aws

Guida per l'utente

AWS Sign-In

AWS Sign-In: Guida per l’utente

Table of Contents

Che cos'è AWS Sign-In?

Questa guida ti aiuta a comprendere i diversi modi in cui puoi accedere ad Amazon Web Services (AWS), a seconda del tipo di utente. Per ulteriori informazioni su come accedere in base al tipo di utente e alle AWS risorse a cui desideri accedere, consulta uno dei seguenti tutorial.

- Accedi al Console di gestione AWS
- Accedi al tuo AWS portale di accesso
- Accedi come identità federata
- Accedi tramite AWS Command Line Interface
- Accedi con ID Builder AWS

Se riscontri problemi di accesso al tuo Account AWS, consulta. Risoluzione dei problemi Account AWS problemi di accesso Per assistenza con la tua ID Builder AWS vistaRisoluzione dei problemi relativi al AWS Builder ID. Stai cercando di creare un Account AWS? Iscriviti per AWS. Per ulteriori informazioni su come l'iscrizione AWS può aiutare te o la tua organizzazione, consulta Contattaci.

Argomenti

Terminologia

Amazon Web Services (AWS) utilizza una terminologia comune per descrivere la procedura di accesso. Ti consigliamo di leggere e comprendere questi termini.

Amministratore

Chiamato anche Account AWS amministratore o amministratore IAM. L'amministratore, in genere personale IT (Information Technology), è un individuo che supervisiona un Account AWS. Gli amministratori dispongono di un livello di autorizzazioni più elevato Account AWS rispetto agli altri membri dell'organizzazione. Gli amministratori stabiliscono e implementano le impostazioni per. Account AWS Creano inoltre utenti IAM o IAM Identity Center. L'amministratore fornisce a questi utenti le credenziali di accesso e un URL di accesso a cui accedere. AWS

Account

Uno standard Account AWS contiene sia le AWS risorse che le identità che possono accedere a tali risorse. Gli account sono associati all'indirizzo e-mail e alla password del proprietario dell'account.

Credenziali

Chiamate anche credenziali di accesso o credenziali di sicurezza. Nelle procedure di autenticazione e identificazione un sistema utilizza le credenziali per identificare chi effettuare una chiamata e stabilire se consentire l'accesso richiesto. Le credenziali sono le informazioni fornite dagli utenti per AWS effettuare l'accesso e accedere alle risorse. AWS Le credenziali per gli utenti umani possono includere un indirizzo e-mail, un nome utente, una password definita dall'utente, un ID account o un alias, un codice di verifica e un codice di autenticazione a più fattori (MFA) monouso. Per l'accesso programmatico, puoi anche utilizzare le chiavi di accesso. Consigliamo di utilizzare chiavi di accesso a breve termine quando possibile.

Per ulteriori informazioni sulle credenziali, consulta Credenziali AWS di sicurezza.

> **Note**
>
> Il tipo di credenziali che un utente deve inviare dipende dal tipo di utente.

Credenziali aziendali

Le credenziali fornite dagli utenti quando accedono alla rete e alle risorse aziendali. L'amministratore aziendale può configurare l'utente in Account AWS modo che utilizzi le stesse credenziali utilizzate per accedere alla rete e alle risorse aziendali. Queste credenziali vengono fornite dall'amministratore o dal dipendente dell'help desk.

Profilo

Quando ti registri per un AWS Builder ID, crei un profilo. Il tuo profilo include le informazioni di contatto che hai fornito e la possibilità di gestire i dispositivi di autenticazione a più fattori (MFA) e le sessioni attive. Puoi anche saperne di più sulla privacy e su come gestiamo i tuoi dati nel tuo profilo. Per ulteriori informazioni sul tuo profilo e su come è correlato a un Account AWS, vediID Builder AWS e altre AWS credenziali.

Credenziali utente root

Le credenziali dell'utente root sono l'indirizzo e-mail e la password utilizzati per creare il. Account AWS Si consiglia vivamente di aggiungere l'MFA alle credenziali dell'utente root per una maggiore sicurezza. Le credenziali dell'utente root forniscono l'accesso completo a tutti i AWS servizi e le risorse dell'account. Per ulteriori informazioni sull'utente root, vedereUtente root.

Utente

Un utente è una persona o un'applicazione che dispone delle autorizzazioni per effettuare chiamate API ai AWS prodotti o per accedere alle AWS risorse. Ogni utente dispone di un set unico di credenziali di sicurezza che non vengono condivise con altri utenti. Queste credenziali sono distinte dalle credenziali di sicurezza dell' Account AWS. Per ulteriori informazioni, consulta Determina il tipo di utente.

Codice di verifica

Un codice di verifica verifica la tua identità durante il processo di accesso utilizzando l'autenticazione a più fattori (MFA). I metodi di consegna dei codici di verifica variano. Possono essere inviati tramite SMS o e-mail. Rivolgiti al tuo amministratore per ulteriori informazioni.

Disponibilità regionale per AWS Sign-In

AWS Sign-in è disponibile in diverse versioni di uso comune Regioni AWS. Questa disponibilità semplifica l'accesso ai AWS servizi e alle applicazioni aziendali. Per un elenco completo delle regioni Sign-in supportate, consulta AWS Sign-In endpoint e quote.

Sign-in registrazione degli eventi

CloudTrail è abilitato automaticamente sull'utente Account AWS e registra gli eventi quando si verifica un'attività. Le seguenti risorse possono aiutarti a saperne di più sulla registrazione e il monitoraggio degli eventi di accesso.

- CloudTrail registra i tentativi di accesso a. Console di gestione AWS Tutti gli eventi di accesso di utenti IAM, utenti root e utenti federati generano record nei CloudTrail file di registro. Per ulteriori informazioni, consulta Eventi di accesso alla Console di gestione AWS nella Guida per l'utente di AWS CloudTrail .
- Se si utilizza un endpoint regionale per accedere a Console di gestione AWS, CloudTrail registra l'`ConsoleLogin`evento nella regione appropriata per l'endpoint. Per ulteriori informazioni sugli AWS Sign-In endpoint, consulta AWS Sign-In Endpoints and Quotas nella Guida di riferimento generale.AWS
- Per ulteriori informazioni su come CloudTrail registra gli eventi di accesso per IAM Identity Center, consulta Comprendere gli eventi di accesso a IAM Identity Center nella Guida per l'utente di IAM Identity Center.
- Per ulteriori informazioni su come CloudTrail registrare le diverse informazioni sull'identità degli utenti in IAM, consulta la sezione Registrazione delle chiamate IAM e AWS STS API nella Guida per l'utente. AWS CloudTrailAWS Identity and Access Management

AWS Sign-In supporta politiche basate sulle risorse e politiche di controllo delle risorse che consentono di limitare l'accesso alla console in base alla posizione della rete e all'identità principale. Per gli utenti root, la posizione di rete viene convalidata prima che venga visualizzata la richiesta della password. Per tutti i tipi principali, le politiche vengono valutate prima e dopo l'autenticazione. Per ulteriori informazioni, consulta Controllo dell'accesso alla console con policy basate sulle risorse e policy di controllo delle risorse.

Determina il tipo di utente

La modalità di accesso dipende dal tipo di AWS utente. Puoi gestirlo Account AWS come utente root, un utente IAM, un utente in IAM Identity Center o un'identità federata. Puoi utilizzare un profilo AWS Builder ID per accedere a determinati AWS servizi e strumenti. I diversi tipi di utente sono elencati di seguito.

Argomenti

- Utente root
- Utente IAM
- Utente IAM Identity Center
- Identità federata
- AWS Builder ID (utente)

Utente root

Chiamato anche proprietario dell'account o utente root dell'account. In qualità di utente root, hai accesso completo a tutti i AWS servizi e le risorse del tuo Account AWS. La prima volta che ne crei un Account AWS, inizi con un'identità di accesso singolo che ha accesso completo a tutti i AWS servizi e le risorse dell'account. Questa identità è l'utente root dell' AWS account. Puoi accedere come utente root utilizzando l'indirizzo e-mail e la password usati per creare l'account. Gli utenti root accedono con Console di gestione AWS. Per istruzioni dettagliate su come accedere, vedereAccedi Console di gestione AWS come utente root.

> **Important**
>
> Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Per ulteriori informazioni sulle identità IAM, incluso l'utente root, consulta Identità IAM (utenti, gruppi di utenti e ruoli).

Utente IAM

Un utente IAM è un'entità in cui crei. AWS Questo utente è un'identità interna a Account AWS cui sono concesse autorizzazioni personalizzate specifiche. Le tue credenziali utente IAM sono costituite da un nome e una password utilizzati per accedere a. Console di gestione AWS Per istruzioni dettagliate su come accedere, vediAccedi Console di gestione AWS come utente IAM.

Per ulteriori informazioni sulle identità IAM, incluso l'utente IAM, consulta Identità IAM (utenti, gruppi di utenti e ruoli).

Utente IAM Identity Center

Un utente IAM Identity Center è membro di AWS Organizations e può avere accesso a più Account AWS applicazioni tramite il tuo portale di AWS accesso. Se la loro azienda ha integrato Active Directory o un altro provider di identità con IAM Identity Center, gli utenti di IAM Identity Center possono utilizzare le proprie credenziali aziendali per accedere. IAM Identity Center può anche essere un provider di identità in cui un amministratore può creare utenti. Indipendentemente dal provider di identità, gli utenti di IAM Identity Center accedono utilizzando il portale di AWS accesso, che è un URL di accesso specifico per la loro organizzazione. Gli utenti di IAM Identity Center non possono accedere tramite l' Console di gestione AWS URL.

Gli utenti umani in IAM Identity Center possono ottenere l'URL del portale di AWS accesso da:

- Un messaggio dell'amministratore o del dipendente dell'help desk
- Un'e-mail AWS con un invito a iscriversi a IAM Identity Center

> **Tip**
>
> Tutte le e-mail inviate dal servizio IAM Identity Center provengono dall'indirizzo no-reply@signin.aws o no-reply@login.awsapps.com. Ti consigliamo di configurare il tuo sistema di posta elettronica in modo che accetti le e-mail da questi indirizzi e-mail dei mittenti e non le gestisca come posta indesiderata o spam.

Per istruzioni dettagliate su come accedere, consulta. Accedi al tuo AWS portale di accesso

> **Note**
>
> Ti consigliamo di aggiungere ai preferiti l'URL di accesso specifico della tua organizzazione per il tuo portale di AWS accesso in modo da potervi accedere in un secondo momento.

Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center?

Identità federata

Un'identità federata è un utente che può accedere utilizzando un provider di identità esterno (IdP) noto, come Login with Amazon, Facebook, Google o qualsiasi altro IdP compatibile con OpenID

Connect (OIDC). Con la federazione delle identità web, puoi ricevere un token di autenticazione e quindi scambiarlo con credenziali di sicurezza temporanee in AWS quella mappa con un ruolo IAM con le autorizzazioni per utilizzare le risorse del tuo. Account AWS Non accedi né accedi al Console di gestione AWS portale AWS . Al contrario, l'identità esterna in uso determina la modalità di accesso.

Per ulteriori informazioni, consulta Accedi come identità federata.

AWS Builder ID (utente)

Come utente AWS Builder ID, accedi specificamente al AWS servizio o allo strumento a cui desideri accedere. Un utente AWS Builder ID completa Account AWS quello che già possiedi o che desideri creare. Un AWS Builder ID ti rappresenta come persona e puoi utilizzarlo per accedere a AWS servizi e strumenti senza un. Account AWS Hai anche un profilo in cui puoi vedere e aggiornare le tue informazioni. Per ulteriori informazioni, consulta Accedi con ID Builder AWS.

AWS Builder ID è separato dall'abbonamento a AWS Skill Builder, un centro di apprendimento online in cui puoi imparare dagli AWS esperti e sviluppare competenze online sul cloud. Per ulteriori informazioni su AWS Skill Builder, consulta AWS Skill Builder.

Determina l'URL di accesso

Utilizza uno dei seguenti URL per accedere a AWS seconda del tipo di AWS utente che sei. Per ulteriori informazioni, consulta Determina il tipo di utente.

Argomenti

- Account AWS URL di accesso per utenti root
- AWS portale di accesso
- URL di accesso degli utenti IAM
- URL di identità federata
- AWS URL del Builder ID

Account AWS URL di accesso per utenti root

L'utente root accede a Console di gestione AWS dalla pagina di AWS accesso:. `https://console.aws.amazon.com/`

Questa pagina di accesso ha anche la possibilità di accedere come utente IAM.

AWS portale di accesso

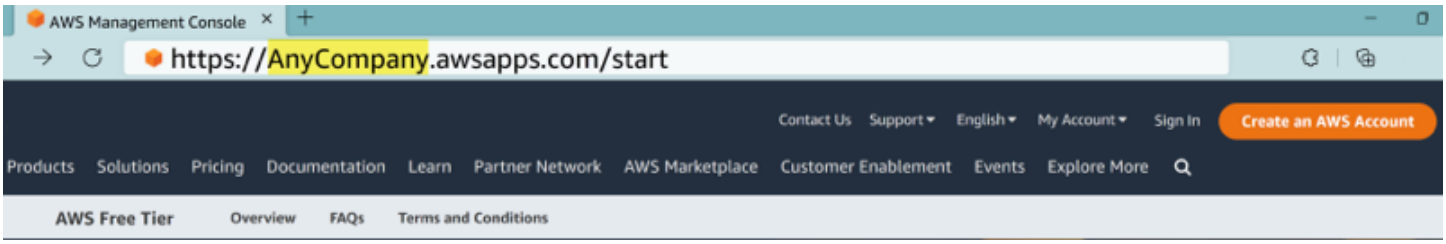
Il portale di AWS accesso è un URL di accesso specifico che consente agli utenti di IAM Identity Center di accedere al tuo account. Quando un amministratore crea l'utente in IAM Identity Center, l'amministratore sceglie se l'utente riceve un invito via e-mail a iscriversi a IAM Identity Center o un messaggio dall'amministratore o dal dipendente dell'help desk contenente una password monouso e AWS l'URL del portale di accesso. Il formato dell'URL di accesso specifico è simile ai seguenti esempi:

```
https://d-xxxxxxxxxx.awsapps.com/start
```

or

```
https://your_subdomain.awsapps.com/start
```

L'URL di accesso specifico varia perché l'amministratore può personalizzarlo. L'URL di accesso specifico potrebbe iniziare con la lettera D seguita da 10 numeri e lettere casuali. Il tuo sottodominio potrebbe essere utilizzato anche nell'URL di accesso e includere il nome della tua azienda, come nell'esempio seguente:



> **Note**
>
> Ti consigliamo di aggiungere ai preferiti l'URL di accesso specifico per il tuo portale di AWS accesso in modo da potervi accedere in un secondo momento.

Per ulteriori informazioni sul portale di AWS accesso, consulta Utilizzo del portale di AWS accesso.

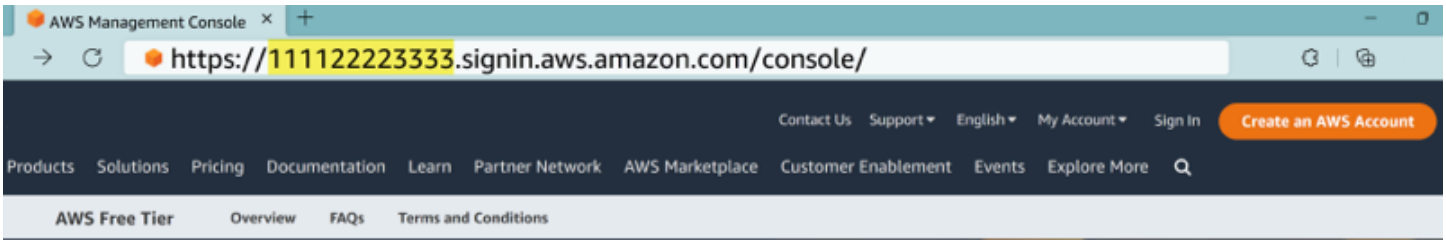
URL di accesso degli utenti IAM

Gli utenti IAM possono accedere a Console di gestione AWS con un URL di accesso utente IAM specifico. L'URL di accesso utente IAM combina il tuo Account AWS ID o alias e `signin.aws.amazon.com/console`

Un esempio di come appare l'URL di accesso di un utente IAM:

```
https://account_alias_or_id.signin.aws.amazon.com/console/
```

Se l'ID del tuo account è 111122223333, l'URL di accesso sarebbe:



Se riscontri problemi di accesso Account AWS con l'URL di accesso utente IAM, consulta Resilience in AWS Identity and Access Management per ulteriori informazioni.

URL di identità federata

L'URL di accesso per un'identità federata varia. L'identità esterna o l'Identity Provider (IdP) esterno determina l'URL di accesso per le identità federate. L'identità esterna potrebbe essere Windows Active Directory, Login with Amazon, Facebook o Google. Contatta il tuo amministratore per maggiori dettagli su come accedere come identità federata.

Per ulteriori informazioni sulle identità federate, consulta Informazioni sulla federazione delle identità web.

AWS URL del Builder ID

L'URL del tuo profilo AWS Builder ID è. https://profile.aws.amazon.com/ Quando usi il tuo AWS Builder ID, l'URL di accesso dipende dal servizio a cui desideri accedere. Ad esempio, per accedere ad Amazon CodeCatalyst, vai ahttps://codecatalyst.aws/login.

Domini da aggiungere all'elenco dei domini consentiti

Se si filtra l'accesso a AWS domini o endpoint URL specifici utilizzando una soluzione di filtraggio dei contenuti Web come firewall di nuova generazione (NGFW) o Secure Web Gateways (SWG), è necessario aggiungere i seguenti domini o endpoint URL agli elenchi consentiti della soluzione di filtraggio dei contenuti Web.

AWS Sign-In domini da inserire nella lista consentita

Se tu o la tua organizzazione implementate il filtraggio degli IP o dei domini, potrebbe essere necessario consentire l'uso di. Console di gestione AWS I seguenti domini devono essere accessibili sulla rete da cui si sta tentando di accedere a. Console di gestione AWS

- `[Region].signin.aws`
- `[Region].signin.aws.amazon.com`
- `signin.aws.amazon.com`
- `*.cloudfront.net`
- `opfcaptcha-prod.s3.amazonaws.com`

AWS Sign-In domini di amministrazione da inserire nella lista consentita

Se si configurano i controlli di accesso alla console utilizzando la AWS CLI, è necessario consentire l'elenco degli endpoint del piano di AWS Sign-In controllo. Questo endpoint gestisce l'amministrazione delle policy ed è distinto dai domini di accesso alla console descritti nella sezione precedente.

- `signin.[Region].api.aws`

  `[Region]`Sostituiscilo con la AWS regione che stai chiamando. Disponibile in tutte le regioni commerciali. Esempio: `signin.us-east-1.api.aws`.

Portale di accesso AWS domini da inserire nella lista consentita

Se si filtra l'accesso a AWS domini o endpoint URL specifici utilizzando una soluzione di filtraggio dei contenuti Web, ad esempio firewall di nuova generazione (NGFW) o Secure Web Gateways (SWG), è necessario aggiungere i seguenti domini o endpoint URL agli elenchi consentiti della soluzione di filtraggio dei contenuti Web. In questo modo è possibile accedere a. Portale di accesso AWS

I seguenti elenchi forniscono i domini IPv4 e dual-stack e gli endpoint URL da aggiungere agli elenchi di autorizzazione della soluzione di filtraggio dei contenuti Web. Per ulteriori informazioni sugli endpoint dual-stack, consulta Aggiorna firewall e gateway per consentire l'accesso alla Guida per l'utente di IAM Identity Center. Portale di accesso AWS

Elenco degli indirizzi consentiti per IPv4

- *[Directory ID or alias]*.awsapps.com
- *[IAM Identity Center instance ID]*.*[Region]*.portal.amazonaws.com
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *.sso-portal.*[Region]*.amazonaws.com

Dual-stack elenco di consentiti

- *[IAM Identity Center instance ID]*.portal.*[Region]*.app.aws
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.api.aws
- sso.*[Region]*.api.aws
- portal.sso.*[Region]*.api.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

ID Builder AWS domini da inserire nell'elenco dei domini consentiti

Se tu o la tua organizzazione implementate il filtraggio degli IP o dei domini, potrebbe essere necessario consentire i domini in elenco per creare e utilizzare un. ID Builder AWS I seguenti domini devono essere accessibili sulla rete da cui si sta tentando di accedere. ID Builder AWS

- `view.awsapps.com/start`
- `*.portal.*.app.aws`
- `*.aws.dev`
- `*.api.aws`
- `*.uis.awsstatic.com`
- `*.console.aws.a2z.com`
- `oidc.*.amazonaws.com`
- `oidc.*.api.aws`
- `*.sso.amazonaws.com`
- `*.sso.*.amazonaws.com`
- `*.sso-portal.*.amazonaws.com`
- `sso.*.api.aws`
- `*.signin.aws`
- `*.cloudfront.net`
- `opfcaptcha-prod.s3.amazonaws.com`
- `profile.aws.amazon.com`

Best practice di sicurezza per Account AWS amministratori

Se sei un amministratore di account che ne ha creato uno nuovo Account AWS, ti consigliamo di seguire i seguenti passaggi per aiutare i tuoi utenti a seguire le migliori pratiche di AWS sicurezza al momento dell'accesso.

