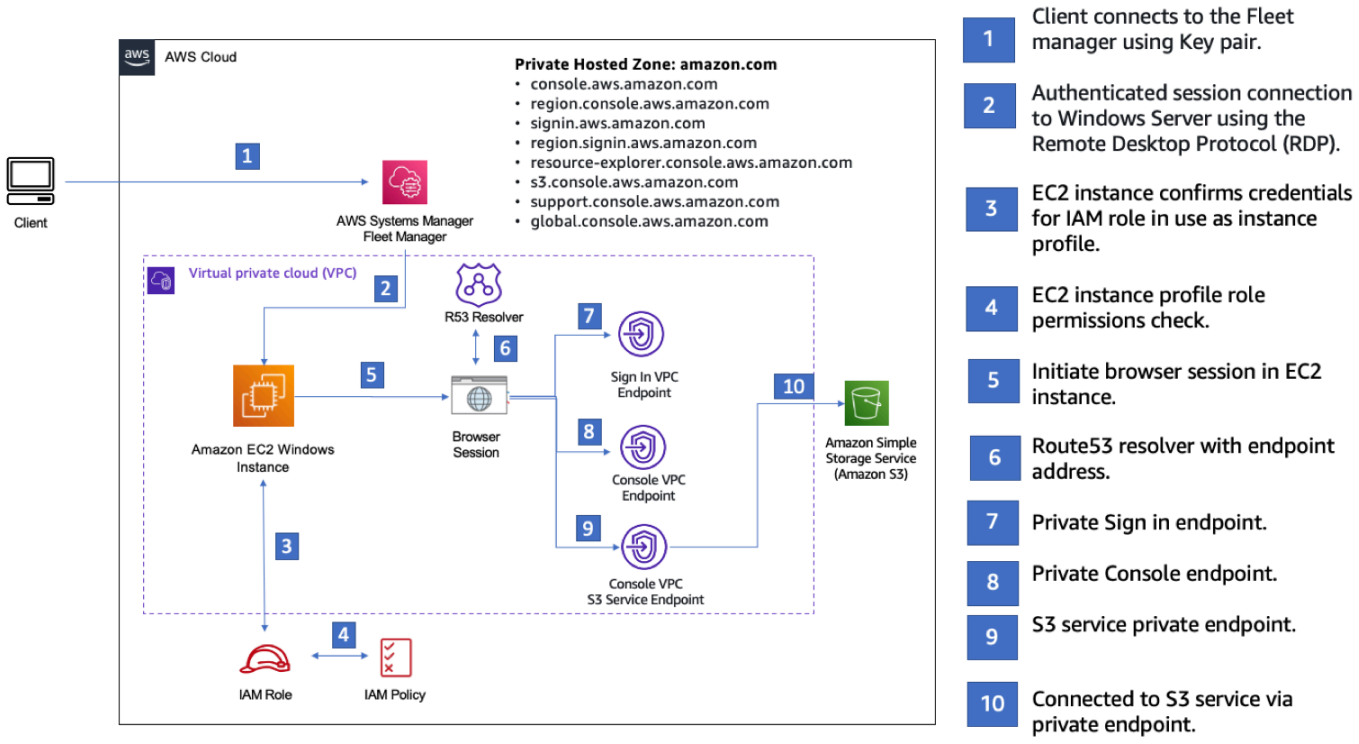
- Prova la configurazione con Amazon EC2
- Prova la configurazione con Amazon WorkSpaces
- Test della configurazione VPC con le policy IAM

Prova la configurazione con Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) fornisce capacità di elaborazione scalabile nel cloud Amazon Web Services. Puoi usare Amazon EC2 per avviare tutti o pochi server virtuali di cui hai bisogno, configurare sicurezza e rete e gestire lo storage. In questa configurazione, utilizziamo Fleet Manager, una funzionalità di AWS Systems Manager, per connetterci a un'istanza Amazon EC2 Windows utilizzando il Remote Desktop Protocol (RDP).

