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?

AWS Management ConsoleÈ un'applicazione web che comprende e fa riferimento a un'ampia raccolta di console di servizio per la gestione delle risorse. AWS Quando effettui l'accesso per la prima volta, visualizzi la home page della console. L'home page consente l'accesso a ogni console dei servizi e offre un unico posto per accedere alle informazioni necessarie per eseguire le attività correlate ad AWS . Consente inoltre di personalizzare l'esperienza Console Home aggiungendo, rimuovendo e riorganizzando widget come Recentemente visitati,AWS Health e altro.

> **Note**
>
> L'opzione di selezione della lingua è stata spostata nella nuova pagina delle Impostazioni unificate. Per ulteriori informazioni, consulta Modifica della lingua della AWS Management Console.

Le singole console dei servizi, poi, offrono una vasta gamma di strumenti per il cloud computing, oltre a informazioni sul tuo account e sulla fatturazione.

Utilizzo del dispositivo selezionato

La AWS Management Console è progettata per funzionare su tablet e altri tipi di dispositivi:

- 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.

AWS Management Console È disponibile anche come app per Android e iOS. L'app consente di eseguire operazioni su dispositivi mobili ed è un valido complemento dell'esperienza Web completa. Ad esempio, puoi visualizzare e gestire facilmente le istanze Amazon EC2 e gli CloudWatch allarmi Amazon esistenti dal tuo telefono.

Puoi scaricare l'app per dispositivi mobili AWS Console da Amazon Appstore, Google Play o iTunes.

Configurazione del AWS Management Console

Questo argomento descrive come configurare AWS Management Console e come utilizzare la pagina Impostazioni unificate per impostare impostazioni predefinite applicabili a tutte le console di servizio. Spiega anche i widget, una funzionalità della dashboard Console Home che consente di aggiungere componenti personalizzati che tengono traccia delle informazioni sui servizi e sulle risorse. AWS

Argomenti

Utilizzo dei widget

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.

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 il simbolo dei puntini di sospensione verticali nell'angolo in alto a 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 trascinalo 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.

Configurazione delle impostazioni unificate

Puoi configurare impostazioni e impostazioni predefinite, come visualizzazione, lingua e regione, dalla pagina Impostazioni unificate AWS Management Console . 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.

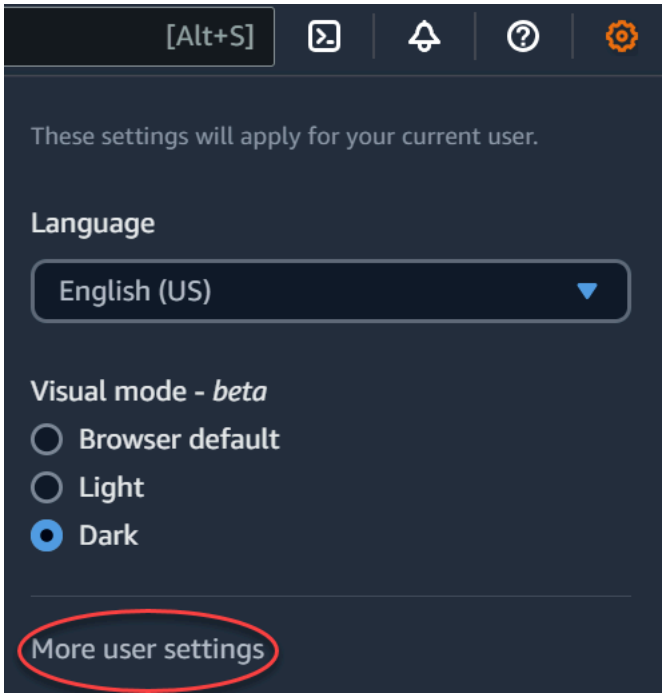
> **Important**
>
> Per garantire che le impostazioni, i servizi preferiti e i servizi visitati di recente persistano a livello globale, questi dati vengono archiviati in tutte le aree Regioni AWS, comprese le regioni che sono disabilitate per impostazione predefinita. Queste Regioni sono Africa (Città 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.

Accesso alle impostazioni unificate

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. Scegli Altre impostazioni utente per aprire la pagina Impostazioni unificate.



Reimpostazione delle impostazioni unificate

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 Impostazioni unificate scegliendo Altre impostazioni utente.
4. Scegli Ripristina tutto.

Modifica delle impostazioni unificate

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 Impostazioni unificate scegliendo Altre 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. Seleziona Salvataggio delle modifiche.

Cambia la 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.

Modifica della lingua predefinita in Impostazioni unificate

La procedura seguente descrive come modificare la lingua predefinita utilizzando la 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.

Scelta di una 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..

Scelta di una regione

1. Accedi alla AWS Management Console.
2. Scegliere un servizio per passare alla relativa console.
3. Sulla barra di navigazione scegliere il nome della Regione attualmente visualizzata. Quindi scegli la Regione alla quale desideri passare.

Per scegliere una Regione di default

1. Nella barra di navigazione scegli l'icona delle impostazioni, quindi Altre impostazioni utente per passare alla pagina Impostazioni unificate.
2. Scegliere Edit (Modifica) accanto a Localization and default Region (Localizzazione e regione di default).
3. Seleziona la tua regione predefinita, quindi scegli Salva impostazioni. Se non selezioni una Regione di default, la Regione di default sarà l'ultima Regione visitata.
4. (Facoltativo) Scegli Vai alla nuova regione predefinita per passare immediatamente alla nuova regione predefinita.

> **Note**
>
> Se hai creato AWS risorse ma non le vedi nella console, è possibile che la console mostri risorse provenienti da una regione diversa. Alcune risorse (ad esempio le istanze Amazon EC2) sono specifiche della Regione in cui sono state create. Per visualizzarle, utilizza il selettore di Regione per scegliere la Regione che contiene le risorse.

Aggiunta e rimozione di Preferiti

Per accedere più rapidamente ai servizi usati di frequente, puoi salvare le console dei servizi in un elenco di Preferiti.

Aggiunta di un servizio all'elenco di Preferiti

1. Accedi alla AWS Management Console.
2. Scegli il pulsante Aggiungi widget sul lato destro superiore o inferiore della pagina.
3. Nel menu Aggiungi widget selezionare i Preferiti da aggiungere alla console, quindi scegliere Aggiungi.

   I Preferiti verranno aggiunti nella parte inferiore della home della console. È possibile trascinare e rilasciare i preferiti selezionando la barra del titolo nella parte superiore del widget, quindi trascinare il widget in una nuova posizione nella pagina.
4. Sulla barra di navigazione, scegli Services (Servizi).