1. Accedi come utente root per abilitare l'autenticazione a più fattori (MFA) e crea AWS un utente amministrativo in IAM Identity Center se non l'hai già fatto. Quindi, proteggi le tue credenziali root e non usarle per le attività quotidiane.
2. Accedi come Account AWS amministratore e configura le seguenti identità:

- Crea utenti con privilegi minimi per altri umani.
- Imposta credenziali temporanee per i carichi di lavoro.
- Crea chiavi di accesso solo per casi d'uso che richiedono credenziali a lungo termine.

3. Aggiungi le autorizzazioni per concedere l'accesso a tali identità. Puoi iniziare con le policy AWS gestite e passare alle autorizzazioni con privilegi minimi.

   - Aggiungi set di autorizzazioni agli utenti di AWS IAM Identity Center (successore di Single). AWS Sign-On
   - Aggiungi policy basate sull'identità ai ruoli IAM utilizzati per i carichi di lavoro.
   - Aggiungi policy basate sull'identità per gli utenti IAM per i casi d'uso che richiedono credenziali a lungo termine.
   - Per ulteriori informazioni sugli utenti IAM, consulta Best practice di sicurezza in IAM.

4. Salva e condividi informazioni suAccedi al Console di gestione AWS. Queste informazioni variano a seconda del tipo di identità che hai creato.
5. Mantieni aggiornati l'indirizzo e-mail dell'utente root e il numero di telefono di contatto dell'account principale per assicurarti di poter ricevere notifiche importanti relative all'account e alla sicurezza.

   - Modifica il nome dell'account, l'indirizzo email o la password per. Utente root dell'account AWS
   - Accedere o aggiornare il contatto principale dell'account.

6. Consulta le best practice di sicurezza in IAM per scoprire altre best practice di gestione delle identità e degli accessi.
7. Implementa controlli di accesso basati sulla rete: utilizza politiche Sign-in basate sulle risorse o politiche di controllo delle risorse (RCP) per limitare l'accesso alla console alle richieste provenienti da intervalli di indirizzi IP o VPC approvati. Per gli ambienti che utilizzano Console Private Access, configura le policy degli endpoint VPC per controllare a quali account è possibile accedere tramite gli endpoint (vedi Console Private Access). Insieme, le policy Sign-in basate sulle risorse, gli RCP e le policy degli endpoint VPC forniscono controlli di rete a più livelli in diversi punti di applicazione. Per gli utenti root, Sign-in le policy bloccano completamente la pagina delle credenziali in caso di tentativi di accesso da reti non autorizzate. AWS consiglia di configurare i principali esclusi per l'accesso di ripristino per prevenire il blocco dell'account, sebbene ciò sia facoltativo. Per ulteriori informazioni, consulta Controllo dell'accesso alla console con policy basate sulle risorse e policy di controllo delle risorse.

Accedi al Console di gestione AWS

Quando accedi Console di gestione AWS dall'URL di AWS accesso principale (https://console.aws.amazon.com/), devi scegliere il tipo di utente, utente root o utente IAM. Se non sei sicuro del tipo di utente che sei, consultaDetermina il tipo di utente.

L'utente root ha accesso illimitato all'account ed è associato alla persona che ha creato il Account AWS. L'utente root crea quindi altri tipi di utenti, come gli utenti IAM e utenti in Centro identità AWS IAM, e assegna loro le credenziali di accesso.

Un utente IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni personalizzate specifiche. Quando un utente IAM accede, può utilizzare un URL di accesso che include il proprio alias Account AWS or, ad esempio `https://account_alias_or_id.signin.aws.amazon.com/console/` anziché l'URL di AWS accesso principale. `https://console.aws.amazon.com/`

Puoi accedere a un massimo di 5 identità diverse contemporaneamente in un unico browser in. Console di gestione AWS Questi possono essere una combinazione di utenti root, utenti IAM o ruoli federati in account diversi o nello stesso account. Per maggiori dettagli, consulta Accesso a più account nella Guida introduttiva alla Console di gestione AWS .

Esercitazioni

- Accedi Console di gestione AWS come utente root
- Accedi Console di gestione AWS come utente IAM

Se non sei sicuro del tipo di utente che sei, consultaDetermina il tipo di utente.

Esercitazioni

- Accedi Console di gestione AWS come utente root
- Accedi Console di gestione AWS come utente IAM

Accedi Console di gestione AWS come utente root

La prima volta che crei un account Account AWS, inizi con un'unica identità di accesso con accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità si chiama utente Account AWS

root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account.

> **Important**
>
> Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Per accedere come utente root

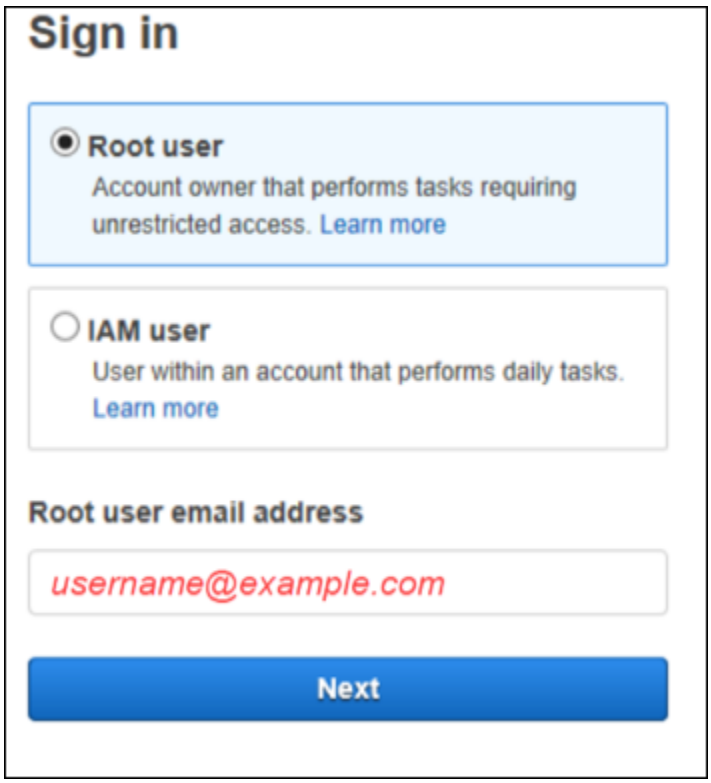
Puoi accedere come utente root mentre hai già effettuato l'accesso a un'altra identità in Console di gestione AWS. Per maggiori dettagli, consulta Accesso a più account nella Guida introduttiva alla Console di gestione AWS .

Account AWS managed using AWS Organizations potrebbe non avere credenziali utente root ed è necessario contattare un amministratore per eseguire azioni utente root nel proprio account membro. Se non riesci ad accedere come utente root, consultaRisoluzione dei problemi Account AWS problemi di accesso.

1. Apri il Console di gestione AWS filehttps://console.aws.amazon.com/.

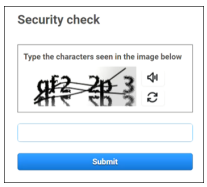
   > **Note**
   >
   > Se hai effettuato l'accesso in precedenza come utente IAM utilizzando questo browser, il tuo browser potrebbe invece visualizzare la pagina di accesso degli utenti IAM. Scegli Accedi utilizzando l'e-mail dell'utente root.

2. Scegli Utente root.



3. In Indirizzo e-mail dell'utente root, inserisci l'indirizzo e-mail associato all'utente root. Quindi, seleziona Avanti.
4. Se ti viene richiesto di completare un controllo di sicurezza, inserisci i caratteri visualizzati per continuare. Se non riesci a completare il controllo di sicurezza, prova ad ascoltare l'audio o ad aggiornare il controllo di sicurezza per un nuovo set di caratteri.

> **Tip**
>
> Digita i caratteri alfanumerici che vedi (o ascolti) in ordine senza spazi.



5. Inserisci la password.

6. Autenticazione con MFA. L'MFA viene applicata per impostazione predefinita all'utente root. Per gli utenti root di account indipendenti e membri, è necessario abilitare manualmente l'MFA, operazione fortemente consigliata. Per ulteriori informazioni, consulta Autenticazione a più fattori per utenti Account AWS root nella Guida per l'utente.AWS Identity and Access Management

   > **Tip**
   >
   > Come best practice in materia di sicurezza, consigliamo di rimuovere tutte le credenziali dell'utente root dagli account dei membri AWS dell'organizzazione per prevenire l'uso non autorizzato. Se scegli questa opzione, gli account membro non possono accedere come utente root, eseguire il ripristino della password o configurare l'MFA. In questo caso, solo l'amministratore dell'account di gestione può eseguire un'operazione che richiede le credenziali dell'utente root in un account membro. Per i dettagli, consulta Gestire centralmente l'accesso root per gli account dei membri nella Guida per l'AWS Identity and Access Management utente.

7. Selezionare Sign in (Accedi). Console di gestione AWS Appare.

Dopo l'autenticazione, Console di gestione AWS si apre la home page della console.

Informazioni aggiuntive

Se desideri maggiori informazioni sull'utente Account AWS root, consulta le seguenti risorse.

- Per una panoramica dell'utente root, vedi utente Account AWS root.
- Per i dettagli sull'utilizzo dell'utente root, vedere Uso dell'utente Account AWS root.
- Per step-by-step istruzioni su come reimpostare la password dell'utente root, vedereHo dimenticato la password dell'utente root per il mio Account AWS.

Accedi Console di gestione AWS come utente IAM

Un utente IAM è un'identità creata all'interno di un utente Account AWS che dispone del permesso di interagire con AWS le risorse. Gli utenti IAM accedono utilizzando l'ID o l'alias dell'account, il nome utente e una password. I nomi utente IAM sono configurati dall'amministratore. I nomi utente IAM possono essere nomi descrittivi*Zhang*, ad esempio, o indirizzi e-mail come*zhang@example.com*. I nomi utente IAM non possono includere spazi, ma possono includere lettere maiuscole e minuscole, numeri e simboli`+ = , . @ _ -`.

> **Tip**
>
> Se il tuo utente IAM ha abilitato l'autenticazione a più fattori (MFA), devi avere accesso al dispositivo di autenticazione. Per i dettagli, consulta Utilizzo dei dispositivi MFA con la pagina di accesso IAM.

Accesso come utente IAM

Puoi accedere come utente IAM mentre hai già effettuato l'accesso a un'altra identità in Console di gestione AWS. Per maggiori dettagli, consulta Accesso a più account nella Guida introduttiva alla Console di gestione AWS .

1. Apri il Console di gestione AWS filehttps://console.aws.amazon.com/.
2. Viene visualizzata la pagina di accesso principale. Inserisci l'ID dell'account (12 cifre) o l'alias, il nome utente IAM e la password.

> **Note**
>
> Potresti non dover inserire l'ID o l'alias del tuo account se hai già effettuato l'accesso come utente IAM con il tuo browser attuale o se stai utilizzando l'URL di accesso del tuo account.

3. Selezionare Sign in (Accedi).
4. Se l'MFA è abilitata per il tuo utente IAM, AWS richiede di confermare la tua identità con un autenticatore. Per ulteriori informazioni, vedere Utilizzo dell'autenticazione a più fattori (MFA) in. AWS

Dopo l'autenticazione, Console di gestione AWS si apre la home page della console.

Informazioni aggiuntive

Se desideri maggiori informazioni sugli utenti IAM, consulta le seguenti risorse.

- Per una panoramica di IAM, consulta What is Identity and Access Management?
- Per informazioni dettagliate sull' AWS account IDs, consulta L'ID AWS dell'account e il suo alias.
- Per step-by-step istruzioni su come reimpostare la password utente IAM, consultaHo dimenticato la mia password utente IAM per il mio Account AWS.

Controllo dell'accesso alla console con policy basate sulle risorse e policy di controllo delle risorse

> **Important**
>
> L'accesso alla console è abilitato per impostazione predefinita. AWS Sign-In consente inizialmente l'accesso illimitato alla console. Per aggiungere restrizioni, abilita la configurazione dell'autorizzazione della console per il tuo account o la tua organizzazione. Le istruzioni di autorizzazione delle risorse create non hanno effetto finché non abiliti l'autorizzazione della console. Per informazioni, consulta Guida introduttiva al controllo degli accessi alla console utilizzando le policy delle risorse.

AWS Sign-In supporta politiche basate sulle risorse e politiche di controllo delle risorse (RCP) per controllare l'accesso a. AWS Sign-In Utilizza queste politiche per verificare l'identità dell'utente e la posizione della rete durante Console di gestione AWS l'accesso, prima, durante e dopo l'autenticazione. Per gli utenti root, queste politiche convalidano la posizione di rete e l'identità dell'utente prima che inizi la raccolta delle credenziali. Le credenziali possono essere inserite solo quando l'accesso proviene dalle reti previste.

AWS Sign-In politiche basate sulle risorse:

- Applica ai singoli account. AWS
- Consenti agli amministratori degli account di limitare l'accesso alla console in base ai parametri di rete e alle identità principali.

Politiche di controllo delle risorse (RCP):

- Applica a livello di organizzazione tramite AWS Organizations.
- Fornisci una governance centralizzata su tutti gli account dei membri.

Entrambi i tipi di policy verificano l'accesso prima dell'autenticazione. Ciò impedisce ai principali destinatari di accedere alla pagina di accesso da reti impreviste.

Queste politiche non sostituiscono le politiche basate sull'identità IAM, che continuano ad essere applicate.

> **Note**
>
> Per una documentazione completa sulle politiche di controllo delle risorse, inclusa la configurazione e la gestione a livello di organizzazione, consulta le policy di controllo delle risorse nella AWS Organizations User Guide. Questa sezione si concentra principalmente sulle politiche basate sulle risorse. AWS Sign-In

AWS Sign-In le politiche e gli RCP basati sulle risorse si applicano ai seguenti metodi di autenticazione:

- Console di gestione AWS— Accesso diretto tramite la pagina di accesso della console.
- AWS IAM Identity Center: accesso alla console tramite IAM Identity Center.
- Provider di identità federati: Sign-in tramite federazione SAML o OIDC.
- Applicazioni integrate con AWS Sign-In: Amazon Connect, Amazon QuickSight, AWS Health Dashboard, Amazon AppStream, Amazon Lightsail, AWS IQ.

Questi controlli non si applicano all'accesso programmatico tramite chiavi di accesso (AWS SDK o chiamate API firmate con SigV4).

In che modo AWS Sign-In valuta le politiche basate sulle risorse

AWS Sign-In valuta le politiche basate sulle risorse o le politiche di controllo delle risorse (RCP) applicabili in due momenti durante l'accesso alla console: prima dell'autenticazione (fase di preautenticazione) e dopo l'autenticazione riuscita (fase post-autenticazione). Ogni valutazione verifica le chiavi di condizione definite nella politica. Le chiavi disponibili dipendono dalla fase e dall'azione. Per informazioni dettagliate, vedi Chiavi di condizione supportate.

> **Note**
>
> Per l'accesso come utente root, un tentativo di accesso da reti impreviste viene bloccato prima che venga visualizzata la richiesta della password. Ciò impedisce l'invio di credenziali da reti impreviste.

Dopo l'autenticazione, la valutazione considera anche le politiche basate sull'identità del principale. Una policy IAM che nega l'azione di accesso pertinente può impedire la concessione della sessione della console, anche quando sono soddisfatte le condizioni di rete.

Azioni supportate

AWS Sign-In le politiche relative alle risorse (politiche basate sulle risorse e RCP) supportano le seguenti azioni:

`signin:Authenticate`

Si tratta di un'azione di sola valutazione (non richiamabile) che viene valutata quando viene ricevuta una richiesta di accesso. Si tratta di un controllo di preautenticazione e viene eseguito quando il principale inserisce le credenziali nella pagina di accesso (utente root, utente IAM) o avvia l'accesso alla console utilizzando le credenziali di un provider di identità o AWS STS (utente federato, ruolo).

Chiavi di condizione supportate:,,,,. `aws:SourceIp` `aws:SourceVpc` `aws:SourceVpce` `aws:VpcSourceIp` `aws:RequestedRegion` `signin:PrincipalArn`

Principal-based le chiavi di condizione globali (`aws:PrincipalArn`,`aws:PrincipalAccount`) non sono disponibili per questa azione perché l'identità dell'utente non è stata ancora confermata.

`signin:AuthorizeOAuth2Access`

Utilizzato per la generazione del codice di autorizzazione OAuth. Dopo una corretta autenticazione, questa azione viene attivata quando il sistema genera un codice di autorizzazione OAuth. A questo punto, l'utente è autenticato e sono disponibili le chiavi di condizione basate sui principali.

Chiavi di condizione supportate:`aws:SourceIp`,`aws:SourceVpc`,,`aws:SourceVpce`,`aws:VpcSourceIp`,`aws:Requested` `aws:PrincipalArn` `aws:PrincipalAccount`

`signin:CreateOAuth2Token`

Questa azione post-autenticazione viene utilizzata per la creazione e lo scambio di token OAuth. Questa azione viene attivata quando si riscattano i codici di autorizzazione per i token di accesso, si aggiornano i token o si eseguono operazioni di scambio di token. Principal-based i tasti di condizione sono disponibili durante questa fase.

Chiavi di condizione supportate: `aws:SourceIp`
`aws:SourceVpcaws:SourceVpce,aws:VpcSourceIp,,aws:RequestedRegion,aws:PrincipalAr`

> **Important**
>
> Quando crei AWS Sign-In policy (policy basate sulle risorse o RCP), includi tutte e tre le azioni della policy, in una dichiarazione di pre-autenticazione e `signin:Authenticate` `signin:Authorize0Auth2Access` in una dichiarazione post-autenticazione. `signin:Create0Auth2Token` L'accesso alla console utilizza OAuth 2.0, che esegue tutte e tre le azioni in sequenza. Se la policy omette un'azione, la fase corrispondente non è protetta. Per le azioni relative alla policy degli endpoint VPC, tra cui, `signin:CreateAccount` consulta l'accesso privato alla Console di gestione AWS.

Chiavi di condizione supportate

AWS Sign-In supporta le seguenti chiavi di condizione nelle politiche basate sulle risorse e nelle politiche di controllo delle risorse (RCP). Usa questi tasti per controllare l'accesso alla console in base alla posizione della rete e all'identità principale:

- Network-based (tutte le azioni):`aws:SourceIp`,`aws:SourceVpc`,`aws:SourceVpce`,`aws:VpcSourceIp`,`aws:RequestedRegi`
- Identity-based (azioni successive all'autenticazione):`aws:PrincipalArn`,`aws:PrincipalAccount`.
- Service-specific (solo preautenticazione):. `signin:PrincipalArn`

Per le regole di utilizzo dettagliate, la compatibilità degli operatori, le restrizioni sulle combinazioni e la matrice di disponibilità per azione, vedereAWS Sign-In riferimento alle chiavi di condizione.

Guida introduttiva al controllo degli accessi alla console utilizzando le policy delle risorse

Prerequisiti

- AWS CLI installata e configurata.

- Autorizzazioni IAM appropriate (vediAWS politica gestita: AWSSignInResourcePolicyManagement).
- Perimetri di rete identificati (intervalli IP, VPC o endpoint VPC).
- Principali esclusi designati per mantenere l'accesso (consigliato ma facoltativo).
- Se la rete utilizza il filtro in uscita, inserite nella lista consentita l'endpoint del piano di AWS Sign-In controllo (vedi). AWS Sign-In domini di amministrazione da inserire nella lista consentita

> **Important**
>
> Prima di abilitare l'autorizzazione della console in produzione, AWS consiglia di configurare almeno un principale escluso per mantenere l'accesso al ripristino di emergenza.
> Tutti i principali, incluso l'utente root, sono soggetti alla politica a meno che non siano esplicitamente esclusi. I principali esclusi sono facoltativi, ma la loro omissione aumenta il rischio di blocco dell'account se le condizioni della rete cambiano inaspettatamente.

Specificare `--region us-east-1` per tutte le operazioni di scrittura sulle politiche. AWS Sign-In AWS replica le politiche a livello globale da questa regione. Le operazioni di lettura possono riguardare qualsiasi regione.

Fase 1: Creare dichiarazioni di autorizzazione alle risorse

Crea dichiarazioni di autorizzazione che definiscono i controlli di accesso. Tutte le operazioni di scrittura richiedono `--region us-east-1` (il AWS Sign-In servizio accetta modifiche alle politiche solo in questa regione). I parametri rimanenti (`--source-vpc--source-ip,--requested-region,,--excluded-principal`) definiscono le condizioni della politica. Ad esempio, `--requested-region us-west-2` aggiunge una condizione che limita l'accesso all'endpoint di accesso regionale us-west-2.