Questa guida illustra un ambiente di test per configurare e provare una connessione AWS Management Console Private Access ad Amazon Simple Storage Service da un' EC2 istanza Amazon. Questo tutorial serve AWS 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 per accedere EC2 a una configurazione di AWS Management Console Private Access. Mostra come un utente è connesso ad Amazon S3 mediante un endpoint privato.



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

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

AWS Management Console EC2 AWS CloudFormation Modello Amazon per l'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::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

  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 AWS CloudFormation.
2. Seleziona Crea stack.

3. Scegliere Con nuove risorse (standard). Carica il file AWS 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 EC2 chiavi Amazon esistenti nel tuo account. Se non disponi di una coppia di EC2 chiavi Amazon esistente, devi crearne una prima di procedere al passaggio successivo. 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.

Per connettersi all' EC2 istanza Amazon

1. Accedi all'account di gestione della tua organizzazione e apri la EC2 console Amazon.
2. Nel riquadro di navigazione, scegliere Instances (Istanze).
3. Nella pagina Istanze, seleziona l'istanza di test Console VPCE creata dal modello. AWS CloudFormation Quindi scegliere Connetti.

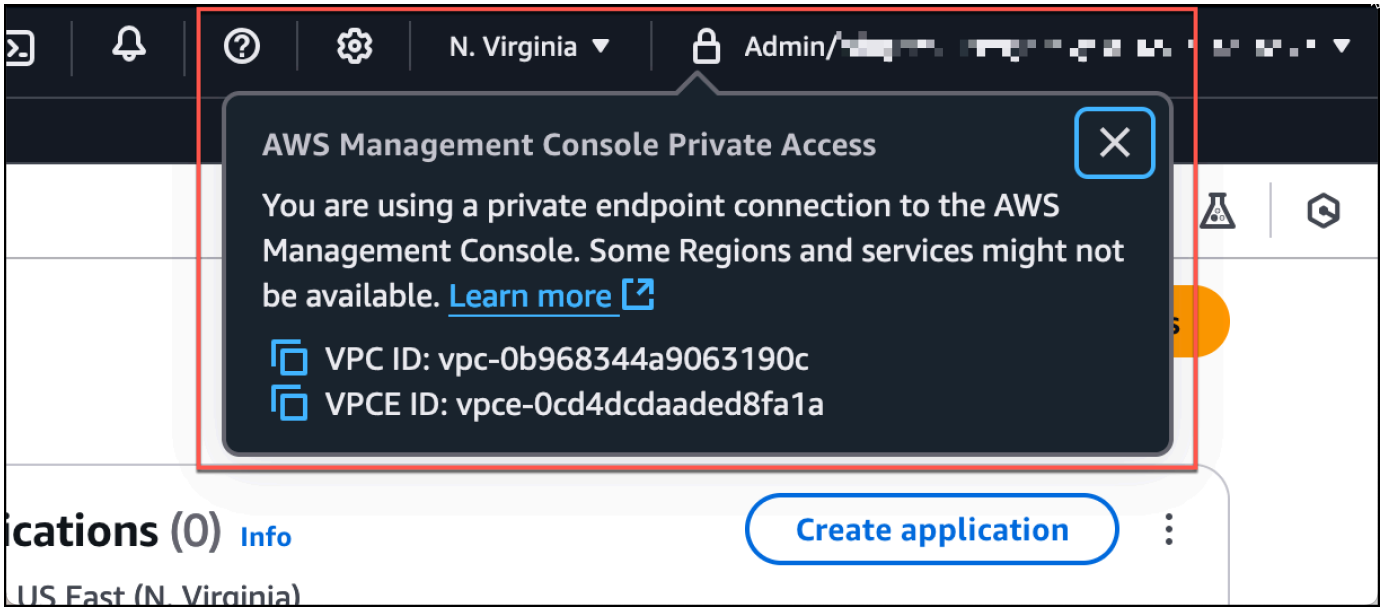
> **Note**
>
> Questo esempio utilizza Fleet Manager, una funzionalità di AWS Systems Manager Explorer, per connettersi a Windows Server. Potrebbero essere necessari alcuni minuti prima che la connessione possa essere avviata.