5. In uno degli elenchi Visitati di recente o Tutti i servizi, passa con il mouse sul nome del servizio che desideri aggiungere come preferito.
6. Seleziona la stella a sinistra del nome del servizio.
7. Ripeti i due passaggi precedenti per aggiungere altri servizi all'elenco Preferiti.

Rimozione di un servizio dall’elenco di Preferiti

1. Sulla barra di navigazione, scegli Services (Servizi).
2. Esegui una di queste operazioni:
   - Nell’elenco Preferiti, posizionati sul nome di un servizio. Quindi, seleziona la x a destra del nome del servizio.
   - In uno degli elenchi Visitati di recente o Tutti i servizi, deseleziona la stella accanto al nome del servizio che si trova nell'elenco dei Preferiti.

Modifica della password

Se sei il proprietario di un account, puoi modificare la password del tuo AWS account da AWS Management Console.

Modifica della password

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).

Modifica della 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, a cui puoi accedere dalla barra di navigazione. Puoi apportare questa modifica ovunque nella console.

> **Note**
>
> Questa procedura modifica la lingua per tutte le console, ma non per la documentazione AWS . Per modificare la lingua della documentazione, utilizza il menu delle lingue in altro a destra nella pagina della documentazione.

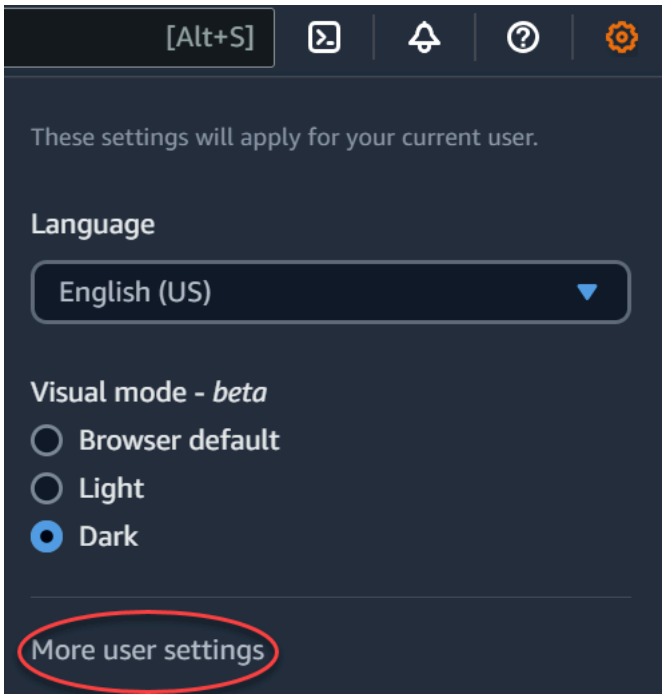
AWS Management Console Attualmente supporta le seguenti lingue:

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

Per cambiare la lingua predefinita in Impostazioni unificate

1. Accedi alla AWS Management Console.
2. Nella barra di navigazione, scegli l’icona delle impostazioni.

3. Scegli Altre impostazioni utente per aprire la pagina Impostazioni unificate.



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.

Per cambiare la lingua predefinita dalla barra di navigazione

1. Accedi alla AWS Management Console.

2. Nella barra di navigazione, scegli l’icona delle impostazioni.
3. Per Lingua, scegli la lingua Predefinita del browser o la lingua preferita dall'elenco a discesa.

Nozioni di base su un servizio

La AWS Management Console offre molteplici modi per spostarsi alle singole console dei servizi.

Per aprire una console per un servizio

Completa una delle seguenti 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, consultare Ricerca di prodotti, servizi, funzionalità e altro utilizzando la ricerca unificata.
- Nel widget Recently visited services (Servizi visitati di recente), scegliere il nome di un servizio.
- Nel widget Recently visited services (Servizi visitati di recente), scegliere View all AWS services (Visualizza tutti i servizi AWS). Quindi, sulla pagina All AWS services (Tutti i servizi AWS), scegliere un nome per il 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.

Ricerca di prodotti, servizi, funzionalità e altro utilizzando la ricerca unificata

La casella di ricerca nella barra di navigazione fornisce uno strumento di ricerca unificato per rintracciare servizi e funzionalità AWS , documentazione del servizio e Marketplace AWS. Basta digitare alcuni caratteri per vedere i risultati di tutte queste categorie. Più caratteri digiti, più la ricerca perfezionerà i risultati.

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

1. Nella casella di ricerca sulla barra di navigazione di AWS Management Console, inserisci tutti o parte dei termini di ricerca.
2. Effettua una delle operazioni seguenti per perfezionare la ricerca e ottenere maggiori dettagli:
   - Per restringere i risultati al tipo di contenuto desiderato, scegli una delle categorie a sinistra.
   - Per visualizzare altri risultati per una determinata categoria, scegli Vedi tutti i ***n*** risultati per ogni intestazione di categoria. Per tornare all'elenco dei risultati principali, scegli Indietro nell'angolo in alto a sinistra.
   - Per passare rapidamente alle funzionalità più comuni di un servizio, posizionati sul nome del servizio nei risultati e scegli un collegamento.
   - Per ottenere maggiori dettagli su una documentazione o un Marketplace AWS risultato, fai una pausa sul titolo del risultato.
3. Scegli un collegamento qualsiasi per accedere al servizio, all'argomento o alla pagina Marketplace AWS .

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

Chatta con Amazon Q Developer

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?`

Su AWS cosa è attivo myApplications?

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. 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 su 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

Funzionalità di myApplications

- Crea applicazioni: crea nuove applicazioni e organizzane le risorse. Le tue applicazioni vengono visualizzate automaticamente in MyApplications, quindi puoi intervenire nelle API AWS Management Console, nella CLI e negli SDK. 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, tra cui 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

MyApplications è disponibile nei seguenti formati: 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)

Nozioni di base su myApplications

Per iniziare a utilizzare myApplications per creare, monitorare e gestire le tue applicazioni, segui i passaggi seguenti.

Fase 1: creazione di un'applicazione

Crea una nuova applicazione o esegui l'onboarding di un' AppRegistry applicazione esistente creata prima dell'8 novembre 2023 per iniziare a usare MyApplications.

Create an application

Per creare un'applicazione

1. Accedi alla AWS Management Console.
2. Nella barra laterale sinistra, 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 e può essere utilizzato per identificare le risorse associate all'applicazione. Per ulteriori informazioni, consulta 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. Seleziona Successivo.
9. (Facoltativo) Aggiungi risorse esistenti:

   > **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.

   a. Scegli Seleziona risorse.

b. (Facoltativo) Scegli una visualizzazione.

c. 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.

d. Seleziona la casella di controllo accanto alle risorse che desideri aggiungere.

e. Scegli Aggiungi.

f. Seleziona Successivo.