Esempio: limita l'accesso al VPC aziendale:

```
aws signin put-resource-permission-statement \
  --source-vpc vpc-0abc123def456789 \
  --requested-region us-west-2 \
  --excluded-principal "arn:aws:iam::123456789012:user/EmergencyAdmin" \
  --client-token unique-request-id-12345 \
  --region us-east-1
```

Esempio: limita l'accesso a un intervallo IP specifico:

```
aws signin put-resource-permission-statement \
  --source-ip "IP_ADDRESS" \
  --excluded-principal "arn:aws:iam::123456789012:role/BreakGlassRole" \
  --region us-east-1
```

> **Note**
>
> Il `--excluded-principal` parametro indica un principale escluso che aggira le restrizioni di rete, preservando l'accesso di emergenza in caso di modifica delle condizioni della rete.

Passaggio 2: abilitare la configurazione dell'autorizzazione della console

Il passaggio seguente attiva l'applicazione delle policy per la procedura di accesso alla console sull'account o sull'organizzazione. Le istruzioni di autorizzazione delle risorse possono essere create in qualsiasi momento, ma non vengono valutate finché non viene abilitata l'autorizzazione della console.

> **Warning**
>
> L'attivazione dell'autorizzazione alla console può bloccare i principali se le condizioni di rete non sono configurate correttamente o se una policy di controllo dei servizi (SCP) o una politica di controllo delle risorse (RCP) esistente nega le azioni. AWS Sign-In Prima di abilitare l'autorizzazione della console, verifica che le istruzioni di autorizzazione siano corrette e rimuovi o modifica eventuali SCP o RCP che negano o. `signin:Authenticate` `signin:AuthorizeOAuth2Access` `signin:CreateOAuth2Token`

Per gli account autonomi:

```
aws signin put-console-authorization-configuration \
  --target-id <your-aws-account-id> \
  --region us-east-1
```

Per AWS Organizations:

```
aws signin put-console-authorization-configuration \
  --target-id <your-aws-organization-id> \
```

```
  --region us-east-1
```

Verifica la configurazione:

```
aws signin get-console-authorization-configuration \
  --target-id <your-target-id> \
  --region <your-region>
```

Elimina la configurazione di autorizzazione della console:

```
aws signin delete-console-authorization-configuration \
  --target-id <your-target-id> \
  --region us-east-1
```

Fase 3: Verifica la tua politica

Elenca tutte le dichiarazioni di autorizzazione:

```
aws signin list-resource-permission-statements \
  --max-results 50 \
  --region <your-region>
```

Recupera la politica consolidata completa:

```
aws signin get-resource-policy \
  --region <your-region>
```

Il `get-resource-policy` comando restituisce la politica completa basata sulle risorse composta da tutte le dichiarazioni di autorizzazione. Esamina questa politica per confermare che rifletta i controlli di accesso previsti prima di testare l'accesso alla console.

Disponibilità regionale

Le API di autorizzazione della console sono disponibili in tutte le regioni AWS commerciali. Puoi chiamare queste API da qualsiasi regione in cui operi.

> **Important**
>
> Le operazioni di scrittura (`put-console-authorization-configurationput-resource-permission-statement`,`delete-console-authorization-`

`configuration`,,`delete-resource-permission-statement`) devono essere eseguite nella `us-east-1` regione. Le politiche create `us-east-1` vengono replicate automaticamente a livello globale. Le operazioni di lettura (`get-console-authorization-configuration`list-resource-permission-statements,,`get-resource-policy`) possono essere eseguite da qualsiasi regione.

Comprensione della struttura delle politiche

AWS Sign-In le policy contengono due dichiarazioni che proteggono diverse fasi del flusso di accesso alla console:

- Pre-authentication dichiarazione (Azione:**`signin:Authenticate`**): valutata quando viene ricevuta la richiesta di accesso, prima del completamento dell'autenticazione. La chiave globale non `aws:PrincipalArn` è disponibile in questa fase perché l'identità del principale non è confermata. In questa fase `signin:PrincipalArn` è possibile esentare i principali specifici dalle restrizioni di rete. Network-based le chiavi delle condizioni sono disponibili per la valutazione in questa fase.
- Post-authentication dichiarazione (Azione:**`signin:AuthorizeOAuth2Access`**,**`signin:CreateOAuth2Token`**): valutata dopo l'autenticazione, durante lo scambio di token OAuth. Viene utilizzato `aws:PrincipalArn` per esentare principi specifici. Tutte le chiavi di condizione basate sulla rete e sull'identità sono disponibili per la valutazione in questa fase.

Entrambe le istruzioni sono obbligatorie perché l'accesso alla console utilizza OAuth 2.0, che esegue tutte e tre le azioni in sequenza. Una politica con una sola istruzione lascia l'altra fase non protetta. `signin:PrincipalArn`supporta i tipi di utente root, utente IAM e ruoli principali. `aws:PrincipalArn`supporta tutti i tipi principali (utente root, utente IAM, utente federato, ruolo).

Esempi di policy

Esempio 1: RCP con perimetro di rete e principali esclusi

La seguente politica di controllo delle risorse (RCP) Console di gestione AWS nega l'accesso dall'esterno della rete aziendale a tutti gli account dell'organizzazione. I principali esclusi designati sono esentati dall'accesso di emergenza. Poiché gli ID VPC sono unici solo all'interno di una regione, la policy include una terza dichiarazione che associa VPC-based l'accesso alla regione prevista.

La `EnforceNetworkPerimeterPreAuth` dichiarazione viene utilizzata `signin:PrincipalArn` per esentare i principali esclusi durante la fase di preautenticazione. La `EnforceNetworkPerimeterPostAuth` dichiarazione utilizza `aws:PrincipalArn` per esentare i principali esclusi dopo l'autenticazione. L'`EnforceSourceVPCRegion`istruzione garantisce che la regione richiesta corrisponda alla regione VPC, limitando l'accesso alla regione prevista per il VPC specificato.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceNetworkPerimeterPreAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root",
            "arn:aws:iam::777788889999:user/EmergencyUser",
            "arn:aws:iam::777788889999:role/OrgBreakGlassRole"
          ]
        },
        "NotIpAddressIfExists": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringNotEquals": {
          "aws:SourceVpc": "<my-vpc>"
        }
      }
    },
    {
      "Sid": "EnforceNetworkPerimeterPostAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:root",
```

```
            "arn:aws:iam::444455556666:root",
            "arn:aws:iam::777788889999:user/EmergencyUser",
            "arn:aws:iam::777788889999:role/OrgBreakGlassRole"
          ]
        },
        "NotIpAddressIfExists": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringNotEquals": {
          "aws:SourceVpc": "<my-vpc>"
        }
      }
    },
    {
      "Sid": "EnforceSourceVPCRegion",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "signin:Authenticate",
        "signin:CreateOAuth2Token",
        "signin:AuthorizeOAuth2Access"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceVpc": "<my-vpc>"
        },
        "StringNotEqualsIfExists": {
          "aws:RequestedRegion": "<my-vpc-region>"
        }
      }
    }
  ]
}
```

Questa politica:

- Nega l'accesso alla pagina di accesso a meno che la richiesta non provenga dall'intervallo IP aziendale o dal VPC aziendale. Gli account root e gli utenti IAM esclusi sono esentati tramite (preautenticazione). `signin:PrincipalArn`

- Nega lo scambio di token OAuth a meno che non provenga dall'intervallo IP aziendale o dal VPC. Gli account root, gli utenti IAM e i ruoli esclusi sono esentati tramite `aws:PrincipalArn` (chiave globale post-autenticazione).
- Se una richiesta proviene dal VPC specificato ma la Regione non corrisponde, l'accesso viene negato. AWS Gli ID VPC sono unici all'interno di una regione e lo stesso ID VPC può esistere in diverse regioni.
- Si applica a livello globale in tutta la tua AWS Organization se configurata come RCP.

Esempio 2: Resource-based policy di IP-based accesso con preside escluso

La seguente politica basata sulle risorse nega l'accesso dalla console a tutti i principali che effettuano richieste al di fuori dell'intervallo IP specificato, con l'esenzione per un principale escluso. La policy contiene due istruzioni: una dichiarazione di pre-autenticazione che utilizza la `signin:PrincipalArn` chiave specifica del servizio e un'istruzione post-autenticazione che utilizza la chiave globale. `aws:PrincipalArn`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": "<excluded-principal-arn>"
        },
        "NotIpAddress": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringEquals": {
          "aws:ResourceAccount": "<my-aws-account-id>"
        }
      }
    },
    {
      "Effect": "Deny",
```

```
      "Principal": { "AWS": "*" },
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": "<excluded-principal-arn>"
        },
        "NotIpAddress": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringEquals": {
          "aws:ResourceAccount": "<my-aws-account-id>"
        }
      }
    }
  ]
}
```

Questa politica:

- Nega l'accesso a tutti i principali a meno che non si connettano dall'intervallo IP. `<my-corporate-cidr>`
- Esonera il principale escluso dalle restrizioni di rete utilizzando `signin:PrincipalArn` (preautenticazione) e `aws:PrincipalArn` (post-autenticazione).
- Si applica solo all'account specifico in cui è configurata la politica basata sulle risorse (identificata da). `<my-aws-account-id>`

Best practice

Configura i principali esclusi per l'accesso al ripristino di emergenza

AWS consiglia di configurare almeno un utente escluso prima di applicare le politiche di autorizzazione della console in produzione. Nella fase di preautenticazione, la chiave `signin:PrincipalArn` condizionale esenta l'utente root, l'utente IAM e i responsabili del ruolo. Nella fase successiva all'autenticazione, la chiave `aws:PrincipalArn` condizionale esenta tutti i tipi principali (utente root, utente IAM, utente federato, ruolo).

I principali esclusi sono facoltativi, ma la loro omissione aumenta il rischio di blocco dell'account se le condizioni di rete cambiano in modo imprevisto o se le politiche non sono configurate correttamente.

Passaggi di configurazione principali esclusi consigliati:

1. Crea un ruolo IAM escluso (ad esempio,). `BreakGlassRole`
2. Per i ruoli esclusi, richiedi l'autenticazione a più fattori nella policy di fiducia dei ruoli.
3. Concedi all'identità esclusa solo le autorizzazioni minime necessarie per il ripristino di emergenza.
4. Includete l'ARN principale escluso nelle dichiarazioni di policy di pre-authentication (`signin:PrincipalArn`) e post-authentication (`aws:PrincipalArn`).
5. Documenta la procedura di ripristino e conservala in modo sicuro all'esterno. AWS
6. Verifica periodicamente l'accesso principale escluso per confermare che funzioni quando necessario.

Mantieni i percorsi di accesso di ripristino

Oltre al principio escluso sopra descritto, assicurati che siano disponibili metodi di accesso alternativi nel caso in cui le politiche di autorizzazione della console blocchino l'accesso in modo imprevisto:

- Role-based accesso programmatico: le politiche di autorizzazione della console si applicano solo all'accesso interattivo alla console. Non si applicano alle richieste API firmate con SigV4. Se disponi di un accesso programmatico (ad esempio, chiavi di accesso esistenti, un ruolo tra più account), utilizzalo per richiamare `signin:DeleteConsoleAuthorizationConfiguration` e rimuovere la politica di restrizione. Le credenziali devono includere `signin:DeleteConsoleAuthorizationConfiguration` l'autorizzazione (inclusa nella politica gestita). `AWSSignInResourcePolicyManagement` AWS consiglia credenziali temporanee rispetto alle chiavi di accesso utente IAM a lungo termine. Per gli account membro, gli amministratori degli account di gestione possono assumere `OrganizationAccountAccessRole` nell'account membro (`aws sts assume-role`) di ottenere queste credenziali temporanee.
- AWS support recovery: mantieni aggiornati l'email e il numero di telefono dell'account utente root. Se l'accesso principale escluso e l'accesso programmatico non sono entrambi disponibili, AWS Support può fornire un collegamento al portale di ripristino dopo la verifica dell'identità. Per il processo di ripristino completo, L'accesso al mio account è bloccato dopo aver abilitato l'autorizzazione della console consulta la sezione.

Esegui il test prima dell'implementazione in produzione

AWS consiglia di non applicare RCP restrittivi alla radice dell'organizzazione senza aver testato a fondo l'impatto che la policy ha sugli account. Create invece un'unità organizzativa in cui spostare i vostri account uno alla volta, o almeno in piccoli numeri, per assicurarvi di non impedire inavvertitamente agli utenti di accedere agli account chiave.

Flusso di lavoro di test:

1. Crea un'unica dichiarazione di autorizzazione con le restrizioni di rete principali.
2. Abilita l'autorizzazione della console in un account non di produzione.
3. Verifica l'accesso alla console sia dalle reti consentite che da quelle negate.
4. Esamina CloudTrail i log di Amazon per confermare il comportamento di valutazione delle politiche.
5. Verifica l'accesso utilizzando il tuo principale escluso.
6. Espandi gradualmente a reti e account aggiuntivi.
7. Monitora prima di applicarlo negli account di produzione.

Progetta con una difesa approfondita

Utilizza le politiche AWS Sign-In basate sulle risorse e le politiche di controllo delle risorse come un unico livello all'interno di una strategia di sicurezza più ampia. AWS Sign-In le policy limitano l'accesso alla console in base alla posizione della rete e all'identità principale. Combinale con altri tipi di policy per creare controlli di accesso completi:

- AWS Sign-In policy (policy basate sulle risorse e RCP): limita l'accesso alla console in base alla posizione della rete e all'identità principale prima, durante e dopo l'autenticazione.
- Politiche IAM: controlla le azioni che gli utenti possono eseguire dopo l'accesso.
- Policy di controllo dei servizi (SCP): applica barriere di autorizzazione a livello di organizzazione a tutti i responsabili.
- Policy degli endpoint VPC: controlla a quali servizi e account è possibile accedere tramite gli endpoint VPC.

Monitora e verifica continuamente

AWS CloudTrail registra automaticamente tutte le valutazioni AWS Sign-In delle politiche e le modifiche alla configurazione. Visualizza questi eventi nella cronologia degli CloudTrail eventi per un massimo di 90 giorni. Per una conservazione più lunga, distribuisci eventi ad Amazon S3 creando un percorso (vedi Creazione di un percorso). Per gli avvisi in tempo reale, crea EventBridge regole Amazon che corrispondano AWS Sign-In agli eventi, configura il percorso da inviare a un gruppo di log CloudWatch Logs per gli allarmi basati su filtri metrici o inoltra gli eventi alla tua soluzione SIEM esistente.

Casi d'uso

Applicazione del perimetro di rete

Limita l'accesso alla console ai VPC aziendali o agli intervalli IP approvati. Utilizza politiche basate sulle risorse per account individuali o politiche di controllo delle risorse (RCP) per applicarle a livello di organizzazione per garantire che gli utenti possano accedere solo da posizioni di rete affidabili, impedendo l'accesso non autorizzato da reti pubbliche o non attendibili.

Scenario di esempio: un'azienda richiede che tutti gli accessi alla console provengano dalla propria rete aziendale o da VPC approvati. AWS Configurano una politica basata sulle risorse per un singolo account, o un RCP all'interno dell'organizzazione, che nega l'accesso da tutte le altre reti mantenendo al contempo l'accesso per il ripristino di emergenza per gli amministratori di emergenza.

Requisiti di conformità

Soddisfa i requisiti normativi per i controlli degli accessi basati sulla rete. Molti framework di conformità richiedono alle organizzazioni di limitare l'accesso ai sistemi sensibili in base alla posizione della rete. AWS Sign-In le politiche forniscono controlli verificabili e applicabili che dimostrano la conformità a questi requisiti.

Scenario di esempio: una società di servizi finanziari deve rispettare le normative che richiedono l'accesso alla console solo da reti approvate. Utilizzano gli RCP per applicare le restrizioni di rete a livello di organizzazione e conservare AWS CloudTrail i log come prova di conformità.

Multi-account governance

Implementa policy di accesso alla console coerenti in AWS Organizations. Usa gli RCP per applicare le restrizioni di rete standard su tutti gli account dei membri, garantendo un livello di sicurezza coerente senza richiedere una configurazione a livello di account individuale.

Scenario di esempio: un'azienda con più di 100 AWS account utilizza gli RCP per applicare una policy che richiede che tutti gli accessi alla console provengano dagli endpoint VPC all'interno dell'organizzazione, confermando controlli di rete coerenti su tutti gli account.

Third-party controllo degli accessi

Concedi l'accesso temporaneo alla console a partner o appaltatori da reti specifiche. Le organizzazioni possono creare un accesso alla console limitato nel tempo e limitato alla rete per parti esterne senza compromettere il livello di sicurezza generale.

Scenario di esempio: un'azienda deve concedere a una società di consulenza l'accesso temporaneo alla console. Creano una policy basata sulle risorse che consente l'accesso solo dagli intervalli IP noti della società di consulenza e solo per i ruoli IAM assegnati ai consulenti.

Limita l'accesso alla console a principali specifici

Consenti solo a un insieme definito di principali di accedere a e nega tutti gli altri Console di gestione AWS, indipendentemente dalla posizione della rete. Ciò è utile per i clienti che non utilizzano endpoint VPC e desiderano restrizioni della console basate sull'identità. I principali a cui viene negato l'accesso alla console mantengono l'accesso programmatico; AWS Sign-In le policy limitano solo l'accesso alla console e solo i principali esentati possono accedere.

Scenario di esempio: un'azienda desidera che solo i suoi amministratori utilizzino la console. Configurano un RCP che nega l'accesso alla console per tutti i principali server ad eccezione degli ARN principali dell'amministratore. Un ruolo di istanza Amazon EC2 con credenziali valide non può accedere alla console, perché non è un principale esente, anche se mantiene le sue autorizzazioni programmatiche. Questo risolve il caso comune in cui le credenziali del ruolo di istanza vengono utilizzate per l'accesso alla console.

Risoluzione dei problemi di controllo dell'accesso alla console

Non riesco ad accedere a causa delle condizioni di rete nelle politiche Sign-in basate sulle risorse

È possibile che venga visualizzato uno dei seguenti messaggi di errore quando l'accesso viene negato da una politica: AWS Sign-In

- «Le informazioni di autenticazione non sono corrette. Riprova.» (negazione della preautenticazione in base a una politica basata sulle risorse)

- «Autenticazione fallita Richiesta non valida» (negazione della preautenticazione da parte di RCP)
- «Autenticazione non riuscita: per accedere a questo account, accedi da una rete diversa o contatta l'amministratore per ulteriori informazioni» (rifiuto dopo l'autenticazione)

Se riscontri uno di questi errori e ritieni che il tuo accesso debba essere consentito, contatta l'amministratore AWS . Possono esaminare CloudTrail i registri `ConsoleLogin` degli eventi con `errorMessage` «Autorizzazione negata a causa di una politica basata sulle risorse» o «Autorizzazione negata a causa di una politica di controllo delle risorse» per identificare a quale dichiarazione politica è stato negato l'accesso.

Possibili cause:

- L'indirizzo IP di origine non rientra nell'intervallo CIDR consentito.
- Non sei connesso al VPC o all'endpoint VPC richiesto.
- Stai accedendo a un endpoint di accesso regionale che non corrisponde alla regione prevista nella policy.
- L'ARN principale non è elencato correttamente tra i principali esclusi della politica.
- La politica è stata aggiornata di recente e la modifica non è stata ancora replicata a livello globale.

Risoluzione:

- Verifica di essere connesso alla rete aziendale o alla VPN.
- Verifica che stai accedendo tramite l'endpoint VPC corretto se sono configurate le restrizioni basate sugli endpoint VPC.
- Contatta l' AWS amministratore per verificare la configurazione delle policy e confermare quali reti sono autorizzate.
- Se sei configurato come principale escluso, verifica che il tuo ARN principale sia configurato correttamente nell'elenco dei principali esclusi.
- Se di recente sono state apportate modifiche alle policy, attendi qualche minuto per il completamento della replica globale.

Per gli amministratori che diagnosticano questo problema:

- AWS CloudTrail Esamina i registri degli eventi di valutazione delle politiche per identificare a quale dichiarazione politica è stato negato l'accesso.

- Utilizzare `aws signin get-resource-policy` per esaminare la configurazione corrente delle politiche.
- Verifica che la posizione di rete dell'utente corrisponda alle condizioni della politica.
- Verifica che i principali esclusi siano configurati correttamente se l'utente deve essere esentato dalle restrizioni di rete.

L'accesso al mio account è bloccato dopo aver abilitato l'autorizzazione della console

Se hai configurato l'autorizzazione della console e non riesci più ad accedere al tuo account, potresti non aver configurato i principali esclusi prima di applicare la politica.

Esistono diversi percorsi per riottenere l'accesso, a seconda del tipo di account e delle credenziali disponibili.