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' EC2 istanza Amazon e accedere al desktop di Windows tramite l'interfaccia Web, utilizza la chiave privata associata alla coppia di EC2 chiavi Amazon utilizzata durante la creazione del AWS CloudFormation modello.
7. Dall'istanza di Amazon EC2 Windows, apri il file AWS Management Console nel browser.

8. Dopo aver effettuato l'accesso con AWS le tue credenziali, apri la console Amazon S3 e verifica di essere connesso AWS Management Console tramite Private Access.

Per testare la configurazione di AWS Management Console 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.



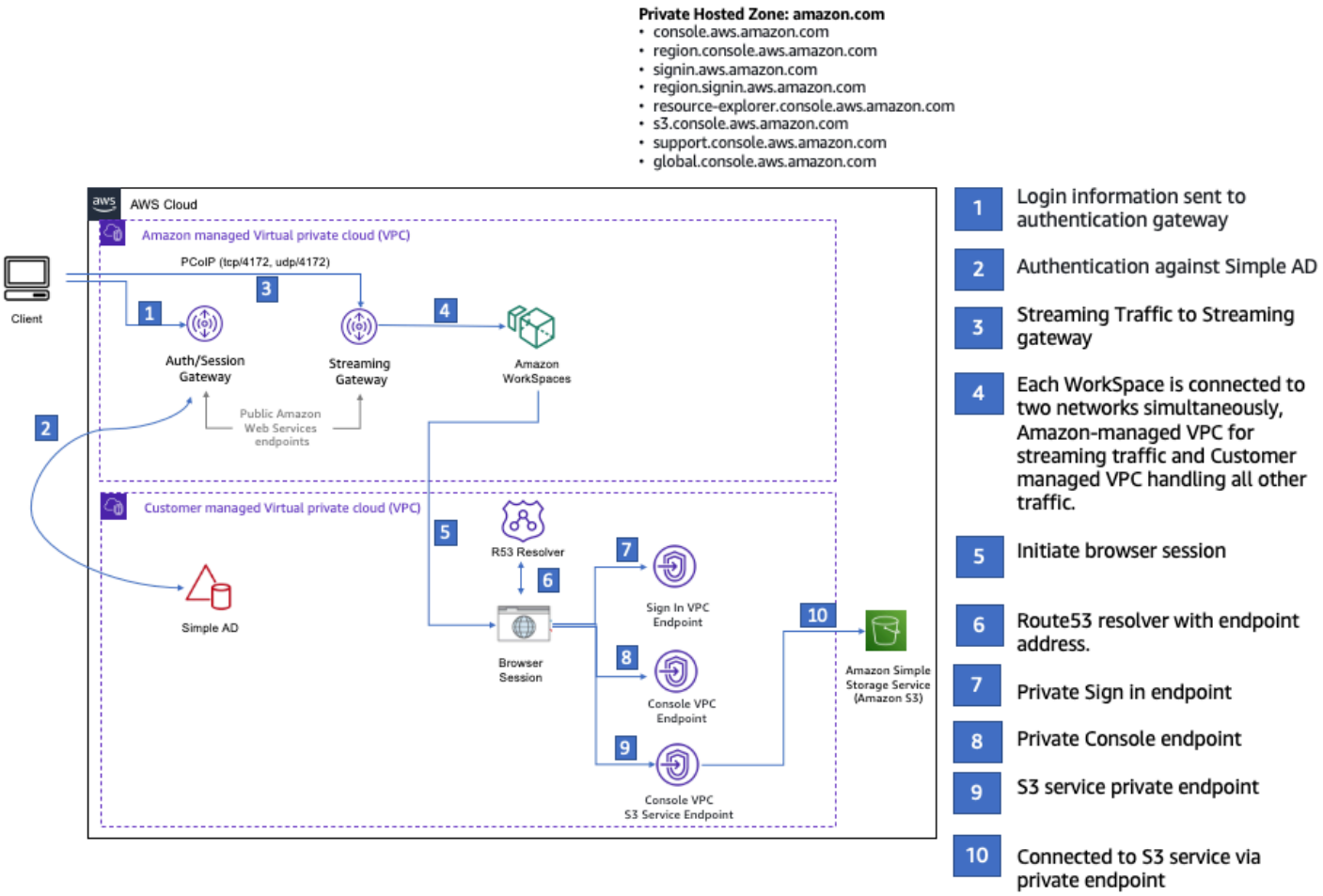
Prova la configurazione con Amazon WorkSpaces