10. Rivedi le scelte effettuate.
11. Se associ una AWS CloudFormation pila, 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 .

12. Scegli Crea applicazione.

Onboard existing application

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 Onboard di ***nome dell'applicazione***.
6. Se associ uno CloudFormation stack, seleziona la casella di controllo nella casella di avviso.
7. Scegli Onboard dell'applicazione.

Fase 2: Visualizzazione delle applicazioni

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.

Gestione delle applicazioni

In questo argomento viene spiegato come gestire le applicazioni.

Modifica delle applicazioni

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 myApplications, seleziona Azioni, poi scegli Modifica applicazione.
5. In Modifica descrizione dell'applicazione, aggiorna la descrizione, quindi scegli Salva modifiche.

Per modificare tag

- Segui la procedura descritta in Gestione dei tag nella Guida per l'AWS Service Catalog AppRegistry amministratore.

Per modificare gruppi di attributi

- Segui la procedura descritta in Modifica dei gruppi di attributi nella Guida per l'AWS Service Catalog AppRegistry amministratore.

Eliminazione delle applicazioni

È possibile eliminare le applicazioni che non sono più necessarie.

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. Scegli Elimina.

7. Conferma l'eliminazione, quindi scegli Elimina applicazione.

Creazione di frammenti di codice

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.

Gestione delle risorse

In questo argomento viene descritto come gestire le risorse.

Aggiungere risorse

Aggiungendo risorse alle applicazioni sei in grado di raggrupparle e di gestirne la sicurezza, le prestazioni e la conformità.

Per aggiungere 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.

Rimozione delle risorse

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

Ogni applicazione creata o integrata ha la propria dashboard myApplications. La dashboard di 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 Utilizzo dei widget.

Widget Configurazione della dashboard dell'applicazione

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

Widget Riepilogo dell'applicazione

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

Widget Calcolo

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

Configurazione del widget Calcolo

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

Widget Costi e utilizzo

Questo widget mostra i dati AWS sui costi e sull'utilizzo delle risorse dell'applicazione. È possibile utilizzare questi dati per confrontare i costi mensili e visualizzare le ripartizioni dei costi per Servizio AWS. Questo widget riepiloga solo i costi delle risorse contrassegnate con il tag AWS dell'applicazione, escluse tasse, commissioni e altri costi condivisi non direttamente associati a

una risorsa. I costi indicati non sono combinati e vengono aggiornati almeno una volta ogni 24 ore. Per ulteriori informazioni, consulta Analisi dei costi con Esploratore di risorse AWS nella Guida per l'utente di AWS Cost Management .

Configurazione del widget Costi e utilizzo

Per configurare il widget Costi 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 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 .

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 istanze Amazon EC2 per la tua applicazione AWS Systems Manager configurando Patch Manager. Per maggiori informazioni, consulta Utilizzo delle policy di patch di Quick Setup nella Guida per l'utente di AWS Systems Manager .

Per informazioni sui prezzi, consulta Prezzi di AWS Systems Manager.

Widget Monitoraggio e operazioni

Questo widget mostra:

- Allarmi e avvisi per le risorse associate all'applicazione
- Obiettivi e metriche del livello di servizio dell'applicazione (SLO)
- Parametri di Application Signals disponibili AWS

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 Insights 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.

AWS Management Console Accesso privato

AWS Management Console Private Access è una funzionalità di sicurezza avanzata per controllare l'accesso a. AWS Management Console AWS Management Console L'accesso privato 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.

Argomenti

Console Regioni AWS di servizio e funzionalità supportate

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 (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)
- 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

- Amazon Athena
- AWS Auto Scaling
- AWS Billing Conductor
- AWS Certificate Manager
- AWS Cloud Map
- Amazon CloudFront
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- Amazon CodeGuru
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Compute Optimizer
- AWS Console Home
- AWS Database Migration Service
- AWS DeepRacer
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon EC2
- Amazon EC2 Global View
- EC2 Image Builder
- Amazon EC2 Instance Connect
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- AWS Elastic Disaster Recovery
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache
- Amazon EMR

- Amazon EventBridge
- Amazon GameLift
- AWS Global Accelerator
- AWS Glue DataBrew
- AWS Ground Station
- Amazon GuardDuty
- 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 video Amazon Kinesis
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Grafana gestito da Amazon
- 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 Manager
- OpenSearch Servizio Amazon
- AWS Organizations
- Amazon S3 su Outposts
- Amazon SageMaker Runtime

- Dati SageMaker sintetici Amazon
- AWS Secrets Manager
- Service Quotas (Quote di Servizio)
- AWS Signer
- Amazon Simple Email Service
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Support
- AWS Systems Manager
- AWS Transfer Family
- Impostazioni unificate
- Amazon VPC IP Address Manager

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 AWS Management Console dalla rete solo a un gruppo specifico di utenti noti Account AWS all'interno dell'organizzazione. 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 L'accesso privato richiede i seguenti due endpoint VPC per regione. Sostituire *regione* con le informazioni relative alla propria 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 Opzioni di connettività da Amazon VPC ad Amazon VPC nel white paper Opzioni di connettività di Amazon Virtual Private Cloud.

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:

- Record CNAME regionali (in tutte le regioni)
- region.signin.aws.amazon.com che punta all'endpoint VPC nella zona di accesso Accedi ad AWS DNS
- region.console.aws.amazon.com che punta all'endpoint VPC nella zona della console AWS Management Console DNS
- Record CNAME senza regioni solo per la Regione Stati Uniti orientali (Virginia settentrionale). Configura sempre la regione Stati Uniti orientali (Virginia settentrionale).
  - signin.aws.amazon.com che punta all'endpoint Accedi ad AWS VPC negli Stati Uniti orientali (Virginia settentrionale) (us-east-1)
  - console.aws.amazon.com che punta all'endpoint 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-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 si utilizza Route 53 per configurare il proprio DNS, andare a https://console.aws.amazon.com/route53/v2/hostedzones# per verificare la configurazione DNS. Per ogni zona ospitata privata in Route 53, verificare che siano presenti i seguenti set di record.

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

Endpoint VPC e DNS configurazione per i servizi AWS

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-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 AWS Management Console Private Access a più console di servizio. 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 dei servizi (SCP) e le policy degli endpoint VPC AWS Management Console per Private Access per limitare il set di account autorizzati a utilizzare il from all'interno AWS Management Console del tuo VPC e delle relative reti locali connesse.