Opzione 1: utilizzare l'accesso programmatico (AWS CLI o SDK)

Le politiche di autorizzazione della console si applicano solo all'accesso interattivo alla console. Non si applicano alle richieste API firmate con SigV4. Se disponi di un accesso programmatico (ad esempio, chiavi di accesso esistenti, un ruolo tra più account), utilizzalo per richiamare `signin:DeleteConsoleAuthorizationConfiguration` e rimuovere la politica di restrizione. Le credenziali utilizzate devono disporre dell'autorizzazione per la chiamata. `signin:DeleteConsoleAuthorizationConfiguration` La politica `AWSSignInResourcePolicyManagement` gestita include questa autorizzazione. AWS consiglia credenziali temporanee anziché chiavi di accesso utente IAM a lungo termine. Per gli account membro, gli amministratori degli account di gestione possono assumere `OrganizationAccountAccessRole` nell'account membro di ottenere credenziali temporanee. Questo ruolo non viene creato automaticamente negli account che sono stati invitati a far parte dell'organizzazione.

```
aws signin delete-console-authorization-configuration \
  --target-id <your-aws-account-id> \
  --region us-east-1
```

Oppure elimina dichiarazioni di autorizzazione specifiche:

```
# First, list statements to get the statement ID
```

```
aws signin list-resource-permission-statements \
  --region us-east-1

# Then delete the problematic statement
aws signin delete-resource-permission-statement \
  --statement-id <statement-id> \
  --region us-east-1
```

Opzione 2: Contatta l' AWS assistenza

Se non disponi dell'accesso programmatico e non puoi utilizzarlo `OrganizationAccountAccessRole` per l'accesso all'account, contatta l' AWS assistenza per avviare il processo di ripristino del blocco.

Il processo di ripristino funziona nel modo seguente:

1. Se non riesci a risolvere il problema utilizzando le opzioni sopra riportate, apri una richiesta di assistenza presso il AWS Support Center. AWS Support verificherà la tua identità prima di esaminare il tuo account. I metodi di verifica possono includere la conferma dell'indirizzo e-mail dell'account utente root, la risposta a una chiamata di verifica telefonica o la risposta alle domande di sicurezza dell'account.
2. AWS Support conferma che il problema di accesso alla console è causato da un blocco delle policy basato sulle risorse.
3. AWS Support condivide un link al portale di ripristino. Utilizza questo link per accedere con un responsabile IAM nell'account che dispone dell'`signin:DeleteConsoleAuthorizationConfiguration`autorizzazione. Questa autorizzazione consente al principale di eliminare la configurazione di autorizzazione della console che causa il blocco.

> **Important**
>
> Il portale di ripristino rimuove l'intera configurazione di autorizzazione della console per l'account, incluse tutte le istruzioni di autorizzazione delle risorse. Il portale di ripristino non consente la riconfigurazione delle politiche basate AWS Sign-In sulle risorse.

Il link al portale di ripristino scade 72 ore dopo la condivisione da parte di AWS Support. Se non completi il ripristino entro quella finestra, contatta l' AWS assistenza per riavviare il processo.

Dopo aver riacquistato l'accesso:

- Rivedi e aggiorna le istruzioni di autorizzazione delle risorse per includere i principali esclusi configurati correttamente.
- Verifica l'accesso alla console dalle reti previste prima di riattivare l'autorizzazione della console.
- Documenta le tue procedure di ripristino per riferimenti futuri.

Le modifiche che apporto non sono sempre immediatamente visibili

Le modifiche alle policy si replicano a livello globale, ma la replica può richiedere alcuni minuti.

Risoluzione:

- Dopo aver apportato le modifiche alle policy, attendi qualche minuto per completare la replica globale.
- Verifica le modifiche utilizzando il `get-resource-policy` comando:

```
aws signin get-resource-policy --region <your-region>
```

- Controlla AWS CloudTrail i log per verificare la presenza di eventi di valutazione delle politiche per confermare che la nuova politica è in fase di valutazione.
- Conferma di utilizzare la regione corretta per le operazioni (le operazioni di scrittura devono essere utilizzate`us-east-1`).
- Se utilizzi condizioni basate su endpoint VPC, verifica che anche le policy degli endpoint VPC siano configurate correttamente.

Problemi comuni di replica delle policy:

- Pagina di accesso memorizzata nella cache: i browser possono memorizzare nella cache la pagina di accesso. Svuota la cache del browser o utilizza una finestra di navigazione in incognito per testare le modifiche alle politiche.
- Dichiarazioni in conflitto: se hai più istruzioni di autorizzazione, conferma che non siano in conflitto tra loro. Utilizzare `get-resource-policy` per rivedere la politica consolidata.
- Policy degli endpoint VPC: le policy funzionano insieme AWS Sign-In alle policy degli endpoint VPC. Entrambe devono consentire l'accesso desiderato.

AWS Sign-In riferimento alle chiavi di condizione

Questa pagina elenca le chiavi di condizione che è possibile utilizzare nelle politiche AWS Sign-In basate sulle risorse e nelle politiche di controllo delle risorse (RCP) e mostra la fase di valutazione e l'azione a cui si applica ciascuna chiave. Solo `signin:PrincipalArn` è specifico per AWS Sign-In; le altre sono chiavi di condizione globali. AWS Per le definizioni delle chiavi globali, consulta le chiavi di contesto delle condizioni AWS globali.

Per l'elenco completo delle azioni e delle chiavi di condizione nel Service Authorization Reference, vedi Azioni, risorse e chiavi di condizione per AWS Sign-In.

Network-based chiavi di condizione

Queste chiavi di condizione controllano da dove proviene la richiesta. AWS Sign-In li valuta per tutte le AWS Sign-In azioni (`signin:Authenticatesignin:Authorize0Auth2Access`, `esignin:Create0Auth2Token`) sia nelle politiche basate sulle risorse che negli RCP.

Network-based tasti di condizione

Chiave di condizione	operatori	Description	Regole di utilizzo
`aws:SourceIp`	`IpAddress` , `NotIpAddress`	Indirizzo IP pubblico o intervallo CIDR	Non presente quando una richiesta utilizza un endpoint VPC. Utilizza `IfExists` gli operatori quando combini con VPC-based le condizioni della stessa istruzione.
`aws:SourceVpc`	`StringEquals` , `StringNotEquals`	ID VPC () `vpc-xxxxxxxx`	Presente solo quando una richiesta utilizza un endpoint VPC. Usalo con `aws:RequestedRegion` per prevenire la collisione degli ID VPC tra regioni.

Chiave di condizione	operatori	Description	Regole di utilizzo
`aws:SourceVpce`	`StringEquals` , `StringNotEquals`	ID endpoint VPC () `vpce-xxxxxxxx`	Presente solo quando una richiesta utilizza un endpoint VPC.
`aws:VpcSourceIp`	`IpAddress` , `NotIpAddress`	IP privato all'interno del VPC	Usa sempre il tasto di `aws:VpcSourceIp` condizione con i tasti di `aws:SourceVpce` condizione `aws:SourceVpc` or.
`aws:RequestedRegion`	`StringEquals` , `StringNotEquals`	Codice AWS della regione di destinazione	Consigliato quando si utilizza `aws:SourceVpc` per prevenire la collisione tra ID VPC tra regioni. È possibile specificare più regioni.

> **Important**
>
> Una singola richiesta contiene `aws:SourceIp` (rete pubblica) o `aws:SourceVpc` (endpoint VPC), non entrambi. Quando scrivi politiche deny-unless che coprono entrambi i percorsi, usa `IfExists` gli operatori (ad esempio`NotIpAddressIfExists`) o crea istruzioni separate.

Identity-based chiavi di condizione

Queste chiavi condizionali controllano chi sta effettuando la richiesta. Sono disponibili solo per le azioni successive all'autenticazione (`signin:AuthorizeOAuth2Accessandsignin:CreateOAuth2Token`), in cui è stata stabilita l'identità principale.

Identity-based tasti di condizione

Chiave di condizione	operatori	Description	Esempi
`aws:PrincipalArn`	`ArnEquals` , `ArnLike`, `ArnNotEquals` , `StringEquals` , `StringLike`	ARN del principale IAM autenticato	`arn:aws:iam::123456789012:user/alice` , `arn:aws:iam::123456789012:role/Admin`
`aws:PrincipalAccount`	`StringEquals` , `StringNotEquals`	AWS ID dell'account del principale	`123456789012`

Service-specific chiave di condizione: signin: PrincipalArn

La seguente chiave di condizione è specifica AWS Sign-In e non è una AWS chiave globale. È disponibile solo durante la valutazione di pre-autenticazione. Viene utilizzato `signin:PrincipalArn` per identificare il principale che avvia l'accesso prima del completamento dell'autenticazione. Si tratta dell'equivalente di preautenticazione di`aws:PrincipalArn`, disponibile solo dopo l'autenticazione.

Operatori

Operatori ARN (`ArnEquals`,, `ArnLikeArnNotEquals`,`ArnNotLike`) e operatori stringa (`StringEquals`,`StringLike`).

Disponibilità

AWS Sign-In include questa chiave nel contesto della richiesta durante la fase di preautenticazione (l'`signin:Authenticate`azione). Non è disponibile per le azioni successive all'autenticazione (`signin:AuthorizeOAuth2Access`and`signin:CreateOAuth2Token`).

Tipo di dati

ARN. Utilizzate gli operatori ARN anziché gli operatori di stringa.

Value type (Tipo di valore)

Single-valued.

Supportato in

Resource-based politiche e RCP.

Usa gli operatori ARN per confrontare i valori. È possibile specificare i seguenti tipi principali:

- Account AWS utente root (`arn:aws:iam::123456789012:root`)
- utente IAM (`arn:aws:iam::123456789012:user/`*`user-name`*)
- Ruolo IAM (`arn:aws:iam::123456789012:role/`*`role-name`*)

Caso d'uso: esenta un'identità principale esclusa dalle restrizioni di rete, prevenendo il blocco e applicando comunque i controlli di rete per tutti gli altri tentativi di accesso.

Esempio: nega l'accesso di preautenticazione da reti non autorizzate, ad eccezione dell'utente root:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": "arn:aws:iam::123456789012:root"
        },
        "NotIpAddress": {
          "aws:SourceIp": "203.0.113.0/24"
        },
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    },
    {
      "Effect": "Deny",
```

```
      "Principal": { "AWS": "*" },
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:root"
        },
        "NotIpAddress": {
          "aws:SourceIp": "203.0.113.0/24"
        },
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    }
  ]
}
```

Questa politica nega l'accesso alla console dall'esterno dell'intervallo `203.0.113.0/24` IP, ad eccezione dell'utente root dell'account. L'istruzione di preautenticazione utilizza `signin:PrincipalArn` l'esonero dall'utente root prima del completamento dell'autenticazione. L'istruzione di post-autenticazione utilizza `aws:PrincipalArn` l'esenzione dello stesso principale dopo l'autenticazione, durante lo scambio di token OAuth. Per informazioni, consulta Esempi di policy.

Condiziona la disponibilità delle chiavi in base all'azione

Disponibilità delle chiavi di condizione per azione

Chiave di condizione	Accesso: autenticazione	accesso: AuthorizeOAuth2Access	accesso: CreateOAuth2Token
`aws:SourceIp`	Sì	Sì	Sì
`aws:SourceVpc`	Sì	Sì	Sì
`aws:SourceVpce`	Sì	Sì	Sì
`aws:VpcSourceIp`	Sì	Sì	Sì

Chiave di condizione	Accesso: autenticazione	accesso: AuthorizeOAuth2Access	accesso: CreateOAuth2Token
`aws:RequestedRegion`	Sì	Sì	Sì
`aws:PrincipalArn`	–	Sì	Sì
`aws:PrincipalAccount`	–	Sì	Sì
`signin:PrincipalArn`	Sì	–	–

> **Note**
>
> L'`signin:CreateAccount`azione viene utilizzata esclusivamente nelle policy degli endpoint VPC per Console Private Access e non è disponibile per le policy basate sulle risorse o gli RCP. Non è associata alcuna chiave di condizione specifica del servizio. Vedi Console Private Access.

Informazioni correlate

- Controllo dell'accesso alla console con policy basate sulle risorse e policy di controllo delle risorse
- Console di gestione AWS Accesso privato
- Chiavi di contesto delle condizioni globali di AWS
- Azioni, risorse e chiavi di condizione per AWS Sign-In

Accedi al tuo AWS portale di accesso

Un utente di IAM Identity Center è membro di AWS Organizations. Un utente di IAM Identity Center può accedere a più Account AWS applicazioni aziendali accedendo al portale di AWS accesso con un URL di accesso specifico. Per ulteriori informazioni sull'URL di accesso specifico, consulta. AWS portale di accesso

Prima di accedere Account AWS come utente a IAM Identity Center, raccogli le seguenti informazioni obbligatorie.

- Nome utente aziendale
- Password aziendale
- URL di accesso specifico

> **Note**
>
> Dopo l'accesso, la sessione del portale di AWS accesso è valida per 8 ore. È necessario effettuare nuovamente l'accesso dopo 8 ore.

Per accedere al tuo AWS accedere al portale

1. Nella finestra del browser, incolla l'URL di accesso che ti è stato fornito tramite e-mail, ad esempio il `https://your_subdomain.awsapps.com/start` formato URL dual-stack. `https://[IAM Identity Center instance ID].portal.[Region].app.aws` Quindi, premere Invio.
2. Accedi utilizzando le tue credenziali aziendali (come nome utente e password).

> **Note**
>
> Se l'amministratore ti ha inviato un'e-mail con una password monouso (OTP) e questa è la prima volta che accedi, inserisci quella password. Dopo aver effettuato l'accesso, devi creare una nuova password per gli accessi futuri.

3. Se ti viene chiesto un codice di verifica, controlla la tua email. Quindi copia e incolla il codice nella pagina di accesso.

   > **Note**
   >
   > I codici di verifica vengono generalmente inviati tramite e-mail, ma il metodo di consegna potrebbe variare. Se non ne hai ricevuto uno nella tua email, contatta l'amministratore per i dettagli sul codice di verifica.

4. Se l'MFA è abilitata per il tuo utente in IAM Identity Center, esegui l'autenticazione utilizzandola.
5. Dopo l'autenticazione, puoi accedere a qualsiasi Account AWS applicazione visualizzata nel portale.

   a. Per accedere, Console di gestione AWS scegli la scheda Account e seleziona il singolo account da gestire.

      Viene visualizzato il ruolo dell'utente. Scegli il nome del ruolo per l'account da aprire Console di gestione AWS. Scegli le chiavi di accesso per ottenere le credenziali per l'accesso da riga di comando o programmatico.

   b. Scegli la scheda Applicazioni per visualizzare le applicazioni disponibili e scegli l'icona dell'applicazione a cui desideri accedere.

L'accesso come utente in IAM Identity Center fornisce le credenziali per accedere alle risorse per un determinato periodo di tempo, chiamato sessione. Per impostazione predefinita, un utente può accedere a un account Account AWS per 8 ore. L'amministratore di IAM Identity Center può specificare una durata diversa, da un minimo di 15 minuti a un massimo di 90 giorni. Al termine della sessione, puoi accedere nuovamente.

Informazioni aggiuntive

Se desideri maggiori informazioni sugli utenti in IAM Identity Center, consulta le seguenti risorse.

- Per una panoramica di IAM Identity Center, consulta Cos'è IAM Identity Center?
- Per i dettagli sul tuo portale di AWS accesso, consulta Utilizzo del portale di AWS accesso.
- Per i dettagli sulle sessioni di IAM Identity Center, consulta Autenticazioni degli utenti.
- Per istruzioni dettagliate su come reimpostare la password utente di IAM Identity Center, consulta. Ho dimenticato la password del mio IAM Identity Center Account AWS

- Se tu o la tua organizzazione implementate il filtraggio degli IP o dei domini, potrebbe essere necessario consentire ai domini di creare e utilizzare il portale di accesso. AWS IAM Identity Center supporta sia gli endpoint IPv4 che quelli dual-stack. Se la tua rete utilizza IPv6, utilizza i domini endpoint dual-stack. Per informazioni dettagliate sull'elenco consentito dei domini, consulta. Domini da aggiungere all'elenco dei domini consentiti

Accedi tramite AWS Command Line Interface

È necessario stabilire in che modo si AWS CLI autentica con. AWS Scegliete il metodo più adatto al vostro flusso di lavoro e ai vostri requisiti di sicurezza.

- Accedi con le credenziali della console (consigliato)se utilizzi root, utenti IAM o federazione con IAM per l'accesso all' AWS account.
- Accedi con le credenziali IAM Identity Centerse utilizzi Identity Center per l'accesso all' AWS account.

Accedi con le credenziali della console (consigliato)

Questo metodo di autenticazione consente di utilizzare le credenziali della console con AWS CLI, semplificando l'avvio AWS programmatico entro pochi minuti dalla configurazione dell'account. Puoi ottenere credenziali temporanee che funzionano perfettamente con strumenti di sviluppo locali come, and. AWS CLI AWS SDKs AWS Strumenti per PowerShell

Prerequisiti

- Installa il. AWS CLI Per ulteriori informazioni, consulta Installazione o aggiornamento alla versione più recente della AWS CLI. Per utilizzare il comando è richiesta una versione minima di 2.32.0. `aws login`
- Accesso per accedere Console di gestione AWS come utente root, utente IAM o tramite federazione con IAM. Se utilizzi IAM Identity Center, accedi Accedi con le credenziali IAM Identity Center invece a.
- Assicurati che l'identità IAM disponga delle autorizzazioni appropriate. Allega la policy SignInLocalDevelopmentAccessgestita al tuo utente, ruolo o gruppo IAM. Se accedi come utente root, non sono richieste autorizzazioni aggiuntive.

Per accedere con le credenziali della console

1. Esegui il comando seguente per avviare il processo di autenticazione basato su browser:

   ```
   $ aws login
   ```

   Il `aws login` comando supporta diversi parametri opzionali:

- `aws login --remote`- Per l'autenticazione tra dispositivi quando il dispositivo non supporta un browser

> **Note**
>
> Puoi controllare l'accesso all'autenticazione sullo stesso dispositivo (`aws login`) e su più dispositivi (). `aws login --remote` Utilizza la seguente risorsa ARNs in qualsiasi policy IAM pertinente.
>
> - `arn:aws:signin:region:account-id:oauth2/public-client/localhost`— Usa questo ARN per l'autenticazione sullo stesso dispositivo con. `aws login`
> - `arn:aws:signin:region:account-id:oauth2/public-client/remote`— Utilizza questo ARN per l'autenticazione tra dispositivi con. `aws login --remote`

- `aws login --profile profile-name`- Per autenticarsi con un profilo specifico
- `aws login --region region`- Per autenticarsi in una regione specifica

2. Segui le istruzioni del tuo terminale. Il comando aprirà automaticamente il browser predefinito e ti guiderà attraverso il processo di autenticazione. Una volta completata l'autenticazione, la AWS CLI sessione sarà valida per un massimo di 12 ore.
3. Per terminare la sessione, usa:

```
$ aws logout
```

Se accedi ai AWS servizi in modo programmatico utilizzando AWS Strumenti per PowerShell, consulta Authenticating the AWS Tools for PowerShell with AWS. Se lo stai utilizzando AWS SDKs, consulta Autenticazione e accesso tramite AWS SDKs e strumenti.

Accedi con le credenziali IAM Identity Center

Il portale di AWS accesso consente agli utenti di IAM Identity Center di selezionare Account AWS e ottenere facilmente credenziali di sicurezza temporanee per. AWS CLI Per ulteriori informazioni su come ottenere queste credenziali, consulta. Disponibilità regionale per ID Builder AWS Puoi anche configurarlo AWS CLI direttamente per autenticare gli utenti con IAM Identity Center.

Per accedere con le credenziali di IAM Identity Center

1. Verifica di aver completato i prerequisiti.
2. Se accedi per la prima volta, configura il tuo profilo con la `aws configure sso` procedura guidata.
3. Dopo aver configurato il profilo, esegui il comando seguente, quindi segui le istruzioni nel tuo terminale:

```
$ aws sso login --profile my-profile
```

Informazioni aggiuntive

Se desideri maggiori informazioni sull'accesso tramite la riga di comando, consulta le seguenti risorse.

- Per ulteriori informazioni sull'utilizzo delle credenziali della console per accedere allo sviluppo AWS locale, consulta Autenticazione e credenziali di accesso per l'AWS CLI.
- Per ulteriori informazioni sulla procedura di AWS CLI accesso, consulta Autenticazione con credenziali a breve termine per. AWS CLI
- Per i dettagli sulla configurazione di IAM Identity Center, consulta Configurazione AWS CLI per l'utilizzo di IAM Identity Center.

Accedi come identità federata

Un'identità federata è un utente che può accedere a Account AWS risorse sicure con identità esterne. Le identità esterne possono provenire da un archivio di identità aziendali (ad esempio LDAP o Windows Active Directory) o da terze parti (ad esempio Login with Amazon, Facebook e Google). Le identità federate non accedono né accedono al Console di gestione AWS portale. AWS Il tipo di identità esterna in uso determina il modo in cui le identità federate accedono.

Gli amministratori devono creare un URL personalizzato che includa `https://signin.aws.amazon.com/federation`. Per ulteriori informazioni, consulta Abilitazione dell'accesso del gestore di identità personalizzato alla Console di gestione AWS.

> **Note**
>
> L'amministratore crea le identità federate. Contatta il tuo amministratore per maggiori dettagli su come accedere come identità federata.

Per ulteriori informazioni sulle identità federate, consulta About web identity federation.

Accedi con ID Builder AWS

ID Builder AWS è un profilo personale che fornisce l'accesso a strumenti e servizi selezionati, tra cui Amazon CodeCatalyst, Amazon Q Developer AWS Training e Certification. ID Builder AWS ti rappresenta come individuo ed è indipendente dalle credenziali e dai dati che potresti avere negli AWS account esistenti. Come gli altri profili personali, ID Builder AWS rimane con te mentre progredisci verso i tuoi obiettivi personali, educativi e di carriera.

I ID Builder AWS complementi Account AWS che possiedi già o che desideri creare. Sebbene un Account AWS funga da contenitore per AWS le risorse che crei e fornisca un limite di sicurezza per tali risorse, il tuo ti ID Builder AWS rappresenta come individuo. Per ulteriori informazioni, consulta ID Builder AWS e altre AWS credenziali.

ID Builder AWS è gratuito. Paghi solo per le AWS risorse che consumi nel tuo Account AWS. Per ulteriori informazioni sui prezzi, consulta Prezzi di AWS.

Se tu o la tua organizzazione implementate il filtraggio degli IP o dei domini, potrebbe essere necessario consentire ai domini di creare e utilizzare un. ID Builder AWS Per informazioni dettagliate sulla creazione di domini consentiti, consulta. Domini da aggiungere all'elenco dei domini consentiti

> **Note**
>
> AWS Builder ID è separato dall'abbonamento a AWS Skill Builder, un centro di apprendimento online in cui puoi imparare dagli AWS esperti e sviluppare competenze online sul cloud. Per ulteriori informazioni su AWS Skill Builder, consulta AWS Skill Builder.

Argomenti

- Elimina il tuo ID Builder AWS
- Gestione dell' ID Builder AWS autenticazione a più fattori (MFA)
- Privacy e dati in ID Builder AWS
- ID Builder AWS e altre AWS credenziali

Per accedere con ID Builder AWS

1. Vai al ID Builder AWS profilo o alla pagina di accesso dello AWS strumento o del servizio a cui desideri accedere. Ad esempio, per accedere ad Amazon CodeCatalyst, vai ahttps://codecatalyst.aws.
2. Scegli come accedere al tuo ID Builder AWS
   - Ho un account esistente
   - Ho un account Google
   - Ho un account Apple
   - Ho un GitHub account
   - Ho un account Amazon

Ho un account esistente

1. Per gli account esistenti, inserisci l'email che hai usato per creare il tuo ID Builder AWS e scegli Accedi.
2. Inserisci l'email che hai usato per creare il tuo ID Builder AWS e scegli Accedi.
3. Nella pagina Accedi con la tua ID Builder AWS pagina, inserisci la tua password.
4. (Facoltativo) Se desideri che i futuri accessi da questo dispositivo non richiedano ulteriori verifiche, seleziona la casella accanto a Questo è un dispositivo affidabile.
5. Scegli Continua.
6. Se viene richiesta una pagina di verifica aggiuntiva, segui le istruzioni del browser per fornire il codice o la chiave di sicurezza richiesti.

> **Note**
>
> Per la tua sicurezza, analizziamo il browser di accesso, la posizione e il dispositivo. Se indichi questo dispositivo come attendibile, non dovrai fornire un codice di autenticazione a più fattori (MFA) ogni volta che accedi. Per ulteriori informazioni, consulta Dispositivi attendibili.

Ho un account Google

Se il tuo account Google è già associato a un ID Builder AWS, devi utilizzare un indirizzo email diverso per accedere a un'applicazione. Per ulteriori informazioni, consulta Non riesco ad accedere con Google.

1. Per utilizzare il tuo account Google per accedere ID Builder AWS, scegli Continua con Google.
2. Nella pagina Accedi con Google, inserisci le informazioni relative al tuo account Google a cui accedere.
3. Scegli Continua per caricare la home page AWS dell'applicazione.

Ho un account Apple

Se il tuo account Apple è già associato a un ID Builder AWS, devi usare un indirizzo email diverso per accedere a un'applicazione. Per ulteriori informazioni, consulta Non riesco ad accedere con Apple.

1. Per usare il tuo account Apple per accedere ID Builder AWS, scegli Continua con Apple.
2. Nella pagina Accedi con Apple, inserisci le informazioni relative al tuo account Apple a cui accedere.
3. Scegli Continua per caricare la home page AWS dell'applicazione.

Ho un GitHub account

Se il tuo GitHub Account è già associato a un ID Builder AWS, devi utilizzare un indirizzo email diverso per accedere a un'applicazione. Per ulteriori informazioni, consulta Non riesco ad accedere con GitHub.

1. Per utilizzare il tuo GitHub account per accedere ID Builder AWS, scegli Continua con GitHub.

2. Nella GitHub pagina Accedi con, inserisci le informazioni relative al tuo GitHub account a cui accedere.
3. Scegli Continua per caricare la home page AWS dell'applicazione.

Ho un account Amazon

Se il tuo account Amazon è già associato a un ID Builder AWS, devi utilizzare un indirizzo e-mail diverso per accedere a un'applicazione. Per ulteriori informazioni, consulta Non riesco ad accedere con Amazon.

1. Per utilizzare il tuo account Amazon per accedere ID Builder AWS, scegli Continua con Amazon.
2. Nella pagina Accedi con Amazon, inserisci le informazioni relative al tuo account Amazon per accedere.
3. Scegli Continua per caricare la home page AWS dell'applicazione.

Disponibilità regionale per ID Builder AWS

ID Builder AWS è disponibile di seguito Regioni AWS. Le applicazioni che utilizzano ID Builder AWS possono funzionare in altre regioni.

Nome	Codice
Stati Uniti orientali (Virginia settentrionale)	us-east-1

Crea il tuo ID Builder AWS

Crei il tuo ID Builder AWS quando ti iscrivi a uno degli AWS strumenti e servizi che lo utilizzano. Registrati con il tuo indirizzo e-mail, nome e password come parte della procedura di registrazione a AWS uno strumento o servizio.

La tua password deve soddisfare i seguenti requisiti:

- Le password distinguono tra maiuscole e minuscole.
- La lunghezza delle password deve essere compresa tra 8 e 64 caratteri.
- Le password devono contenere almeno un carattere per ognuna delle quattro categorie seguenti:

  - Lettere minuscole (a-z)
  - Lettere maiuscole (A-Z)
  - Numeri (0-9)
  - Caratteri non alfanumerici (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)
- Le ultime tre password non possono essere riutilizzate.
- Le password che sono note pubblicamente attraverso un set di dati divulgato da terzi non possono essere utilizzate.

> **Note**
>
> Gli strumenti e i servizi che utilizzi ID Builder AWS ti consentono di crearli e utilizzarli ID Builder AWS quando necessario.

Per creare il tuo ID Builder AWS

1. Vai al ID Builder AWS profilo o alla pagina di registrazione dello AWS strumento o del servizio a cui desideri accedere. Ad esempio, per accedere ad Amazon CodeCatalyst, vai ahttps://codecatalyst.aws.
2. Scegli come creare il tuo ID Builder AWS
   - Per utilizzare il tuo account Google, scegli Continua con Google e segui le istruzioni per completare la procedura di registrazione. Questa operazione salta i passaggi da 3 a 8 riportati di seguito. Vai al passaggio 9.
   - Per usare il tuo account Apple, scegli Continua con Apple e segui le istruzioni per completare la procedura di registrazione. Questa operazione salta i passaggi da 3 a 8 riportati di seguito. Vai al passaggio 9.

     > **Note**
     >
     > Se scegli di abilitare la funzione «Nascondi la mia email» di iCloud+ per Accedi con Apple, il tuo indirizzo email ID Builder AWS verrà creato con l'indirizzo email designato Nascondi il mio indirizzo email nel tuo account Apple anziché con il tuo indirizzo email reale. Non potrai modificare questo indirizzo email, ma il tuo nome e cognome saranno comunque modificabili. Se devi accedere a ID Builder AWS, devi usare il tuo indirizzo email Hide My Email. ID Builder AWS utilizzerà il tuo indirizzo

Hide My Email per inviarti comunicazioni via e-mail. Per maggiori dettagli, vedi Come usare Nascondi la mia email con Accedi con Apple.

- Per usare il tuo GitHub account, scegli Continua con GitHub e segui le istruzioni per completare la procedura di registrazione. Questa operazione salta i passaggi da 3 a 8 riportati di seguito. Vai al passaggio 9.
- Per utilizzare il tuo account Amazon, scegli Continua con Amazon e segui le istruzioni per completare la procedura di registrazione. Questa operazione salta i passaggi 3-8 riportati di seguito. Vai al passaggio 9.
- Per creare un account con e-mail e password, continua con i seguenti passaggi.

3. Nella ID Builder AWS pagina Crea, inserisci il tuo indirizzo email. Consigliamo di utilizzare un indirizzo e-mail personale.
4. Scegli Next (Successivo).
5. Inserisci il tuo nome, quindi scegli Avanti.
6. Nella pagina Email verification (Verifica e-mail), inserisci il codice di verifica inviato al tuo indirizzo e-mail. Selezionare Verify (Verifica). A seconda del tuo provider di posta elettronica, per ricevere l'e-mail potrebbero essere necessari alcuni minuti. Controlla le cartelle dello spam e della posta indesiderata. Se non vedi l'email inviata AWS dopo cinque minuti, scegli Reinvia codice.
7. Dopo aver verificato la tua e-mail, nella pagina Choose a password (Scegli una password), inserisci una password e poi scegli Confirm password (Conferma password).
8. Se viene visualizzato un Captcha come protezione aggiuntiva, inserisci i caratteri che vedi.
9. Scegli Create ID Builder AWS (Crea).

Dispositivi attendibili

Dopo aver selezionato l'opzione This is a trusted device (Questo è un dispositivo attendibile) dalla pagina di accesso, considereremo autorizzati tutti gli accessi futuri da quel browser Web su quel dispositivo. Ciò significa che non sarà più necessario fornire un codice MFA per quel dispositivo attendibile. Tuttavia, se il browser, i cookie o l'indirizzo IP cambiano, potrebbe essere necessario utilizzare il codice MFA per una verifica aggiuntiva.

AWS strumenti e servizi che utilizzano ID Builder AWS

Puoi accedere con il tuo ID Builder AWS per accedere ai seguenti AWS strumenti e servizi. L'accesso alle funzionalità o ai vantaggi offerti a pagamento richiede un Account AWS.

Per impostazione predefinita, quando accedi a AWS uno strumento o servizio utilizzando il tuo ID Builder AWS, la durata della sessione dura 30 giorni ad eccezione di Amazon Q Developer, che ha una durata della sessione di 90 giorni. Al termine della sessione, dovrai effettuare nuovamente l'accesso.

AWS Comunità cloud

Community.aws è una piattaforma di e per la community di AWS costruttori a cui puoi accedere con il tuo. ID Builder AWSÈ un posto dove scoprire contenuti didattici, condividere pensieri e progetti personali, commentare i post degli altri e seguire i tuoi costruttori preferiti.

Amazon CodeCatalyst

Creerai un alias ID Builder AWS quando inizierai a usare Amazon CodeCatalyst e sceglierai un alias da associare ad attività come issue, code commit e pull request. Invita altre persone nel tuo CodeCatalyst spazio Amazon, che è completo degli strumenti, dell'infrastruttura e degli ambienti di cui il tuo team ha bisogno per realizzare il tuo prossimo progetto di successo. Ti servirà un Account AWS account per implementare un nuovo progetto nel cloud.

AWS Migration Hub

Accedi a AWS Migration Hub(Migration Hub) con il tuo ID Builder AWS. Migration Hub offre un unico posto per scoprire i server esistenti, pianificare le migrazioni e monitorare lo stato di ogni migrazione di applicazioni.

Amazon Q Developer

Amazon Q Developer è un assistente conversazionale generativo basato sull'intelligenza artificiale che può aiutarti a comprendere, creare, estendere e utilizzare le applicazioni. AWS Per ulteriori informazioni, consulta Cos'è Amazon Q Developer? nella Guida per l'utente di Amazon Q Developer.

AWS re:Post

AWS re:Postti fornisce una guida tecnica esperta in modo da poter innovare più velocemente e migliorare l'efficienza operativa utilizzando i servizi. AWS Puoi accedere con la tua ID Builder AWS ed entrare a far parte della community su re:post senza carta di credito Account AWS .

AWS Startup

Usa il tuo ID Builder AWS per iscriverti a AWS Startup dove puoi utilizzare contenuti didattici, strumenti, risorse e supporto per far crescere la tua startup. AWS

AWS Training e certificazione

Puoi utilizzare la tua certificazione ID Builder AWS per accedere AWS Training e sviluppare Cloud AWS le tue competenze con AWS Skill Builder, imparare dagli AWS esperti e convalidare la tua esperienza nel cloud con una credenziale riconosciuta nel settore.

Kiro

Kiro è un IDE agentico che ti aiuta a passare dal prototipo alla produzione con uno sviluppo basato sulle specifiche. Dalle attività semplici a quelle complesse, Kiro collabora con te per trasformare le istruzioni in specifiche dettagliate, quindi in codice, documenti e test funzionanti. Con Kiro, ciò che crei è esattamente ciò che desideri ed è pronto per essere condiviso con il tuo team. Gli agenti di Kiro ti aiutano a risolvere problemi complessi e ad automatizzare attività come la generazione di documentazione e i test unitari. Con Kiro, puoi andare oltre i prototipi rimanendo al posto di guida in ogni fase del processo.

Portale di registrazione del sito Web (WRP)

È possibile utilizzare l'identità ID Builder AWS del cliente e il profilo di registrazione permanenti per il sito Web AWS di marketing. Per registrarti a nuovi webinar e per visualizzare tutti i webinar a cui ti sei registrato o a cui hai partecipato, consulta La sezione I miei webinar.

Modifica il tuo ID Builder AWS profilo

Puoi modificare le informazioni del tuo profilo in qualsiasi momento. Puoi modificare l'indirizzo e-mail e il nome che hai usato per creare un account ID Builder AWS, oltre al tuo soprannome. Quando si utilizzano accessi social come Google o Apple, solo il nome e il soprannome sono modificabili.

Il nome è il modo in cui vieni chiamato negli strumenti e nei servizi mentre interagisci con gli altri. Il tuo soprannome indica come vuoi farti conoscere AWS, dai tuoi amici e dalle altre persone con cui collabori a stretto contatto.

> **Note**
>
> Gli strumenti e i servizi che utilizzi ID Builder AWS ti consentono di creare e utilizzare il tuo ID Builder AWS quando necessario.

Modifica delle informazioni del profilo

1. Accedi al tuo ID Builder AWS profilo suhttps://profile.aws.amazon.com.
2. Scegli My details (I miei dettagli).
3. Nella pagina My details (I miei dettagli), scegli il pulsante Edit (Modifica) accanto a Profile (Profilo).
4. Nella pagina Edit profile (Modifica profilo), apporta le modifiche desiderate al nome e al soprannome.