Amazon ti 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 AWS Management Console Private Access. Poi, l'utente visita la console di Amazon Simple Storage Service. WorkSpace Questo ha lo scopo di simulare l'esperienza di un utente aziendale con un laptop su una rete connessa a VPC, accedendovi dal AWS Management Console 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 AWS Management Console

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



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

AWS Management ConsoleAWS 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
```

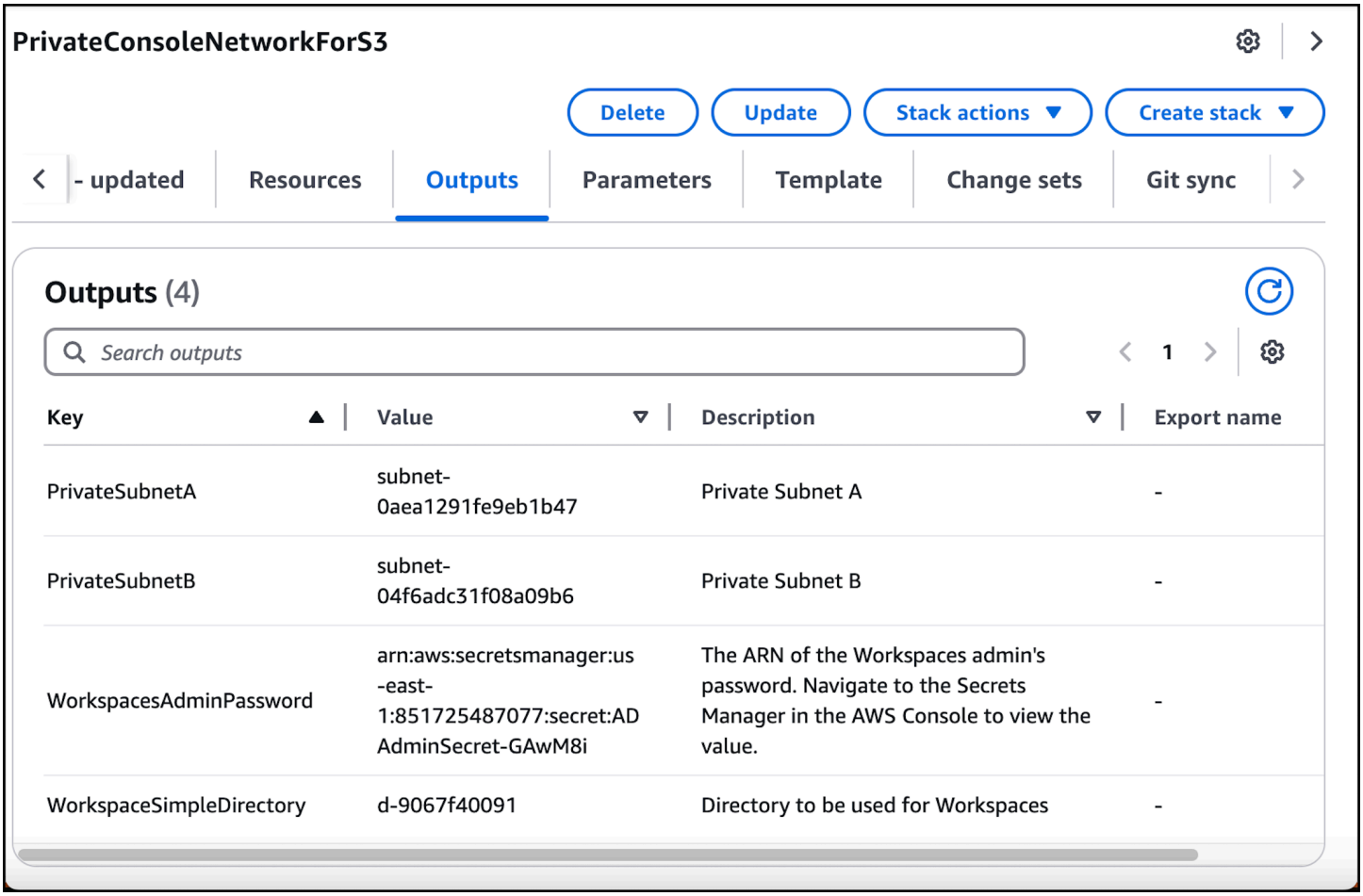
> **Note**
>
> Questa configurazione test è progettata per essere eseguita nella regione Stati Uniti orientali (Virginia settentrionale) (us-east-1).

Configurazione di una rete

1. Accedere all'account di gestione dell'organizzazione e aprire la console AWS CloudFormation.