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

Se AWS l'organizzazione utilizza una policy di controllo dei servizi (SCP) che consente servizi specifici, è necessario aggiungere altre azioni `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 sulle SCP, consulta Policy di controllo dei servizi (Service Control Policies, SCP) nella Guida per l'utente di AWS Organizations .

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 console Amazon EC2, queste policy sugli endpoint VPC non verranno valutate rispetto alle azioni di Amazon EC2 intraprese per visualizzare quella pagina. Piuttosto, puoi utilizzare le policy IAM associate all'IAM Principal che ha effettuato l'accesso per controllarne l'autorizzazione alle azioni di servizio. AWS

> **Note**
>
> Le policy degli endpoint VPC per gli endpoint VPC e gli endpoint 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 creando policy e collegandole alle identità o alle risorse IAM (utenti, gruppi di utenti o ruoli). AWS 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 condizione `aws:SourceVpce` verrà impostata sui rispettivi ID di endpoint VPC di accesso o della 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 dei VPC. Questo argomento descrive come provare Accesso privato alla AWS Management Console senza un'infrastruttura completa.

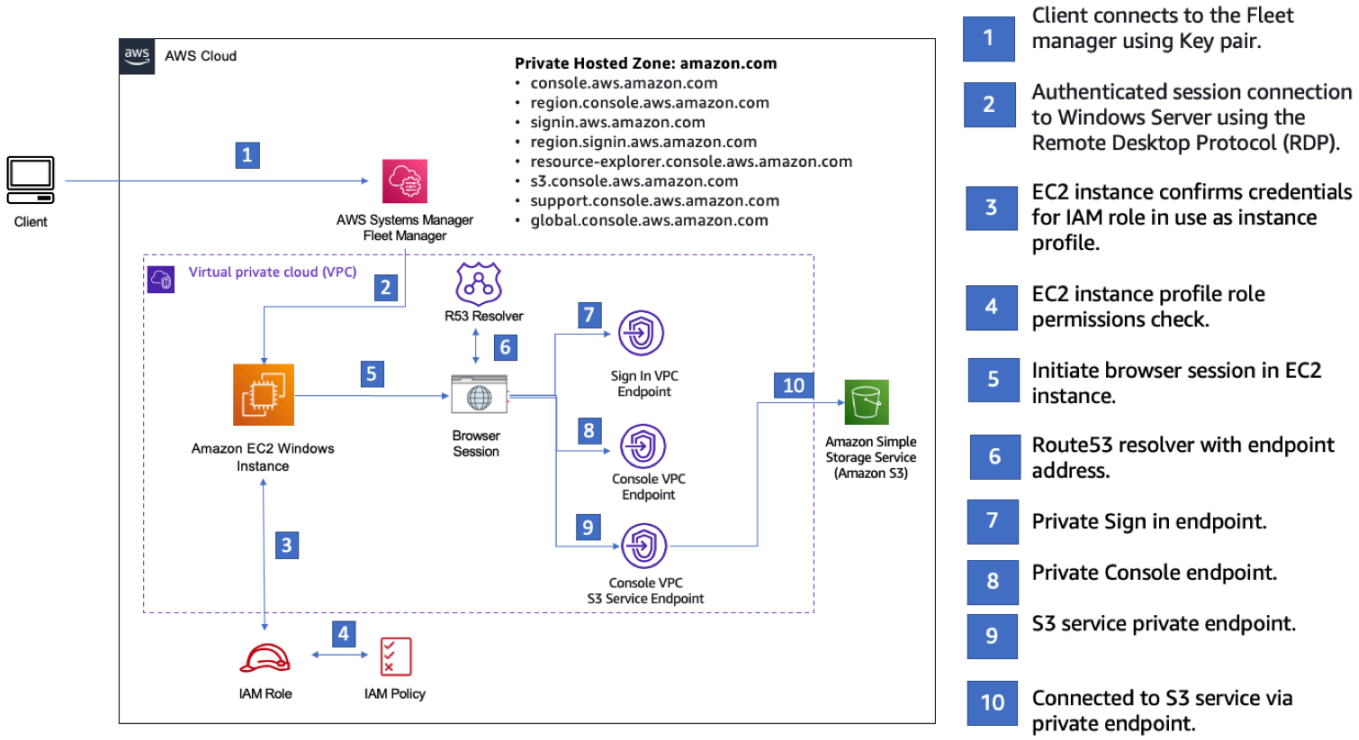
Argomenti

Test della configurazione con Amazon EC2

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

Questa guida illustra un ambiente di test per configurare e provare una connessione AWS Management Console Private Access ad Amazon Simple Storage Service da un'istanza Amazon EC2. 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 EC2 per accedere a una configurazione di Accesso privato alla AWS Management Console . 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 Modello Amazon AWS CloudFormation EC2 per ambiente di accesso privato