5. Scegli Save changes (Salva modifiche). Nella parte superiore della pagina viene visualizzato un messaggio di conferma che il profilo è stato aggiornato.

> **Note**
>
> La modifica del nome e del soprannome con uno degli altri nostri partner di accesso non aggiorna le stesse impostazioni per i tuoi ID Builder AWS.

Per modificare le informazioni di contatto,

1. Accedi al tuo ID Builder AWS profilo all'indirizzohttps://profile.aws.amazon.com.
2. Scegli My details (I miei dettagli).
3. Nella pagina My details (I miei dettagli), scegli il pulsante Edit (Modifica) accanto a Contact information (Informazioni di contatto).
4. Nella pagina Edit contact information (Modifica le informazioni di contatto), modifica il tuo indirizzo e-mail.
5. Scegli Verifica email. Viene visualizzata una finestra di dialogo.
6. Nella finestra di dialogo Verifica e-mail, dopo aver ricevuto il codice nell'e-mail, inserisci il codice in Codice di verifica. Selezionare Verify (Verifica).

Cambia la tua ID Builder AWS password

La tua password deve soddisfare i seguenti requisiti:

- Le password distinguono tra maiuscole e minuscole.
- La lunghezza delle password deve essere compresa tra 8 e 64 caratteri.

- Le password devono contenere almeno un carattere per ognuna delle quattro categorie seguenti:
  - Lettere minuscole (a-z)
  - Lettere maiuscole (A-Z)
  - Numeri (0-9)
  - Caratteri non alfanumerici (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- Le ultime tre password non possono essere riutilizzate.

> **Note**
>
> Le modifiche alla password non sono disponibili per ID Builder AWS gli account che utilizzano accessi social come Google o Apple. Se hai effettuato l'accesso utilizzando un accesso social, gestisci la password tramite il tuo account di accesso social. Per modificare la password per un accesso social:
>
> - Per un account Google, vedi Modificare o reimpostare la password (Google).
> - Per un account Apple, vedi Modificare la password del tuo account Apple.
> - Per un GitHub account, vedi Aggiornamento delle credenziali di GitHub accesso.
> - Per un account Amazon, consulta Come modificare la password Amazon.

Per modificare la ID Builder AWS password

1. Accedi al tuo ID Builder AWS profilo all'indirizzohttps://profile.aws.amazon.com.
2. Scegliere Sicurezza.
3. Nella pagina Security (Sicurezza), scegli Change password (Modifica password). Verrai reindirizzato a una nuova pagina.
4. Nella pagina Reinserisci la password, in Password, inserisci la password attuale. Quindi scegli Accedi.
5. Nella pagina Modifica la password, in Nuova password, inserisci la nuova password che desideri utilizzare. Quindi, in Conferma password, inserisci nuovamente la nuova password che desideri utilizzare.
6. Scegli Cambia password. Verrai reindirizzato al tuo ID Builder AWS profilo.

Elimina tutte le sessioni attive per il tuo ID Builder AWS

In Dispositivi connessi, puoi visualizzare tutti i dispositivi a cui hai attualmente effettuato l'accesso. Se non riconosci un dispositivo, come procedura consigliata in materia di sicurezza, devi prima modificare la password e poi disconnetterti ovunque. Puoi disconnetterti da tutti i dispositivi eliminando tutte le sessioni attive nella pagina Sicurezza relativa a ID Builder AWS.

> **Note**
>
> ID Builder AWS supporta sessioni estese di 90 giorni per Amazon Q Developer in un IDE. Per ogni nuovo accesso IDE, puoi visualizzare due voci di sessione. Quando esci dal tuo IDE, puoi continuare a vedere le sessioni IDE elencate in Dispositivi connessi anche se non sono più valide. Queste sessioni scompaiono una volta scaduti i 90 giorni.

Per eliminare tutte le sessioni attive

1. Accedi al tuo ID Builder AWS profilo all'indirizzohttps://profile.aws.amazon.com.
2. Scegliere Sicurezza.
3. Nella pagina Security (Sicurezza), scegli Delete all active sessions (Elimina tutte le sessioni attive).
4. Nella finestra di dialogo Elimina tutte le sessioni, inserisci elimina tutto. Eliminando tutte le sessioni, ti disconnetti da tutti i dispositivi a cui potresti aver effettuato l'accesso utilizzando il tuo ID Builder AWS, compresi i diversi browser. Quindi scegli Elimina tutte le sessioni.

> **Note**
>
> Quando utilizzi un account di accesso social come Google o Apple, l'eliminazione delle ID Builder AWS sessioni attive non ti disconnetterà dal tuo account di accesso social.

Elimina il tuo ID Builder AWS

La procedura seguente descrive come eliminare l' ID Builder AWS account.

Warning

L'eliminazione del tuo ID Builder AWS comporterà quanto segue:

- Perdita di accesso: non è più possibile accedere a AWS strumenti e servizi tramite ID Builder AWS i quali si accedeva in precedenza. ID Builder AWS Il tuo account è separato da qualsiasi altro AWS account che possiedi e la cancellazione del tuo account non ID Builder AWS comporterà la chiusura del tuo AWS account.
- Eliminazione dei contenuti: tutti i contenuti rimanenti associati esclusivamente all'utente ID Builder AWS verranno eliminati e l'utente non sarà più in grado di accedere o recuperare i contenuti dalle applicazioni che utilizzano il ID Builder AWS
- Eliminazione delle informazioni personali: tutte le informazioni personali fornite dall'utente in relazione alla creazione e all'amministrazione dell'utente ID Builder AWS verranno eliminate, ad eccezione di quelle che AWS potrebbero conservare le informazioni personali come richiesto o consentito dalla legge, come le registrazioni della richiesta di cancellazione o i dati in un formato che non consente l'identificazione dell'utente.

  Per ulteriori informazioni su come gestiamo le tue informazioni, consulta l'Informativa sulla privacy di AWS. Puoi aggiornare le tue preferenze di AWS comunicazione o annullare l'iscrizione visitando l'AWS Communications Preferences Center.
- Gli account di accesso social rimangono invariati: se utilizzi un accesso social come Google o Apple, l'eliminazione del tuo ID Builder AWS non elimina nulla relativo al tuo account di accesso social. Consulta la documentazione del tuo provider di accesso ai social network per scoprire come eliminare tali account. L'eliminazione della ID Builder AWS connessione dal tuo account di accesso social non elimina il tuo ID Builder AWS account, ma non potrai più accedere al tuo ID Builder AWS profilo.

Per eliminare il tuo ID Builder AWS

1. Accedi al tuo ID Builder AWS profilo all'indirizzohttps://profile.aws.amazon.com.
2. Scegli Privacy & data (Privacy e dati).
3. Nella pagina Privacy e dati, in Eliminazione ID Builder AWS, scegli Elimina ID Builder AWS.
4. Seleziona la casella di controllo accanto a ogni dichiarazione di non responsabilità per confermare che sei pronto per procedere.
5. Scegli Delete ID Builder AWS (Elimina).

Gestione dell' ID Builder AWS autenticazione a più fattori (MFA)

L'autenticazione a più fattori (MFA) è un meccanismo semplice ed efficace per migliorare la sicurezza. Il primo fattore, la password, è un segreto che viene memorizzato, noto anche come fattore di conoscenza. Altri fattori possono essere fattori di possesso (qualcosa che possiedi, come una chiave di sicurezza) o fattori intrinseci (qualcosa che sei, come una scansione biometrica). Ti consigliamo vivamente di configurare l'MFA per aggiungere un livello aggiuntivo per il tuo. ID Builder AWS

Puoi registrare un autenticatore integrato e anche registrare una chiave di sicurezza da conservare in un luogo fisicamente sicuro. Se non riesci a utilizzare l'autenticatore integrato, puoi utilizzare la chiave di sicurezza registrata. Per le applicazioni di autenticazione, puoi anche abilitare la funzionalità di backup o sincronizzazione su cloud in tali app. Questo ti aiuta a evitare di perdere l'accesso al tuo profilo in caso di smarrimento o danneggiamento del dispositivo MFA.

Punti chiave

- Consigliamo di registrare più dispositivi MFA. Se perdi l'accesso a tutti i dispositivi MFA registrati, non potrai ripristinare i tuoi. ID Builder AWS
- Ti consigliamo di controllare periodicamente i dispositivi MFA registrati per assicurarti che siano aggiornati e funzionanti. Inoltre, è necessario conservare tali dispositivi in un luogo fisicamente sicuro quando non vengono utilizzati.
- Se hai creato il tuo account utilizzando Continua con Google, puoi abilitare l'autenticazione a più fattori tramite il tuo account Google. Per maggiori dettagli, consulta Attivare la verifica in due passaggi.
- Se hai creato il tuo account utilizzando Continua con Apple, è probabile che l'autenticazione a più fattori sia già abilitata nel tuo account Apple. In caso contrario, per i dettagli su come abilitarla, consulta Autenticazione a due fattori per l'account Apple.
- Se hai creato il tuo account utilizzando Continua con GitHub, puoi abilitare l'autenticazione a più fattori tramite il tuo GitHub account. Per i dettagli, consulta Configurazione (GitHub) dell'autenticazione a due fattori.
- Se hai creato il tuo account utilizzando Continue with Amazon, puoi abilitare l'autenticazione a più fattori tramite il tuo account Amazon. Per maggiori dettagli, consulta Cos'è la verifica in due passaggi? .

Tipi di MFA disponibili per ID Builder AWS

ID Builder AWS supporta i seguenti tipi di dispositivi di autenticazione a più fattori (MFA).

FIDO2 autenticatori

FIDO2è uno standard che include CTAP2 WebAuthne si basa sulla crittografia a chiave pubblica. Le credenziali FIDO sono resistenti al phishing perché sono uniche per il sito Web in cui sono state create, ad esempio. AWS

AWS supporta i due fattori di forma più comuni per gli autenticatori FIDO: autenticatori integrati e chiavi di sicurezza. Di seguito sono riportate ulteriori informazioni sui tipi più comuni di autenticatori FIDO.

Argomenti

Autenticatori integrati

Alcuni dispositivi dispongono di autenticatori integrati, come TouchID on o una fotocamera compatibile con Windows Hello. MacBook Se il dispositivo è compatibile con i protocolli FIDO, tra cui WebAuthn, è possibile utilizzare l'impronta digitale o il viso come secondo fattore. Per ulteriori informazioni, consulta Autenticazione FIDO.

Chiavi di sicurezza

È possibile acquistare una chiave di FIDO2 sicurezza esterna compatibile con USB, BLE o NFC. Quando ti viene richiesto un dispositivo MFA, tocca il sensore della chiave. YubiKey o Feitian crea dispositivi compatibili. Per un elenco di tutte le chiavi di sicurezza compatibili, consulta Prodotti certificati FIDO.

Gestori di password, fornitori di chiavi di accesso e altri autenticatori FIDO

Diversi provider terzi supportano l'autenticazione FIDO nelle applicazioni mobili, come funzionalità nei gestori di password, nelle smart card con modalità FIDO e in altri fattori di forma. Questi dispositivi compatibili con FIDO possono funzionare con IAM Identity Center, ma ti consigliamo di testare personalmente un autenticatore FIDO prima di abilitare questa opzione per l'MFA.

> **Note**
>
> Alcuni autenticatori FIDO possono creare credenziali FIDO individuabili note come passkey. Le passkey possono essere associate al dispositivo che le crea oppure possono essere sincronizzate e salvate su un cloud. Ad esempio, puoi registrare una passkey utilizzando Apple Touch ID su un Macbook supportato, quindi accedere a un sito da un laptop Windows utilizzando Google Chrome con la tua passkey in iCloud seguendo le istruzioni sullo schermo al momento dell'accesso. Per ulteriori informazioni sui dispositivi che supportano le passkey sincronizzabili e l'attuale interoperabilità delle passkey tra sistemi operativi e browser, vedere Device Support su passkeys.dev, una risorsa gestita da FIDO Alliance And World Wide Web Consortium (W3C).

Applicazioni di autenticazione

Le applicazioni di autenticazione sono autenticatori di terze parti basati su codice OTP (One-Time Password). È possibile utilizzare un'applicazione di autenticazione installata sul dispositivo mobile o sul tablet come dispositivo MFA autorizzato. L'applicazione di autenticazione di terze parti deve essere conforme a RFC 6238, un algoritmo TOTP (password monouso) basato su standard in grado di generare codici di autenticazione a sei cifre.

Quando viene richiesta l'autenticazione MFA, è necessario inserire un codice valido dall'app di autenticazione nella casella di input visualizzata. Ogni dispositivo MFA assegnato a un utente deve essere univoco. È possibile registrare due app di autenticazione per ogni utente.

Puoi scegliere tra le seguenti famose app di autenticazione di terze parti. Tuttavia, qualsiasi applicazione conforme a TOTP funziona con l'MFA. ID Builder AWS

Sistema operativo	Applicazione di autenticazione testata
Android	1Password, Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator
iOS	1Password, Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

Registra il tuo ID Builder AWS dispositivo MFA

> **Note**
>
> Dopo aver effettuato la registrazione all'MFA, esserti disconnesso e aver effettuato l'accesso sullo stesso dispositivo, potresti non ricevere alcuna richiesta di autenticazione a MFA sui dispositivi considerati attendibili.

Registrazione del dispositivo MFA tramite un'app di autenticazione

1. Accedi al tuo ID Builder AWS profilo all'indirizzohttps://profile.aws.amazon.com.
2. Scegliere Sicurezza.
3. Nella pagina Security (Sicurezza), scegli Register device (Registra dispositivo).
4. Nella pagina Register MFA device (Registra dispositivo MFA), scegli l'app di autenticazione.
5. ID Builder AWS gestisce e visualizza le informazioni di configurazione, inclusa una grafica con codice QR. Il grafico è una rappresentazione della "chiave di configurazione segreta" disponibile per l'inserimento manuale nelle applicazioni di autenticazione che non supportano i codici QR.
6. Apri l'app di autenticazione. Per un elenco di applicazioni, consulta Applicazioni di autenticazione.

   Se l'applicazione di autenticazione supporta più account o dispositivi MFA, seleziona l'opzione che consente di creare un nuovo account o dispositivo MFA.
7. Determina se l'app MFA supporta i codici QR e completa una delle seguenti operazioni sulla pagina Set up your authenticator app (Configurazione dell'applicazione di autenticazione):

   1. Scegli Show QR code (Mostra codice QR) e utilizza l'app per eseguire la scansione del codice QR. Ad esempio, è possibile selezionare l'icona della fotocamera o un'opzione simile a Scan code (Scannerizza codice). Quindi usa la fotocamera del dispositivo per la scansione del codice.
   2. Scegli Show secret key (Mostra chiave segreta), quindi inserisci la chiave segreta nell'app MFA.

   Al termine, l'app di autenticazione genererà e visualizzerà una password monouso.
8. Nella casella Authenticator (Autenticatore), digitar la password monouso visualizzata nell'app di autenticazione. Scegliere Assign MFA (Assegna MFA).

> **Important**
>
> Invia la richiesta immediatamente dopo la generazione del codice. Se generi il codice e poi attendi troppo a lungo per inviare la richiesta, il dispositivo MFA viene associato correttamente al tuo ID Builder AWS, ma il dispositivo MFA non è sincronizzato. Ciò accade perché le password monouso temporanee (TOTP) scadono dopo un breve periodo di tempo. Se ciò accade, è possibile sincronizzare nuovamente il dispositivo. Per ulteriori informazioni, consulta Ricevo il messaggio "An unexpected error has occurred" (Si è verificato un errore imprevisto) quando provo a registrarmi o accedere con un'app di autenticazione.

9. Per assegnare al dispositivo un nome descrittivo ID Builder AWS, scegli Rinomina. Questo nome ti aiuta a distinguere il dispositivo dagli altri registrati.

Il dispositivo MFA è ora pronto per l'uso con. ID Builder AWS

Registra una chiave di sicurezza come dispositivo ID Builder AWS MFA

Registrazione del dispositivo MFA tramite una chiave di sicurezza

1. Accedi al tuo ID Builder AWS profilo all'indirizzohttps://profile.aws.amazon.com.
2. Scegliere Sicurezza.
3. Nella pagina Security (Sicurezza), scegli Register device (Registra dispositivo).
4. Nella pagina Register MFA device (Registra dispositivo MFA), scegli Security key (Chiave di sicurezza).