2. Seleziona Crea stack.
3. Scegliere Con nuove risorse (standard). Carica il file AWS 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.
8. 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

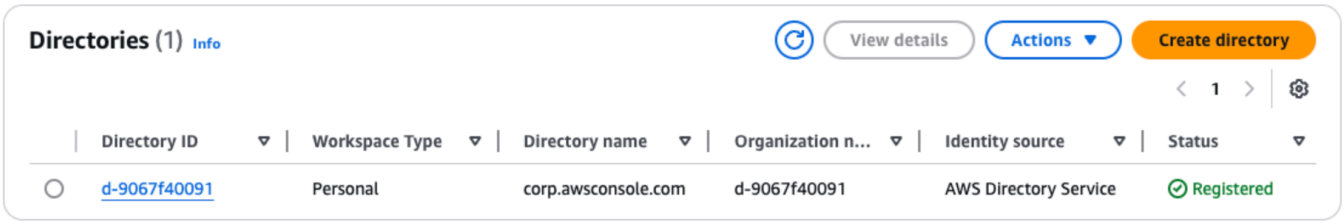
La schermata seguente mostra la visualizzazione della scheda Outputs che mostra i valori per le sottoreti private e per la Workspace Simple Directory.



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

Per creare un WorkSpace

1. Apri la WorkSpaces console.
2. Nel riquadro di navigazione, seleziona Directory.
3. Nella pagina Directory, verificare che lo stato della directory sia Attivo. La schermata seguente mostra una pagina Directory con una directory attiva.



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 AWS 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 AWS Management Console privato.

Per accedere a WorkSpace

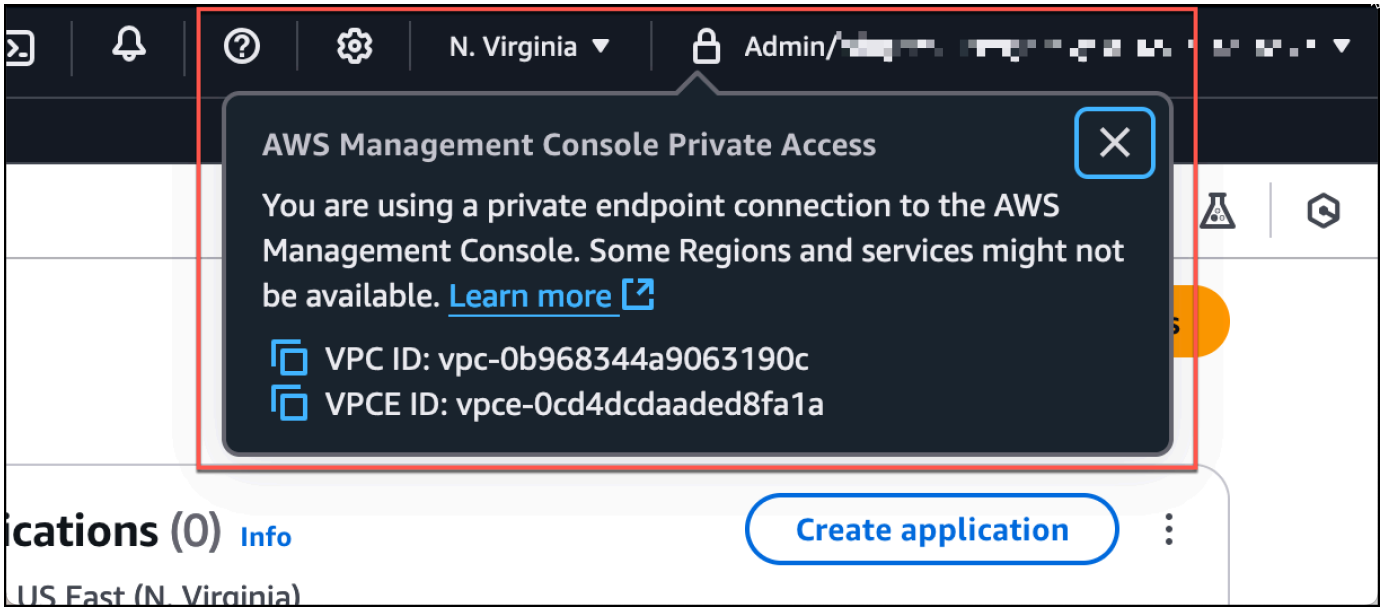