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

```
  Ec2KeyPair:
    Type: AWS::EC2::KeyPair::KeyName
    Description: The EC2 KeyPair to use to connect to the Windows instance

  PublicSubnet1CIDR:
    Type: String
    Default: 172.16.1.0/24
    Description: CIDR range for Public Subnet A

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

  PublicSubnet3CIDR:
    Type: String
    Default: 172.16.2.0/24
    Description: CIDR range for Public Subnet C

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

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

  PrivateSubnet3CIDR:
    Type: String
    Default: 172.16.3.0/24
    Description: CIDR range for Private Subnet C

  LatestWindowsAmiId:
    Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
    Default: '/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-Base'

  InstanceTypeParameter:
    Type: String
    Default: 't2.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

  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

  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 chiavi Amazon EC2 esistenti nel tuo account. Se non si dispone di una coppia di chiavi Amazon EC2 esistente, è necessario creane una prima di passare alla fase successiva. Per ulteriori informazioni, consulta Create a key pair using Amazon EC2 nella Amazon EC2 User Guide.
7. Seleziona Crea stack.
8. Dopo aver creato lo stack, scegliere la scheda Risorse per visualizzare le risorse che sono state create.

Eseguire la connessione all'istanza Amazon EC2

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

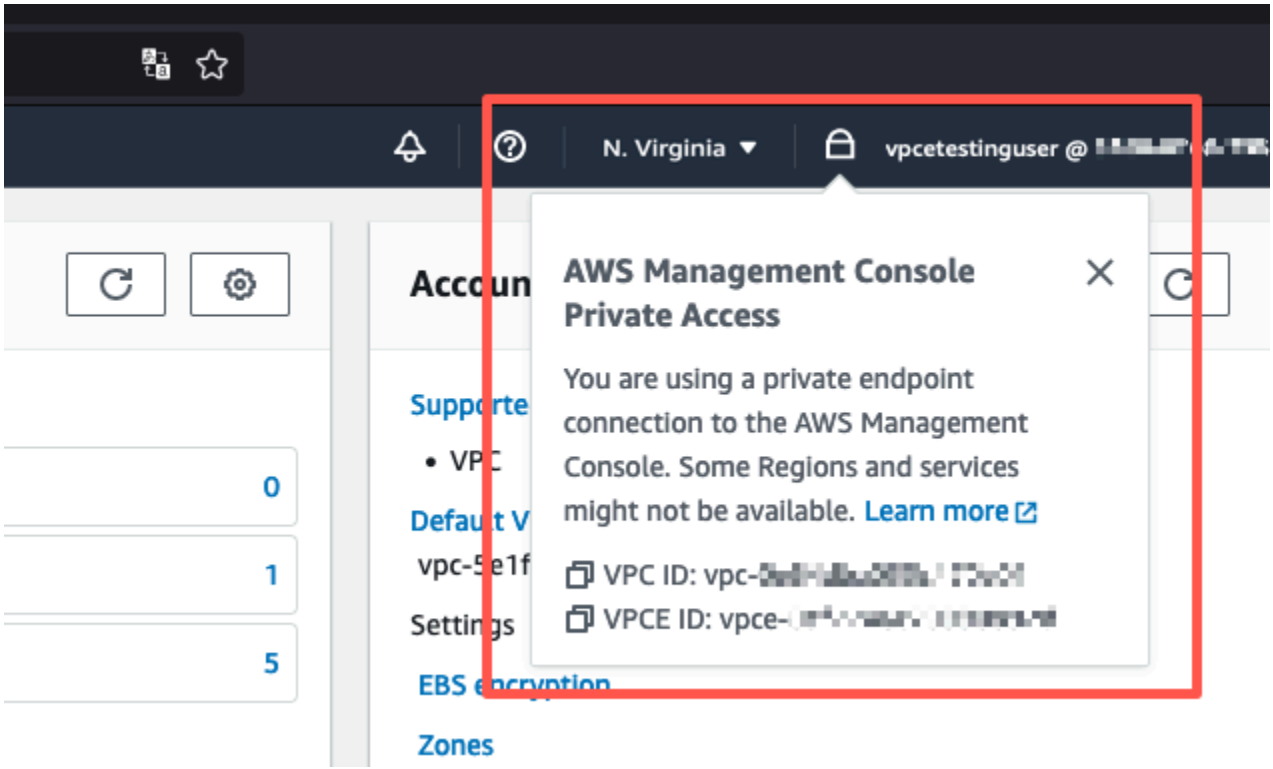
> **Note**
>
> Questo esempio utilizza Fleet Manager, una funzionalità di AWS Systems Manager Explorer, per connettersi a Windows Server. Potrebbero essere necessari alcuni minuti prima che la connessione possa essere avviata.

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

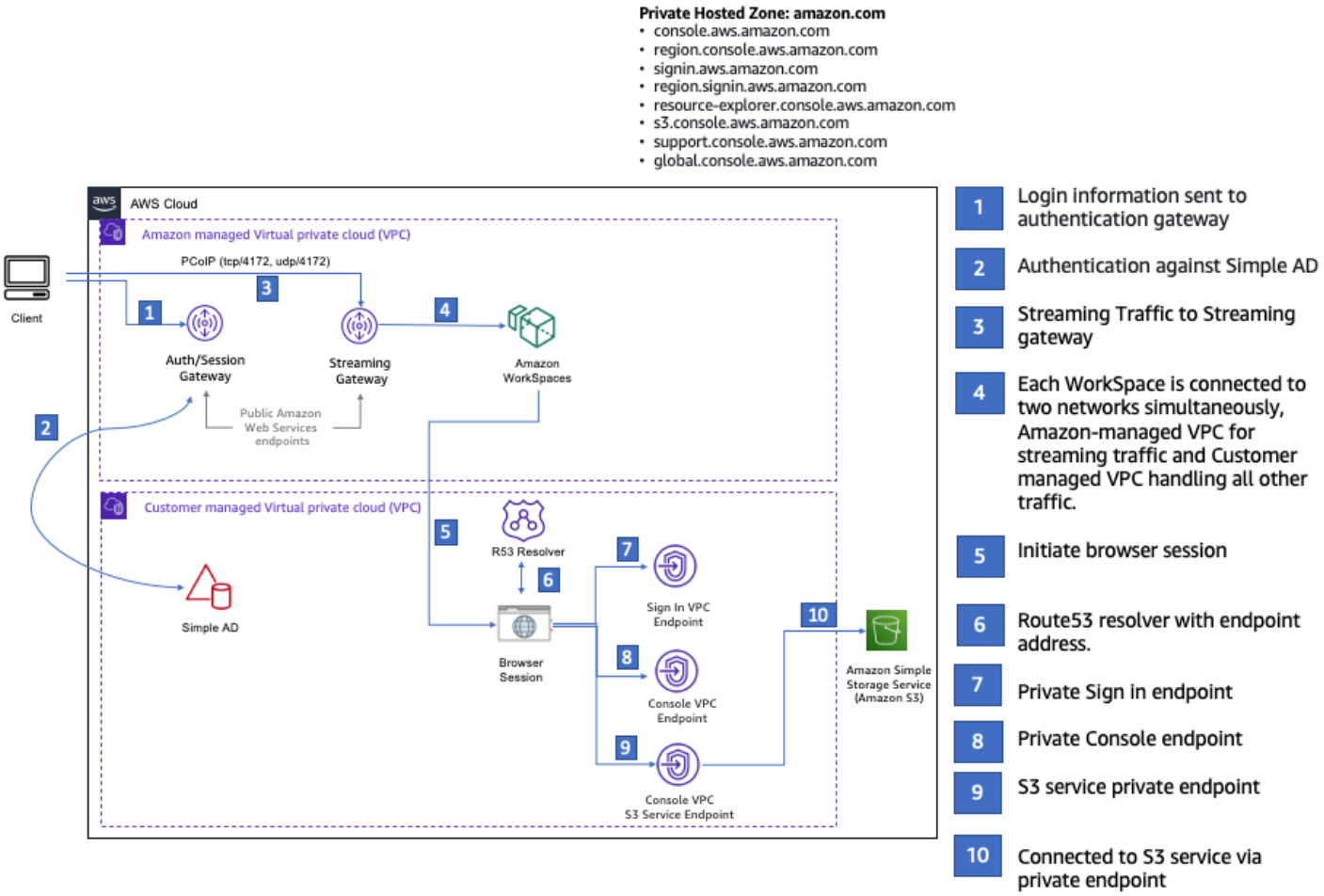
Amazon ti WorkSpaces consente di fornire desktop virtuali basati su cloud Windows, Amazon Linux o Ubuntu Linux per i tuoi utenti, noti come. WorkSpaces È possibile aggiungere o rimuovere rapidamente utenti man mano che le proprie esigenze cambiano. Gli utenti possono accedere ai propri desktop virtuali 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

# 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

 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

  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: "ADAdminSecret"
      Description: "Password for directory services admin"
      GenerateSecretString:
        SecretStringTemplate: '{"username": "Admin"}'
        GenerateStringKey: password
        PasswordLength: 30
        ExcludeCharacters: '"@/\'

  WorkspaceSimpleDirectory:
    Type: AWS::DirectoryService::SimpleAD
    DependsOn: AppVPC
    DependsOn: PrivateSubnetA
    DependsOn: PrivateSubnetB
    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
```