5. Assicurati che la chiave di sicurezza sia abilitata. Se utilizzi una chiave di sicurezza fisica separata, collegala al computer.
6. Segui le istruzioni riportate sullo schermo. La tua esperienza varierà in base al sistema operativo e al browser.
7. Per assegnare al dispositivo un nome descrittivo ID Builder AWS, scegli Rinomina. Questo nome ti aiuta a distinguere il dispositivo dagli altri registrati.

Il dispositivo MFA è ora pronto per l'uso con. ID Builder AWS

Rinomina il tuo dispositivo ID Builder AWS MFA

Ridenominazione del dispositivo MFA

1. Accedi al tuo ID Builder AWS profilo all'indirizzo. https://profile.aws.amazon.com
2. Scegliere Sicurezza. Quando arrivi alla pagina, il campo Rename (RinominaI è disattivato.
3. Seleziona il dispositivo MFA che desideri modificare. Questo ti permette di scegliere Rename (Rinomina). Quindi, si apre una finestra di dialogo.
4. Nel prompt visualizzato, inserisci il nuovo nome in MFA device name (Nome del dispositivo MFA) e scegli Rename (Rinomina). Il dispositivo rinominato viene visualizzato in Multi-factor authentication (MFA) devices (Dispositivi di autenticazione a più fattori (MFA).

Eliminare il dispositivo MFA

Consigliamo di mantenere attivi due o più dispositivi MFA. Prima di rimuovere un dispositivo, consulta Registra il tuo ID Builder AWS dispositivo MFA per registrare un dispositivo MFA sostitutivo. Per disabilitare l'autenticazione a più fattori per il tuo ID Builder AWS, rimuovi tutti i dispositivi MFA registrati dal tuo profilo.

Eliminazione di un dispositivo MFA

1. Accedi al tuo ID Builder AWS profilo all'indirizzo. https://profile.aws.amazon.com
2. Scegliere Sicurezza.
3. Seleziona il dispositivo MFA che desideri eliminare e scegli Delete (Elimina).
4. Nella finestra Delete MFA device? (Eliminare il dispositivo MFA?), segui le istruzioni per eliminare il dispositivo.
5. Scegli Elimina.

Il dispositivo non sarà più visualizzato in Multi-factor authentication (MFA) devices (Dispositivi di autenticazione a più fattori (MFA).

Privacy e dati in ID Builder AWS

Nella sezione Informativa sulla privacy di AWS è riportato come gestiamo i tuoi dati personali. Per informazioni su come eliminare il tuo ID Builder AWS profilo, consultaElimina il tuo ID Builder AWS.

Richiedi i tuoi ID Builder AWS dati

Puoi richiedere e visualizzare le informazioni personali associate a te e alle AWS applicazioni ID Builder AWS e ai servizi a cui hai avuto accesso tramite il tuo ID Builder AWS. Per ulteriori informazioni sull'esercizio dei diritti dell'interessato, incluse le informazioni personali fornite in relazione ad altri AWS siti Web, applicazioni, prodotti, servizi, eventi ed esperienze, consultahttps://aws.amazon.com/privacy.

Richiesta dei dati

1. Accedi al tuo ID Builder AWS profilo all'indirizzohttps://profile.aws.amazon.com.
2. Scegli I miei ID Builder AWS dati.
3. Nella pagina I miei ID Builder AWS dati, in Eliminazione ID Builder AWS, scegli Richiedi i tuoi dati.
4. Nella parte superiore della pagina viene visualizzato un messaggio verde di conferma, in cui è indicato che abbiamo ricevuto la tua richiesta e che verrà completata entro 30 giorni.
5. Quando ricevi un'email da noi indicante che la richiesta è stata elaborata, torna alla pagina Privacy e dati del tuo ID Builder AWS profilo. Scegli il nuovo pulsante disponibile Download ZIP archive with your data (Scarica il file ZIP con i tuoi dati).

   Mentre la tua richiesta di dati è in sospeso, non potrai eliminare i tuoi ID Builder AWS.

ID Builder AWS e altre AWS credenziali

ID Builder AWS La tua è separata da Account AWS qualsiasi credenziale di accesso. Puoi utilizzare la stessa e-mail per la tua e-mail ID Builder AWS e per quella dell'utente root di un Account AWS.

Un ID Builder AWS:

- Consente di accedere agli strumenti e ai servizi che utilizza ID Builder AWS.
- Non influisce sui controlli di sicurezza esistenti, come le politiche e le configurazioni che hai specificato sulle tue Account AWS applicazioni.
- Non sostituisce utenti, credenziali o account root, IAM Identity Center o IAM esistenti.
- Impossibile ottenere le credenziali AWS IAM per accedere a Console di gestione AWS, AWS CLI AWS SDKs, o AWS Toolkit.

An Account AWS è un contenitore di risorse con informazioni di contatto e pagamento. Stabilisce un limite di sicurezza entro il quale gestire AWS servizi fatturati e misurati, come S3, EC2 o Lambda. I titolari di account possono accedere a un account. Account AWS Console di gestione AWS Per ulteriori informazioni, consulta Firma nella Console di gestione AWS.

In che modo ID Builder AWS si collega alla tua identità IAM Identity Center esistente

In qualità di individuo proprietario dell'identità, gestisci il ID Builder AWS. Non è collegato ad alcun'altra identità che potresti avere per un'altra organizzazione, come scuola o lavoro. Potresti utilizzare un'identità della forza lavoro in IAM Identity Center per rappresentare la tua identità lavorativa e una ID Builder AWS per rappresentare la tua personalità privata. Queste identità operano in modo indipendente.

Gli utenti in AWS IAM Identity Center (successore di AWS Single Sign-On) sono gestiti da un amministratore IT o cloud aziendale o dall'amministratore del provider di identità dell'organizzazione, come Okta, Ping o Azure. Gli utenti nel Centro identità IAM possono accedere alle risorse su più account in AWS Organizations.

Profili multipli ID Builder AWS

Puoi crearne più di uno ID Builder AWS purché ogni ID utilizzi un indirizzo email univoco. Tuttavia, utilizzarne più di uno ID Builder AWS può rendere difficile ricordare quale ID Builder AWS hai usato per quale scopo. Quando possibile, ti consigliamo di utilizzarne uno ID Builder AWS per tutte le tue attività relative a AWS strumenti e servizi.

Esci da AWS

Il modo in cui ti Account AWS disconnetti dipende dal tipo di AWS utente che sei. Puoi essere un utente root dell'account, un utente IAM, un utente in IAM Identity Center, un'identità federata o un utente AWS Builder ID. Se non sei sicuro del tipo di utente che sei, consulta. Determina il tipo di utente

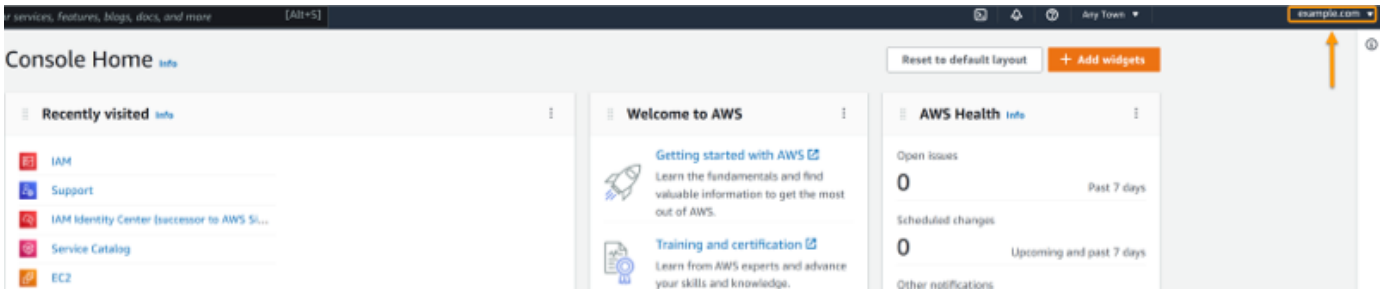
Argomenti

- Esci dal Console di gestione AWS
- Esci dal tuo portale di AWS accesso
- Esci da AWS Builder ID

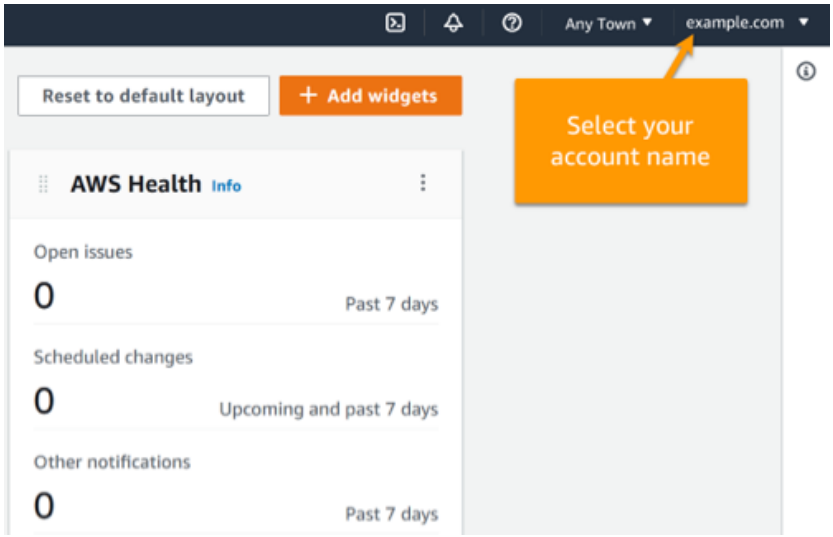
Esci dal Console di gestione AWS

Per disconnettersi da Console di gestione AWS

1. Dopo aver effettuato l'accesso a Console di gestione AWS, arriverai a una pagina simile a quella mostrata nell'immagine seguente. Il nome del tuo account o il nome utente IAM è mostrato nell'angolo in alto a destra.



2. Nella barra di navigazione in alto a destra, scegli il tuo nome utente.



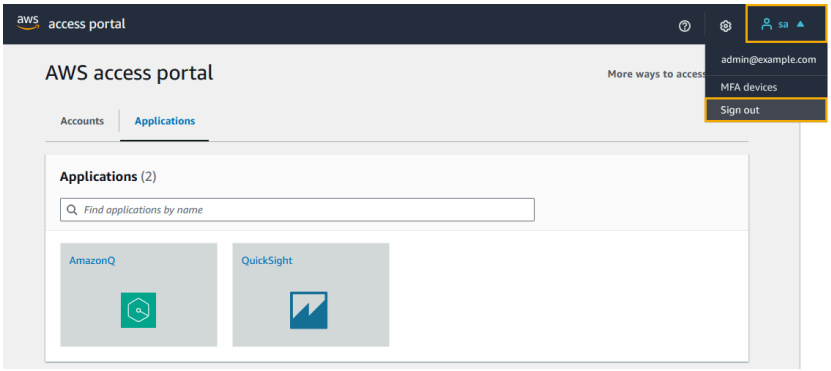
3. Scegli un'opzione di disconnessione. Le opzioni dei pulsanti variano in base al numero di account a cui hai effettuato l'accesso.
   - Seleziona Esci se hai effettuato l'accesso a un solo account.
   - Seleziona Esci da tutte le sessioni per disconnetterti da tutte le tue identità contemporaneamente.
   - Seleziona Esci dalla sessione corrente per disconnetterti dall'identità che hai selezionato.
4. Verrai reindirizzato alla Console di gestione AWS pagina web.

Per ulteriori informazioni sull'accesso a più account, consulta Accesso a più account nella Guida Console di gestione AWS introduttiva.

Esci dal tuo portale di AWS accesso

Per uscire dal portale di AWS accesso

1. Nella barra di navigazione in alto a destra, scegli il tuo nome utente.
2. Seleziona Esci come mostrato nell'immagine seguente.



3. Se la disconnessione è riuscita, ora viene visualizzata la pagina di AWS accesso al portale di accesso.

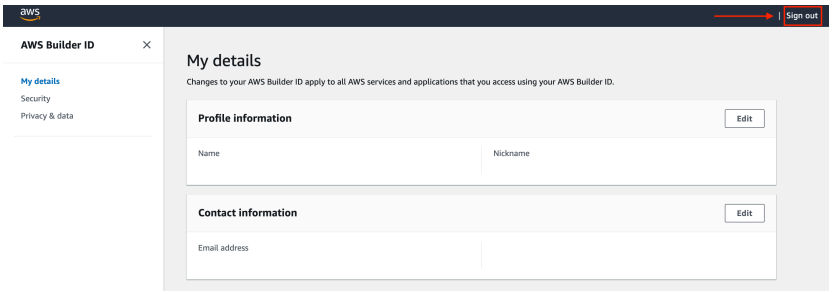
Se utilizzi un provider di identità esterno (IdP) come fonte di identità, la sessione attiva per le tue credenziali non viene interrotta quando ti disconnetti. Se si torna al portale di AWS accesso, è possibile che venga effettuato automaticamente l'accesso senza dover fornire le proprie credenziali.

Esci da AWS Builder ID

Per uscire da un AWS servizio a cui hai effettuato l'accesso utilizzando il tuo AWS Builder ID, devi disconnetterti dal servizio. Se vuoi uscire dal tuo profilo AWS Builder ID, consulta la procedura seguente.

Per uscire dal tuo profilo AWS Builder ID

1. Dopo aver effettuato l'accesso al tuo profilo AWS Builder ID all'indirizzohttps://profile.aws.amazon.com/, accedi alla pagina I miei dati.
2. In alto a destra della pagina del tuo profilo AWS Builder ID, scegli Esci.



3. Ti disconnetti quando non vedi più il tuo profilo AWS Builder ID.

Risoluzione dei problemi Account AWS problemi di accesso

Utilizza le informazioni qui per aiutarti a risolvere i problemi di accesso e altri problemi. Account AWS Per istruzioni dettagliate sull'accesso a un file, consulta. Account AWSAccedi al Console di gestione AWS

Se nessuno degli argomenti di risoluzione dei problemi ti aiuta a risolvere il problema di accesso, puoi creare un caso Supporto compilando questo modulo: Sono un AWS cliente e cerco assistenza per la fatturazione o l'account. Come procedura consigliata in materia di sicurezza, non Supporto puoi parlare dei dettagli di Account AWS persone diverse dall'account a cui hai effettuato l'accesso. Inoltre, AWS Support non può modificare le credenziali associate a un account per nessun motivo.

> **Note**
>
> Supporto non pubblica un numero di telefono diretto per contattare un rappresentante dell'assistenza.

Per ulteriore assistenza sulla risoluzione dei problemi di accesso, vedi Cosa devo fare se ho problemi ad accedere o accedere al mio? Account AWS Se riscontri problemi di accesso Amazon.com, consulta il Servizio clienti Amazon anziché questa pagina.

Argomenti

- Ho dimenticato la mia password utente IAM per il mio Account AWS
- Ho dimenticato la mia password di identità federata per il mio Account AWS
- Non riesco ad accedere al mio account esistente Account AWS e non riesco a crearne uno nuovo Account AWS con lo stesso indirizzo email
- Devo riattivare il mio account sospeso Account AWS
- Devo contattare Supporto per problemi di accesso
- Devo contattare AWS Billing per problemi di fatturazione
- Ho una domanda su un ordine al dettaglio
- Ho bisogno di aiuto per gestire il mio Account AWS
- Il mio AWS le credenziali del portale di accesso non funzionano
- Ho dimenticato la password del mio IAM Identity Center Account AWS
- Ricevo un messaggio di errore che dice «Non sei tu, siamo noi» quando provo ad accedere alla console IAM Identity Center

Mio Console di gestione AWS le credenziali non funzionano

Se ricordi nome utente e password, ma le credenziali non funzionano, potresti trovarti nella pagina sbagliata. Prova ad accedere da un'altra pagina:

Pagina di accesso utente root

- Se hai creato o possiedi un account Account AWS e stai eseguendo un'operazione che richiede credenziali di utente root, inserisci l'indirizzo e-mail del tuo account nel campo. Console di gestione AWS Per informazioni su come accedere all'utente root, consultaPer accedere come utente root. Se hai dimenticato la password dell'utente root, puoi reimpostarla. Per ulteriori informazioni, consulta Ho dimenticato la password dell'utente root per il mio Account AWS. Se hai dimenticato l'indirizzo e-mail dell'utente root, controlla se nella tua casella di posta elettronica è presente un'e-mail inviata da. AWS
- Se hai provato ad accedere al tuo account utente root e hai ricevuto l'errore: Il recupero della password è disabilitato per il mio account utente root, non hai le credenziali dell'utente root. Non puoi accedere come utente root o eseguire il recupero della password per l'utente root del tuo account. AWS gli account membro gestiti utilizzando AWS Organizations potrebbero non avere una password utente root, chiavi di accesso, certificati di firma o autenticazione a più fattori (MFA) attiva.

Solo l'account di gestione o l'amministratore delegato di IAM può eseguire azioni utente root nell'account membro. Contatta l'amministratore se devi eseguire un'operazione che richiede le credenziali dell'utente root. Per ulteriori informazioni, consulta Gestire centralmente l'accesso root per gli account dei membri nella Guida per l'AWS Identity and Access Management utente.

Pagina di accesso utente IAM

- Se tu o qualcun altro avete creato un utente IAM all'interno di un Account AWS, devi conoscere quell' Account AWS ID o alias per accedere. Inserisci l'ID o l'alias del tuo account, il nome utente e la password in. Console di gestione AWS Per sapere come accedere alla pagina di accesso degli utenti IAM, consulta. Accesso come utente IAM Se hai dimenticato la password utente IAM, puoi consultare la pagina Ho dimenticato la mia password utente IAM per il mio Account AWS per informazioni sulla reimpostazione della password utente IAM. Controlla la tua e-mail, i preferiti del browser o la cronologia del browser per trovare un URL che includa `signin.aws.amazon.com/`. L'ID o l'alias del tuo account seguiranno il testo `"account="` nell'URL. Se non riesci a trovare l'ID o l'alias del tuo account, contatta l'amministratore. Supporto non posso aiutarti a recuperare queste informazioni. Non puoi vedere l'ID o l'alias del tuo account se non dopo aver effettuato l'accesso.

La reimpostazione della password è richiesta per il mio utente root

Per proteggere il tuo account, potresti ricevere il seguente messaggio quando tenti di accedere a Console di gestione AWS:

È richiesta la reimpostazione della password. Per motivi di sicurezza, è necessario reimpostare la password. Per proteggere il tuo account, devi scegliere Password dimenticata qui sotto e reimpostare la password.

Oltre a questo messaggio, ti avvisa AWS anche quando identifichiamo un potenziale problema tramite l'e-mail associata al tuo account. Questa e-mail include il motivo per cui è richiesta la reimpostazione della password. Ad esempio, quando identifichiamo attività di accesso insolite Account AWS o le credenziali associate all'utente Account AWS sono disponibili pubblicamente online.

Aggiorna la password per assicurarti che le credenziali dell'utente root rimangano sicure. Per informazioni su come reimpostare la password dell'utente root, consulta Ho dimenticato la password dell'utente root per il mio. Account AWS

Non ho accesso all'e-mail del mio Account AWS

Quando ne crei un Account AWS, fornisci un indirizzo e-mail e una password. Queste sono le credenziali per Utente root dell'account AWS. Se non sei sicuro dell'indirizzo e-mail associato al tuo Account AWS, cerca la corrispondenza salvata che termina con @signin .aws o @verify .signin.aws a qualsiasi indirizzo e-mail della tua organizzazione che potrebbe essere stato utilizzato per aprire il. Account AWS Chiedi agli altri membri del tuo team, della tua organizzazione o della tua famiglia. Se qualcuno che conosci ha creato l'account, può aiutarti ad accedervi.

Se conosci l'indirizzo e-mail ma non hai più accesso all'e-mail, prova innanzitutto a recuperare l'accesso all'e-mail utilizzando una delle seguenti opzioni:

- Se sei il proprietario del dominio dell'indirizzo e-mail, puoi ripristinare un indirizzo e-mail eliminato. In alternativa, puoi impostare un catch-all per il tuo account e-mail che "acquisisce tutti" i messaggi inviati a indirizzi e-mail che non esistono più nel server di posta e li reindirizza a un altro indirizzo e-mail.
- Se l'indirizzo e-mail dell'account è parte del sistema di posta elettronica aziendale, si consiglia di contattare gli amministratori del sistema IT. Potrebbero essere in grado di aiutare a ottenere nuovamente l'accesso all'e-mail.

Se ancora non riesci ad accedere al tuo Account AWS, puoi trovare opzioni di supporto alternative Supportocontattando.

Il mio dispositivo MFA si è perso o ha smesso di funzionare

Se il tuo dispositivo MFA viene smarrito, danneggiato o non funziona, non ricevi un codice di accesso monouso (OTP) quando invii una richiesta di verifica MFA.

Utenti IAM

Puoi accedere utilizzando un altro dispositivo MFA registrato allo stesso utente IAM.