1. Aprire l'e-mail ricevuta nella fase 14 della procedura precedente.
2. Nell'e-mail, scegli il link univoco fornito per configurare il tuo profilo e scaricare il WorkSpaces client.
3. Impostazione della password.
4. Scaricare il client preferito.
5. Installare e avviare il client. Inserire il codice 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 AWS Management Console Private Access

1. Dal tuo WorkSpace, apri il browser. Quindi, vai alla AWS Management Console 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 AWS Management Console 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 o WorkSpaces implementando policy IAM che limitano l'accesso.

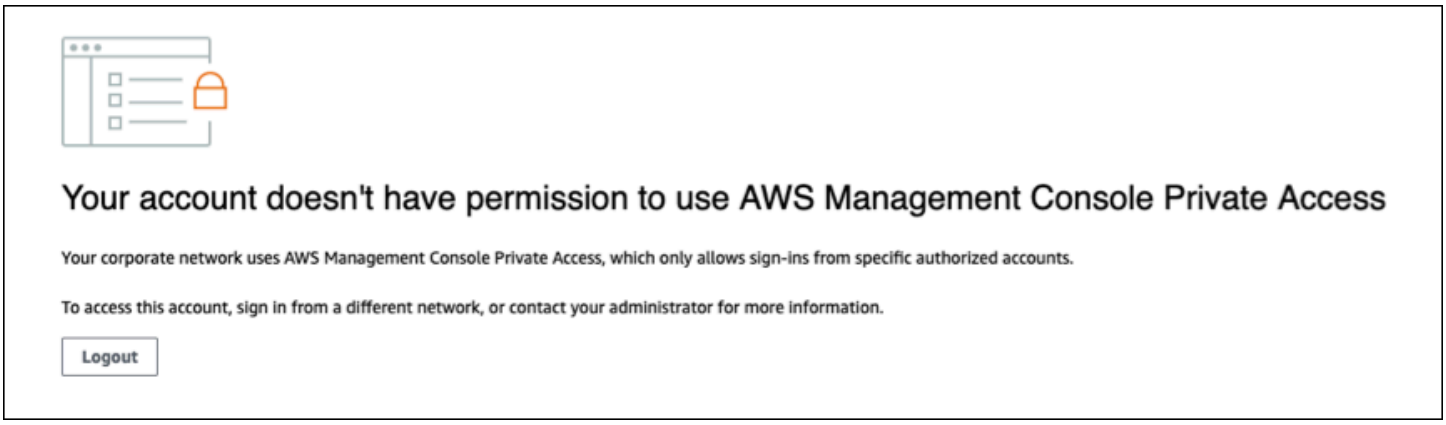
La policy seguente nega l'accesso ad Amazon S3 a meno che non si utilizzi il VPC specificato.

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

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