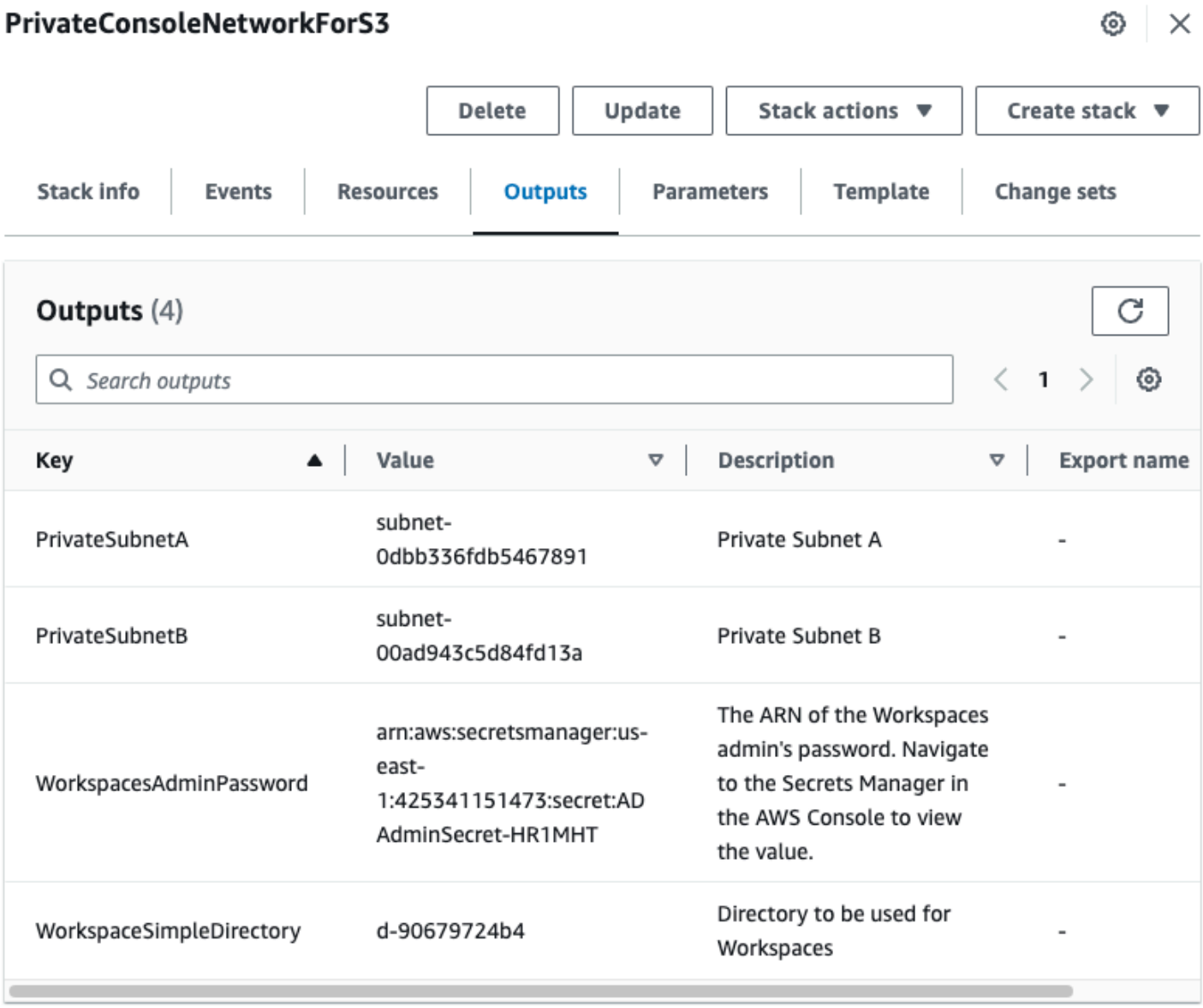
```
  WorkspacesAdminPassword:
    Description : "The ARN of the Workspaces admin's password.  Navigate to the Secrets
Manager in the AWS Console to view the value."
    Value: !Ref ADAdminSecret
```

> **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

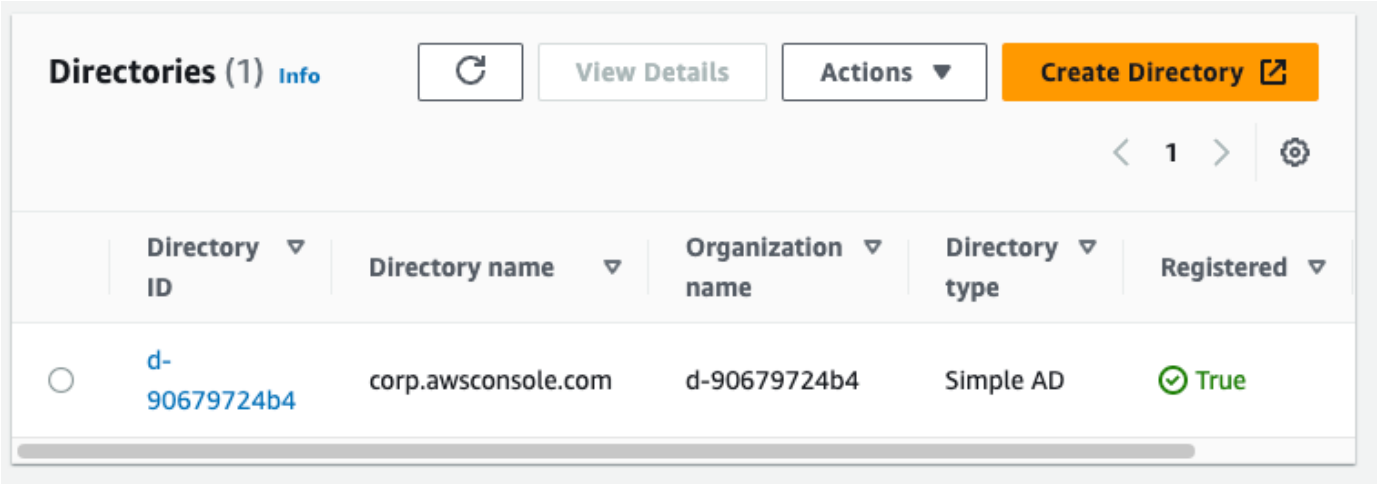
La schermata seguente mostra la visualizzazione della scheda Outputs che mostra i valori per le sottoreti private e per la Workspace Simple Directory.