```
{
    "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.

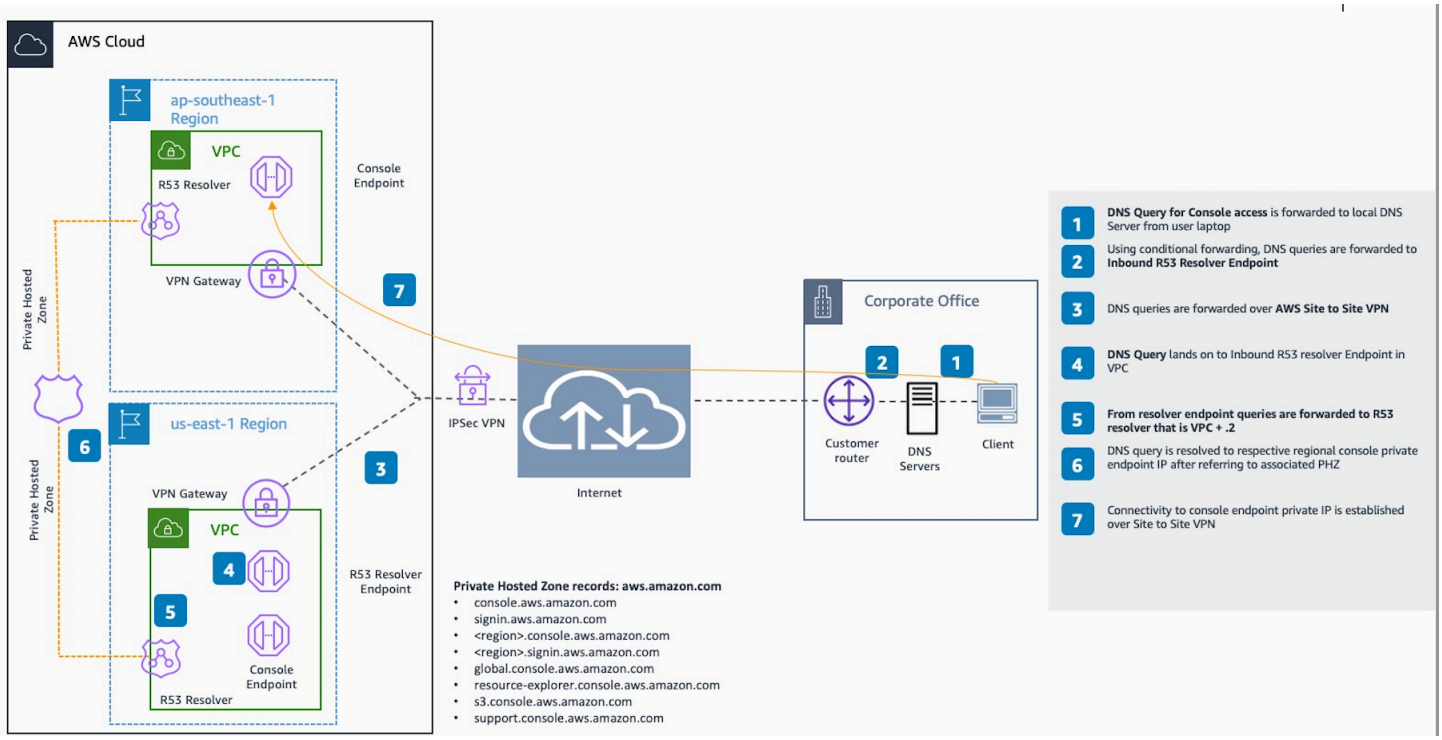


Architettura di riferimento

Per connetterti privatamente a AWS Management Console 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 AWS Management Console 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 AWS Management Console Private Access. AWS Management Console IPs

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

Utilizzo di Markdown nella console

Alcuni servizi AWS Management Console, 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:

```
 

 
```

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:

````
```
This appears in a text box with a background shading.
The text is in monospace.
```
````

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 AWS Management Console.

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 AWS Management Console
- Il mio browser mostra errori di timeout durante la connessione a AWS Management Console
- Voglio cambiare la lingua della AWS Management Console ma non riesco a trovare il menu di selezione delle lingue 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. AWS Management Console 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. AWS Management Console 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 AWS Management Console 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 AWS Management Console

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

- Si accede AWS Management Console 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. Applicale entrambe `aws:SourceIp` e `aws:SourceVpc` dove applicabile.

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

- AWS Management Console Accesso privato

- the section called “Come funziona AWS Management Console 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 AWS Management Console

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. AWS Management Console Per accedere AWS Management Console 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 AWS Management Console service endpoints (Enpoint del servizio della console) nei Riferimenti generali di AWS.

Per visualizzare lo stato di tutti Servizi AWS, incluso il AWS Management Console, vedi. AWS Health Dashboard

Voglio cambiare la lingua della AWS Management Console ma non riesco a trovare il menu di selezione delle lingue in fondo alla pagina

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

Per ulteriori informazioni, consulta Modifica della lingua della AWS Management Console.

Cronologia dei documenti

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

Modifica	Descrizione	Data
Pagina aggiunta	Nuova pagina aggiunta per spiegare la funzionalità multisessione. Per ulteriori informazioni, consulta ???.	6 dicembre 2024
Pagina aggiornata	Modifica della pagina della password aggiornata. Per ulteriori informazioni, consulta ???.	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, consulta ??? e ???.	18 giugno 2024
Pagina aggiornata	Che cos'è il AWS Management Console? pagina aggiornata. Per ulteriori informazioni, consulta ???.	18 giugno 2024
Richiedi assistenza	È stata aggiunta una nuova pagina per descrivere come ottenere assistenza. Per ulteriori informazioni, consulta ???.	18 giugno 2024
Navigazione unificata e AWS Console Home	Nuove pagine aggiunte per descrivere come utilizzare la	18 giugno 2024

Modifica	Descrizione	Data
	console. Per ulteriori informazioni, consulta ??? e ???.	
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 Chatta con Amazon Q Developer.	29 maggio 2024
Le mie applicazioni	Una nuova pagina che presenta MyApplications. Per ulteriori informazioni, consulta What is MyApplications? AWS .	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 Configurazione delle impostazioni unificate	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 Utilizzo dei widget.	25 febbraio 2022

Modifica	Descrizione	Data
Modifica della lingua della console	Scegliere una lingua diversa per la AWS Management Console. Per ulteriori informazioni, consulta Modifica della lingua della AWS Management Console.	1 aprile 2021
Avvio CloudShell	Apri AWS CloudShell da AWS Management Console ed esegui i AWS comandi CLI. Per ulteriori informazioni, consulta AWS CloudShell Launching.	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.