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. Seleziona 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

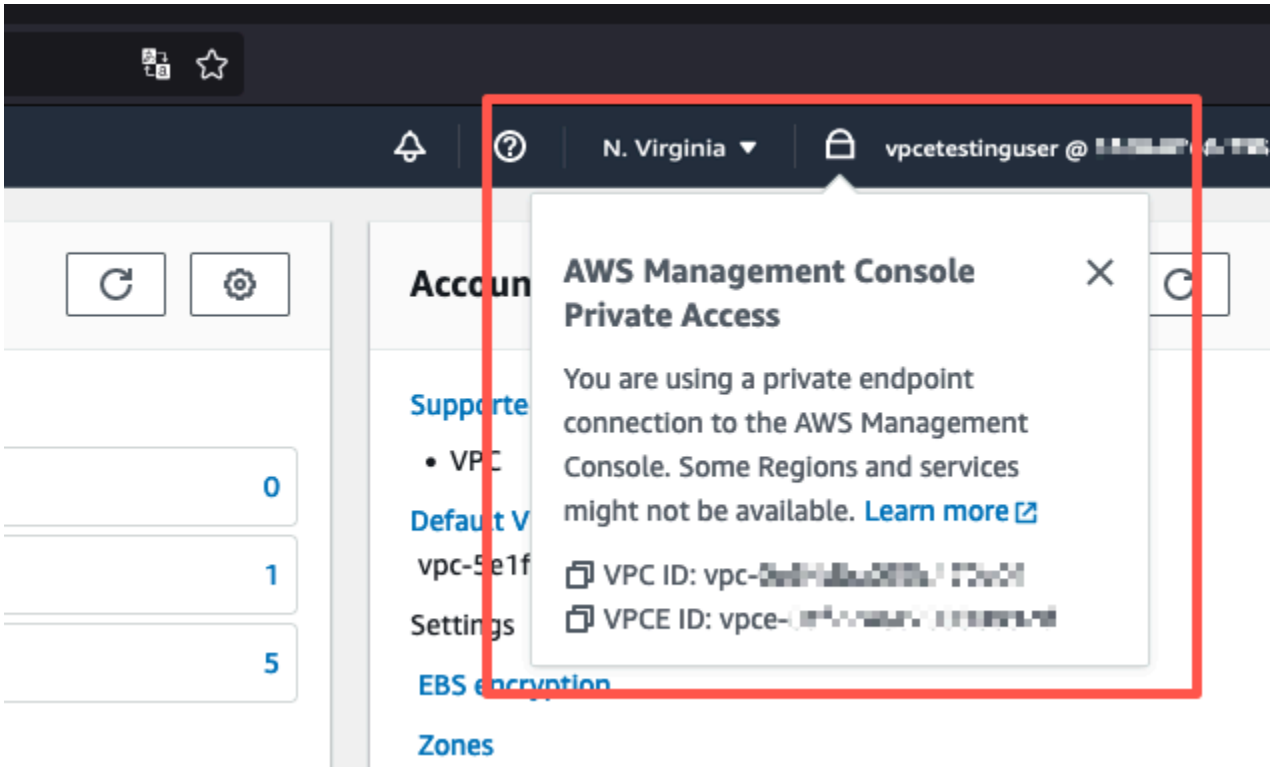
1. Aprire l'e-mail ricevuta nella fase 14 della procedura precedente.
2. Nell'e-mail, scegli il link univoco fornito per configurare il tuo profilo e scaricare il WorkSpaces client.
3. Impostazione della password.
4. Scaricare il client preferito.
5. Installare e avviare il client. Inserire il codice 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 WorkSpaces o implementando policy IAM che limitano l'accesso.

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

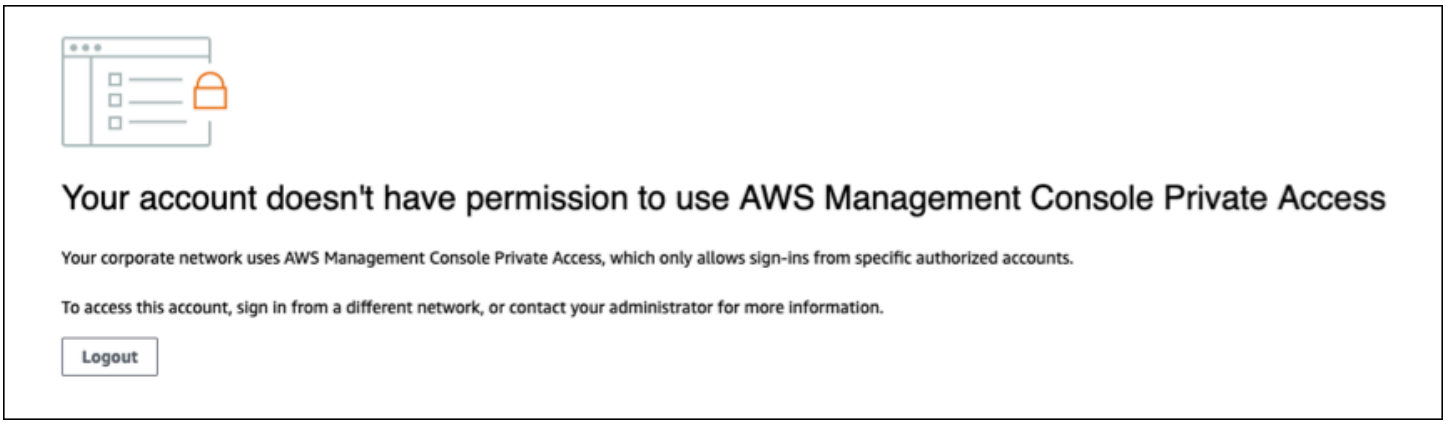
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "S3:*",
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": "sourceVPC"
                },
       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

```
        }
    ]
}
```

La seguente policy limita l'accesso a determinati Account AWS ID 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"
                    ]
                }
            }
        }
    ]
}
```

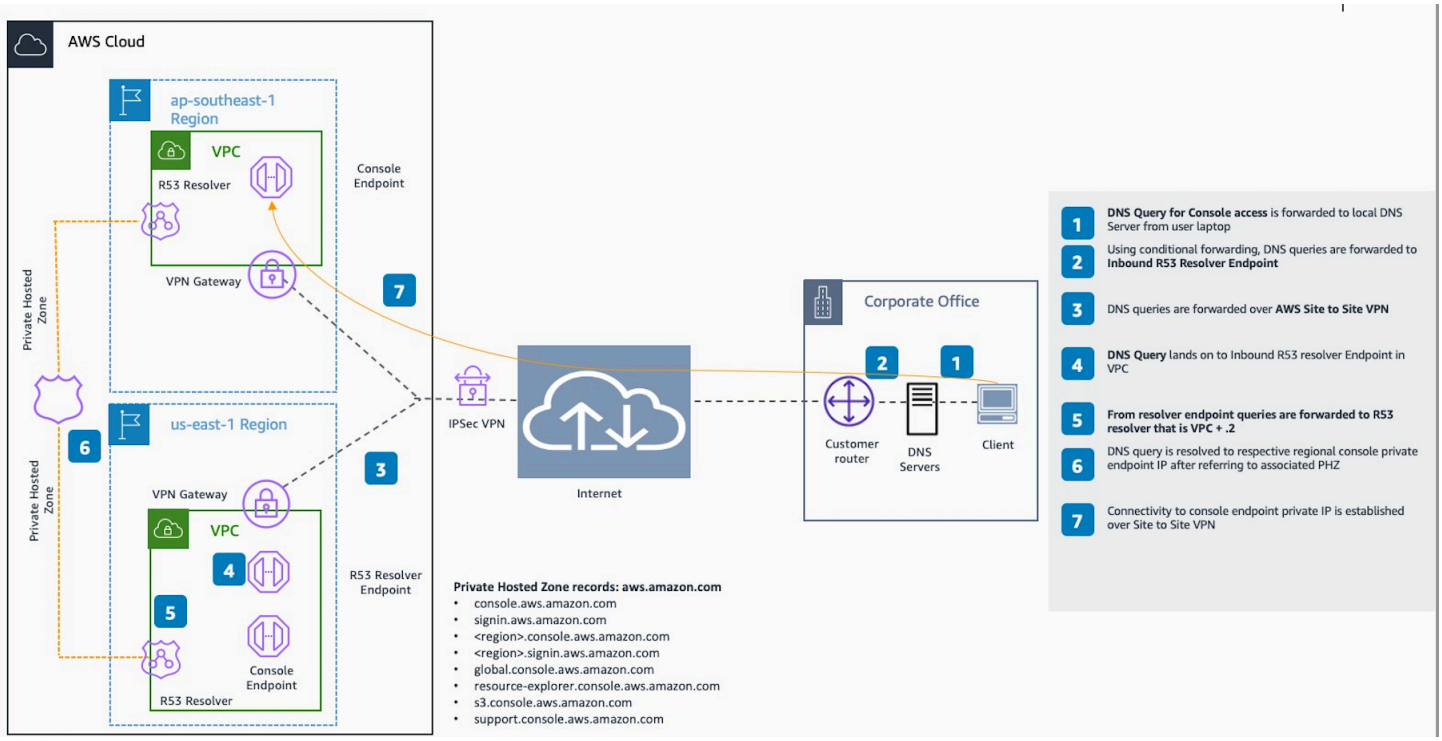
Se ci si connette con un'identità che non appartiene al proprio account, viene visualizzata la seguente pagina di errore.



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 What is AWS Site-to-Site VPN nella Site-to-Site VPN User Guide.AWS 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 agli IP privati degli AWS Management Console endpoint Private Access. AWS Management Console

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 AWS Management Console, nonché nella regione Stati Uniti orientali (Virginia settentrionale) e configurare la zona ospitata privata.

Avvio di AWS CloudShell sulla barra degli strumenti della console

AWS CloudShell è una shell pre-autenticata basata su browser che può essere avviata direttamente da AWS Management Console sulla console. Puoi eseguire i comandi della AWS CLI per i servizi che utilizzano la tua shell preferita (Bash, PowerShell o Z shell).

Puoi avviare CloudShell su Console Toolbar utilizzando uno dei seguenti due metodi:

- Scegli l'icona CloudShell nella parte inferiore a sinistra della console.
- Seleziona l'icona CloudShell 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 in cui è disponibile AWS CloudShell, consulta l'elenco dei servizi regionali AWS. La scelta della regione della console è sincronizzata con la regione CloudShell. Se CloudShell non è disponibile in una regione selezionata, CloudShell opererà nella regione più vicina.

Ottenere le informazioni di fatturazione

Se disponi delle autorizzazioni necessarie, è possibile ottenere informazioni sugli addebiti AWS della console.

Per ottenere le informazioni di fatturazione

1. Nella barra di navigazione, scegli il nome dell'account.
2. Scegli Pannello di controllo fatturazione.
3. Utilizza il pannello di controllo AWS Billing and Cost Management per trovare un riepilogo e un'analisi dettagliata delle spese mensili. Per ulteriori informazioni, consulta la Guida per l'utente di AWS Billing.

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

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 errori 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

- 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 utilizzi tutti i seguenti dispositivi:

- Un browser dall'interno di un VPC.
- Endpoint VPC.
- Policy IAM che contengono una chiave di condizione `aws:SourceIp` globale.

Nella console, vai alla pagina delle politiche IAM. Ti consigliamo di esaminare le politiche IAM che contengono una chiave di condizione `aws:SourceIp` globale e aggiungerne `aws:SourceVpc` una.

In alternativa, puoi prendere in considerazione l'onboarding alla funzionalità di accesso AWS Management Console privato per accedere AWS Management Console tramite un endpoint VPC e utilizzare `aws:SourceVpc` le condizioni previste dalle tue politiche. Per ulteriori informazioni, consulta AWS Management Console Accesso privato.

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-code.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
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	25 febbraio 2022

Modifica	Descrizione	Data
	informazioni, consulta Utilizzo dei widget.	
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

Glossario per AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per Glossario AWS.

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.