Gli utenti IAM devono contattare un amministratore per disattivare un dispositivo MFA che non funziona. Questi utenti non possono ripristinare il proprio dispositivo MFA senza l'assistenza dell'amministratore. L'amministratore è in genere un personale IT (Information Technology) che dispone di un livello di autorizzazioni più elevato Account AWS rispetto agli altri membri dell'organizzazione. Questa persona ha creato l'account e fornisce agli utenti le credenziali di accesso per l'accesso.

Utenti root

Per ripristinare l'accesso all'utente root, è necessario accedere utilizzando un altro dispositivo MFA registrato per lo stesso utente root. Quindi, esamina le seguenti opzioni per ripristinare o aggiornare il tuo dispositivo MFA:

- Per istruzioni dettagliate su come ripristinare un dispositivo MFA, vedi Cosa succede se un dispositivo MFA viene perso o smette di funzionare?
- Per istruzioni dettagliate su come aggiornare un numero di telefono per un dispositivo MFA, vedi Come posso aggiornare il mio numero di telefono per reimpostare il mio dispositivo MFA smarrito?
- Per istruzioni dettagliate sull'attivazione dei dispositivi MFA, consulta Abilitazione dei dispositivi MFA per gli utenti in. AWS
- Se non riesci a ripristinare il tuo dispositivo MFA, contatta. Supporto

> **Note**
>
> Gli utenti IAM devono contattare il proprio amministratore per ricevere assistenza con i dispositivi MFA. Supporto non può assistere gli utenti IAM con problemi relativi ai dispositivi MFA.

Non riesco ad accedere al Console di gestione AWS pagina di accesso

Se non riesci a visualizzare la tua pagina di accesso, il dominio potrebbe essere bloccato da un firewall. Contatta l'amministratore di rete per aggiungere i seguenti domini o endpoint URL agli elenchi di consentiti della tua soluzione di filtraggio dei contenuti web, a seconda del tipo di utente e della modalità di accesso.

Utente root e utenti IAM	*.signin.aws.amazon.com
Amazon.com accesso all'account	www.amazon.com
Accesso agli utenti di IAM Identity Center e alle applicazioni proprietarie	• *.awsapps.com () http://awsapps.com/ • *.signin.aws

Non riesco ad accedere a causa delle condizioni di rete nelle politiche basate sulle risorse Sign-in

Se viene visualizzato uno dei seguenti messaggi di errore, è possibile che una politica Sign-in basata sulle risorse o una politica di controllo delle risorse (RCP) limiti l'accesso in base alla posizione della rete:

- «Le informazioni di autenticazione non sono corrette. Riprova.»
- «Autenticazione fallita Richiesta non valida»
- «Autenticazione non riuscita: per accedere a questo account, accedi da una rete diversa o contatta l'amministratore per ulteriori informazioni»

Contatta l'amministratore o consulta Non riesco ad accedere a causa delle condizioni di rete nelle politiche Sign-in basate sulle risorse la procedura dettagliata per la risoluzione dei problemi.

L'accesso al mio account è bloccato dopo aver abilitato l'autorizzazione della console

Se hai configurato l'autorizzazione della console e non riesci più ad accedere al tuo account, potresti non aver configurato i principali esclusi o l'accesso per il ripristino di emergenza prima di applicare la politica. Per le fasi di risoluzione, tra cui il self-service AWS CLI, le opzioni `OrganizationAccountAccessRole` e AWS Support, consulta. L'accesso al mio account è bloccato dopo aver abilitato l'autorizzazione della console

Le mie modifiche alle politiche non hanno effetto

Le modifiche alla configurazione delle autorizzazioni della console e alle istruzioni di autorizzazione delle risorse vengono replicate a livello globale e potrebbero essere necessari alcuni minuti per diventare effettive. Se le modifiche non sono visibili dopo l'attesa, consulta la procedura Le modifiche che apporto non sono sempre immediatamente visibili per la risoluzione dei problemi.

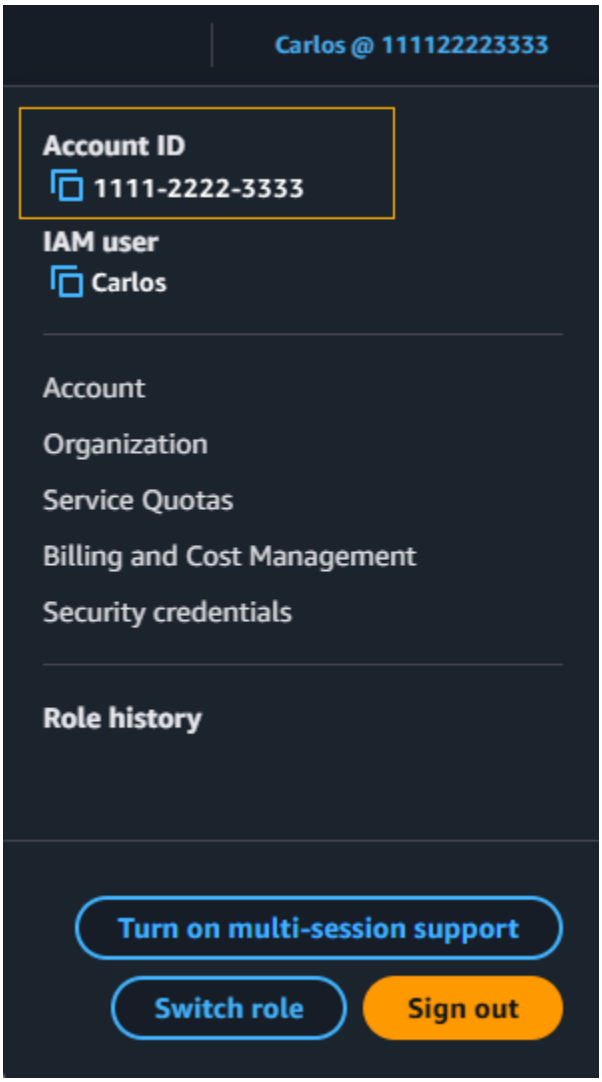
Come posso trovare il mio Account AWS ID o alias

Se sei un utente IAM e non hai effettuato l'accesso, chiedi all'amministratore l' Account AWS ID o l'alias. L'amministratore è in genere un personale IT (Information Technology) che dispone di un

livello di autorizzazioni più elevato Account AWS rispetto agli altri membri dell'organizzazione. Questa persona ha creato l'account e fornisce agli utenti le credenziali di accesso per l'accesso.

Se sei un utente IAM con accesso a Console di gestione AWS, l'ID del tuo account si trova nell'URL di accesso. Controlla le e-mail del tuo amministratore per l'URL di accesso. L'ID dell'account è costituito dalle prime dodici cifre dell'URL di accesso. Ad esempio, nel seguente URL`https://111122223333.signin.aws.amazon.com/console`, il tuo Account AWS ID è 111122223333.

Dopo aver effettuato l'accesso Console di gestione AWS, puoi trovare le informazioni sul tuo account nella barra di navigazione accanto alla tua regione. Ad esempio, nella schermata seguente, l'utente IAM Carlos ha un valore Account AWS di 1111-2222-3333.



Per ulteriori informazioni sul tuo Account AWS ID e alias e su come trovarli, vedi Il tuo ID e il suo alias. Account AWS

Ho bisogno del codice di verifica dell'account

Se hai fornito l'indirizzo e-mail e la password del tuo account, AWS a volte è necessario fornire un codice di verifica valido una tantum. Per recuperare il codice di verifica, controlla l'e-mail associata al tuo indirizzo Account AWS per cercare un messaggio da Amazon Web Services. L'indirizzo e-mail termina con @signin .aws o @verify .signin.aws. Seguire le istruzioni nel messaggio. Se non vedi il messaggio nel tuo account, controlla le cartelle spam e posta indesiderata. Se non si dispone più dell'accesso all'e-mail, consultare Non ho accesso all'e-mail del mio Account AWS.

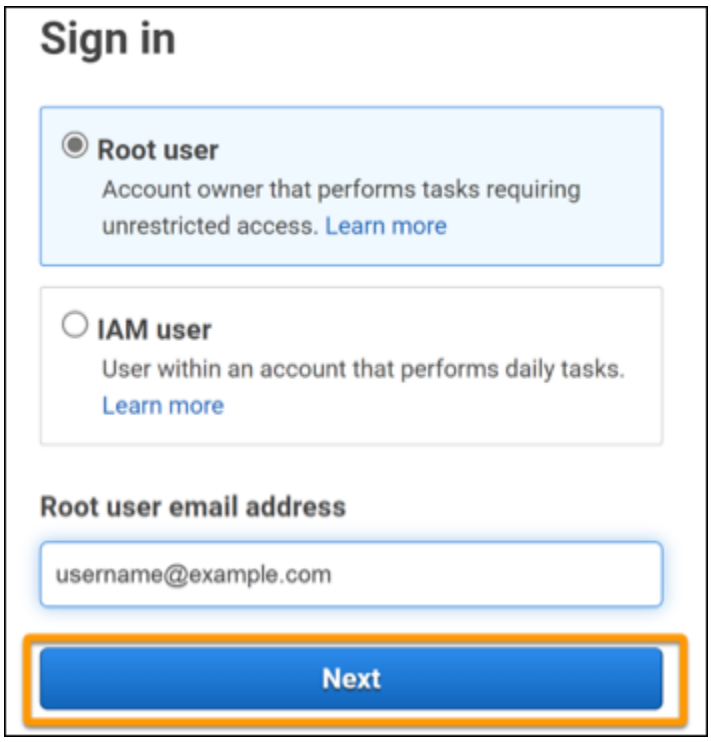
Ho dimenticato la password dell'utente root per il mio Account AWS

Se sei un utente root e hai perso o dimenticato la password del tuo account Account AWS, puoi reimpostarla selezionando il link «Password dimenticata» nel Console di gestione AWS. Devi conoscere l'indirizzo e-mail del tuo AWS account e devi avere accesso all'account e-mail. Durante il processo di recupero della password, ti verrà inviato via email un link per reimpostare la password. Il link verrà inviato all'indirizzo e-mail che hai utilizzato per creare il tuo Account AWS.

Per reimpostare la password per un account creato utilizzando AWS Organizations, vedi Accesso a un account membro come utente root.

Per reimpostare la password dell'utente root

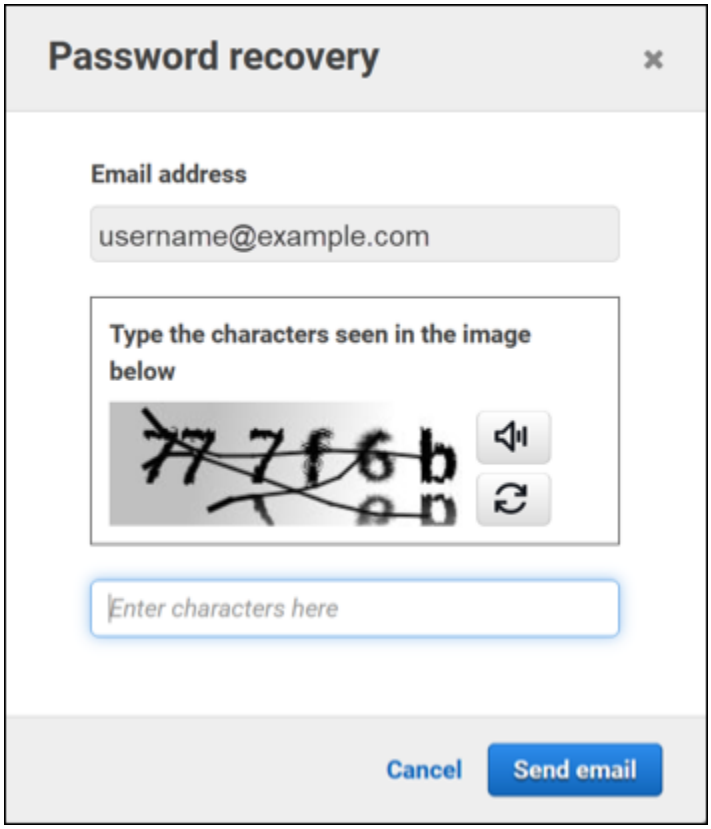
1. Usa il tuo indirizzo AWS e-mail per iniziare ad accedere alla Console di AWS gestione come utente root. Quindi, seleziona Successivo.



> **Note**
>
> Se hai effettuato l'accesso Console di gestione AWScon le credenziali utente IAM, devi disconnetterti prima di poter reimpostare la password dell'utente root. Se vedi la pagina di accesso utente IAM specifica per l'account, scegli di Sign-in utilizzare le credenziali dell'account root nella parte inferiore della pagina. Se necessario, fornisci l'indirizzo e-mail dell'account e scegli Next (Avanti) per accedere alla pagina Root user sign in (Accesso utente root).

2. Scegli Password dimenticata?

3. Completa i passaggi per il recupero della password. Se non riesci a completare il controllo di sicurezza, prova ad ascoltare l'audio o ad aggiornare il controllo di sicurezza per un nuovo set di caratteri. Un esempio di pagina di recupero della password è mostrato nell'immagine seguente.

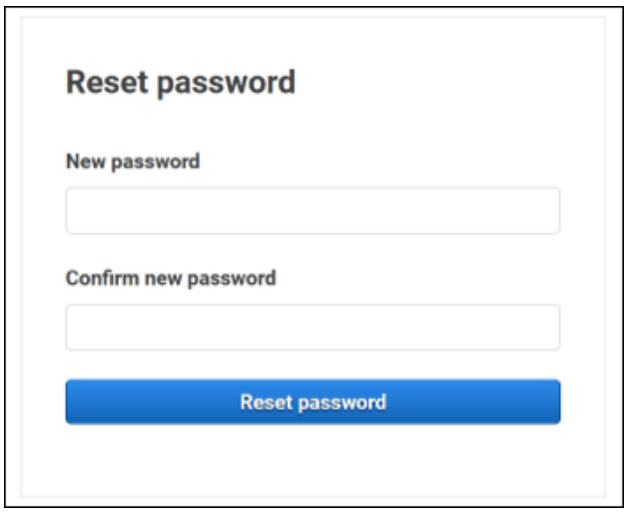


4. Dopo aver completato la procedura di recupero della password, riceverai un messaggio che ti comunica che sono state inviate ulteriori istruzioni all'indirizzo e-mail associato al tuo Account AWS.

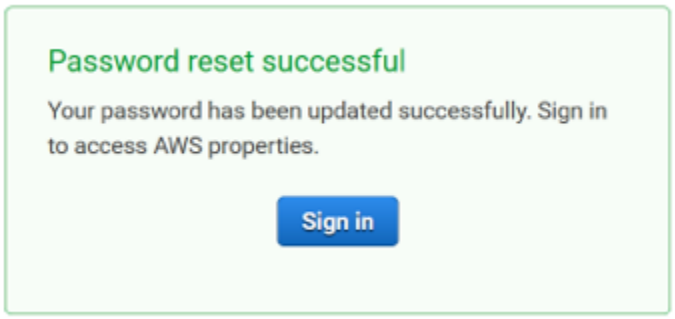
   Un'e-mail con un link per reimpostare la password viene inviata all'indirizzo e-mail utilizzato per creare il Account AWS.

   > **Note**
   >
   > L'e-mail verrà inviata da un indirizzo che termina con @signin .aws o @verify .signin.aws.

5. Seleziona il link fornito nell' AWS e-mail per reimpostare la password dell'utente root. AWS
6. Il link ti indirizza a una nuova pagina web per creare una nuova password per l'utente root.



Riceverai una conferma che la reimpostazione della password è avvenuta con successo. L'immagine seguente mostra una corretta reimpostazione della password.



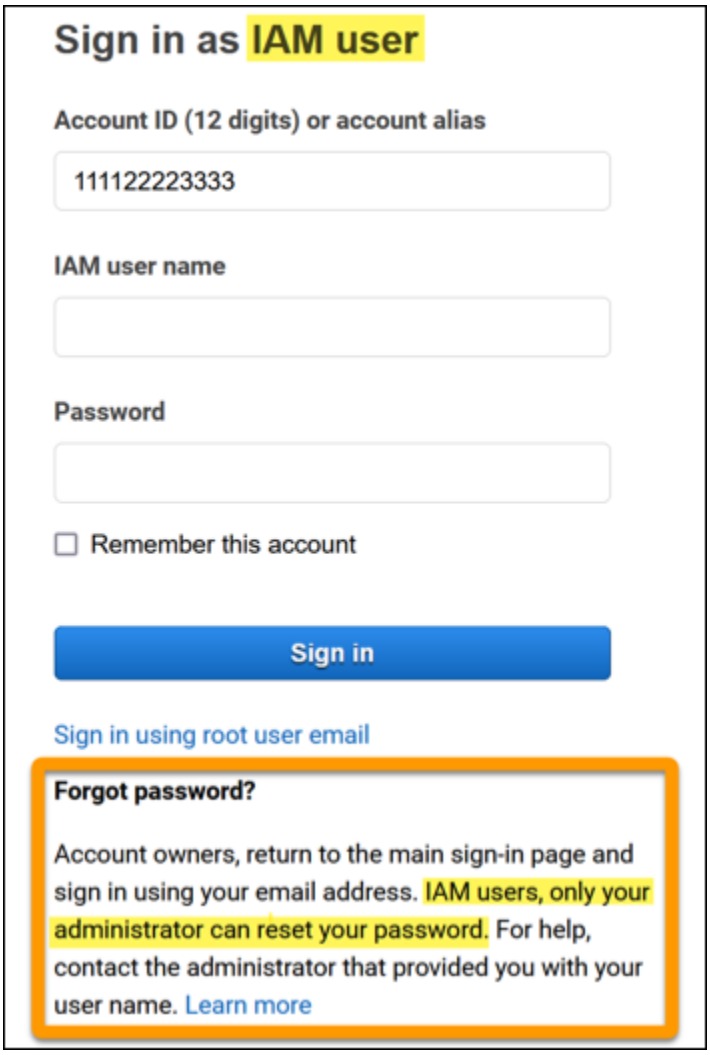
Per ulteriori informazioni sulla reimpostazione della password dell'utente root, vedi Come posso recuperare una password persa o dimenticata? AWS

Ho dimenticato la mia password utente IAM per il mio Account AWS

Per modificare la password utente IAM, devi disporre delle autorizzazioni appropriate. Per ulteriori informazioni sulla reimpostazione della password utente IAM, consulta Come un utente IAM cambia la propria password.

Se non disponi dell'autorizzazione per reimpostare la password, solo l'amministratore IAM può reimpostare la password utente IAM. Gli utenti IAM devono contattare il proprio amministratore IAM per reimpostare la password. L'amministratore è in genere un personale IT (Information Technology) che dispone di un livello di autorizzazioni più elevato Account AWS rispetto agli altri

membri dell'organizzazione. Questa persona ha creato l'account e fornisce agli utenti le credenziali di accesso per l'accesso.



Per motivi di sicurezza, Supporto non ha accesso per visualizzare, fornire o modificare le tue credenziali.

Per ulteriori informazioni sulla reimpostazione della password utente IAM, vedi Come posso recuperare una password persa o dimenticata? AWS

Per sapere come un amministratore può gestire la tua password, consulta Gestione delle password per gli utenti IAM.

Ho dimenticato la mia password di identità federata per il mio Account AWS

Le identità federate accedono per accedere Account AWS con identità esterne. Il tipo di identità esterna in uso determina il modo in cui le identità federate accedono. L'amministratore crea le identità federate. Rivolgiti all'amministratore per maggiori dettagli su come reimpostare la password. L'amministratore è in genere un personale IT (Information Technology) che dispone di un livello di autorizzazioni più elevato Account AWS rispetto agli altri membri dell'organizzazione. Questa persona ha creato l'account e fornisce agli utenti le credenziali di accesso per l'accesso.

Non riesco ad accedere al mio account esistente Account AWS e non riesco a crearne uno nuovo Account AWS con lo stesso indirizzo email

È possibile associare un indirizzo e-mail a uno solo Utente root dell'account AWS. Se chiudi il tuo account utente root e questo rimane chiuso per più di 90 giorni, non potrai riaprire l'account o crearne uno nuovo Account AWS utilizzando l'indirizzo e-mail associato a questo account.

Per risolvere questo problema, puoi utilizzare il sottoindirizzamento in cui aggiungi un segno più (+) dopo il tuo indirizzo e-mail abituale quando registri un nuovo account. Il segno più (+) può essere seguito da lettere maiuscole o minuscole, numeri o altri caratteri supportati dal Simple Mail Transfer Protocol (SMTP). Ad esempio, puoi usare `email+1@yourcompany.com` o `email+tag@yourcompany.com` dove si trova la tua email abituale. `email@yourcompany.com` Questo è considerato un nuovo indirizzo anche se è collegato alla stessa casella di posta in arrivo del tuo indirizzo email abituale. Prima di registrare un nuovo account, ti consigliamo di inviare un'email di prova all'indirizzo e-mail aggiunto per confermare che il tuo provider di posta elettronica supporti il subindirizzamento.

Devo riattivare il mio account sospeso Account AWS

Se il tuo Account AWS è sospeso e desideri ripristinarlo, vedi Come posso riattivare il mio dispositivo sospeso? Account AWS

Devo contattare Supporto per problemi di accesso

Se hai provato tutto, puoi ricevere assistenza Supporto completando la richiesta Billing and Account Support.

Devo contattare AWS Billing per problemi di fatturazione

Se non riesci ad accedere al tuo account Account AWS e desideri contattarci AWS Billing per problemi di fatturazione, puoi farlo tramite una richiesta di Billing and Account Support. Per ulteriori informazioni Gestione dei costi e fatturazione AWS, inclusi addebiti e metodi di pagamento, consulta Ottenere assistenza per. AWS Billing

Ho una domanda su un ordine al dettaglio

Se hai un problema con il tuo account www.amazon.com o una domanda su un ordine al dettaglio, consulta Opzioni di supporto e Contattaci.

Ho bisogno di aiuto per gestire il mio Account AWS

Se hai bisogno di aiuto per cambiare una carta di credito Account AWS, segnalare attività fraudolente o chiudere la tua Account AWS, consulta Risoluzione di altri problemi con. Account AWS

Il mio AWS le credenziali del portale di accesso non funzionano

Quando non riesci ad accedere al tuo portale di AWS accesso, prova a ricordare come hai effettuato l'accesso AWS in precedenza.

Se non ricordi di aver usato una password

Potresti aver effettuato l'accesso in precedenza AWS senza utilizzare AWS credenziali. Questo è comune per il single sign-on aziendale tramite IAM Identity Center. L'accesso in AWS questo modo significa che si utilizzano le credenziali aziendali per accedere agli AWS account o alle applicazioni senza inserire le proprie credenziali.

- AWS portale di accesso: se un amministratore consente di utilizzare credenziali esterne AWS per accedere AWS, è necessario l'URL del portale. Controlla la tua e-mail, i preferiti del browser o la

cronologia del browser per trovare un URL che includa `awsapps.com/start` o `signin.aws/platform/login`.

Ad esempio, il tuo URL personalizzato potrebbe includere un ID o un dominio come `https://d-1234567890.awsapps.com/start`. Se non riesci a trovare il link al portale, contatta l'amministratore. Supporto non posso aiutarti a recuperare queste informazioni.

Se ricordi nome utente e password, ma le credenziali non funzionano, potresti trovarti nella pagina sbagliata. Controlla l'URL nel tuo browser web, se è, https://signin.aws.amazon.com/ allora un utente federato o un utente di IAM Identity Center non può accedere utilizzando le proprie credenziali.

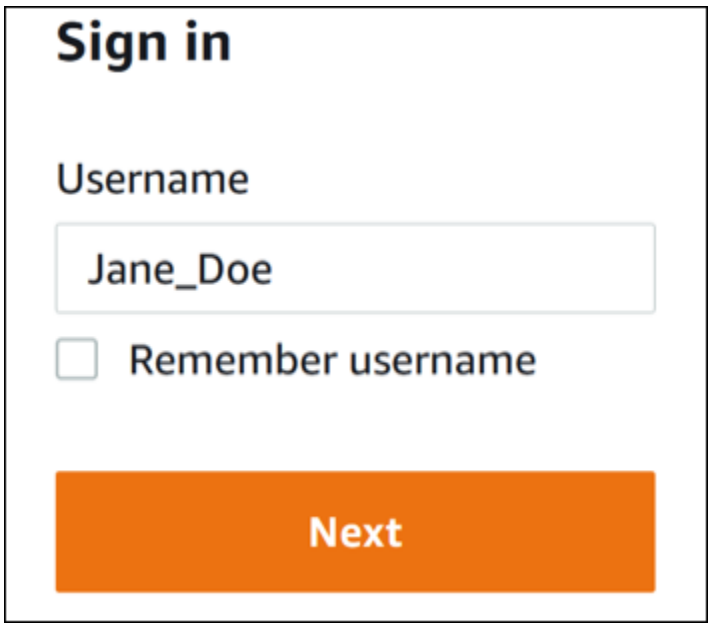
- AWS portale di accesso: se un amministratore configura una fonte di identità AWS IAM Identity Center (successore di AWS Single Sign-On) per AWS, devi accedere utilizzando il tuo nome utente e password al portale di AWS accesso per la tua organizzazione. Per individuare l'URL del portale, controlla la posta elettronica, l'archiviazione sicura delle password, i preferiti del browser o la cronologia del browser per individuare un URL che includa `awsapps.com/start` `osignin.aws/platform/login`. Ad esempio, l'URL personalizzato potrebbe includere un ID o un dominio, ad esempio `https://d-1234567890.awsapps.com/start.` Se non riesci a trovare il link al portale, contatta l'amministratore. Supporto non posso aiutarti a recuperare queste informazioni.

Ho dimenticato la password del mio IAM Identity Center Account AWS

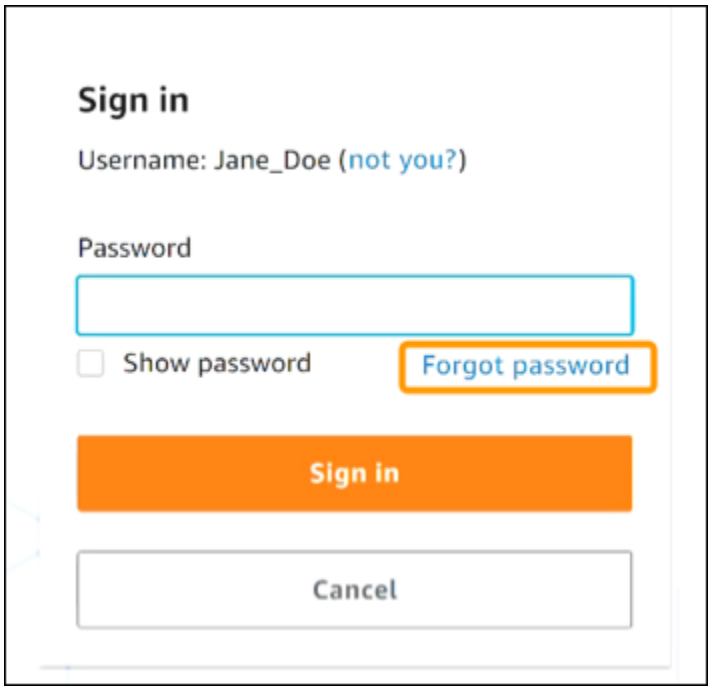
Se sei un utente di IAM Identity Center e hai perso o dimenticato la password del tuo account Account AWS, puoi reimpostarla. Devi conoscere l'indirizzo e-mail utilizzato per l'account IAM Identity Center e potervi accedere. Un link per reimpostare la password viene inviato alla tua Account AWS email.

Per reimpostare la password dell'utente in IAM Identity Center

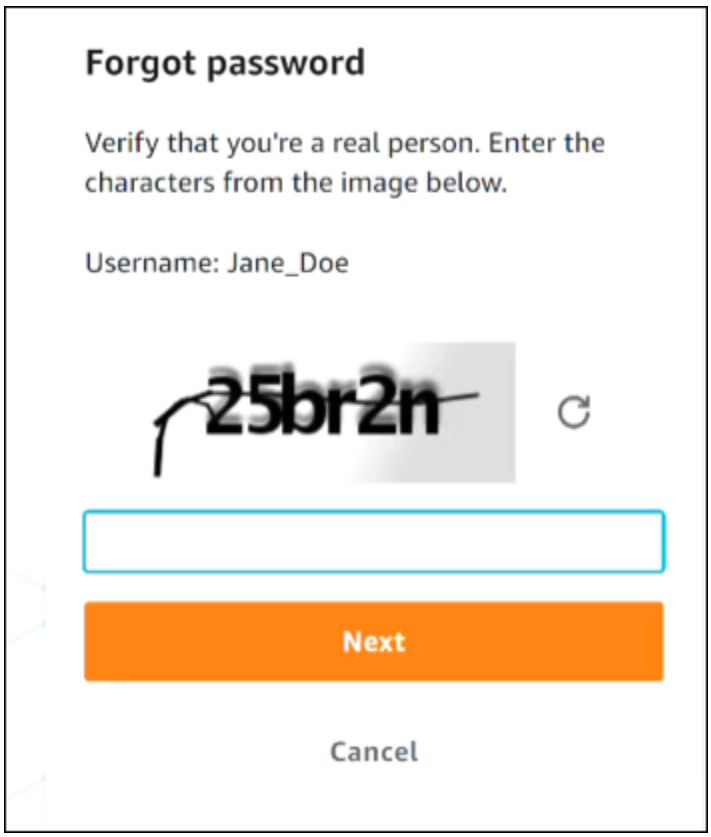
1. Usa il link URL del portale di AWS accesso e inserisci il tuo nome utente. Quindi, seleziona Successivo.



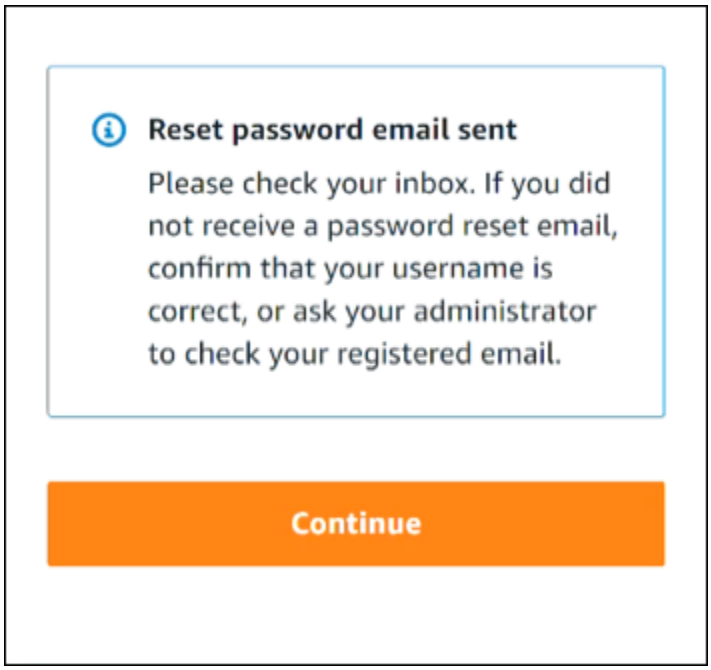
2. Seleziona Password dimenticata come mostrato nell'immagine seguente.



3. Completa i passaggi per il recupero della password.



4. Dopo aver completato la procedura di recupero della password, ricevi il seguente messaggio che conferma che ti è stato inviato un messaggio e-mail che puoi utilizzare per reimpostare la password.



Un'e-mail con un link per reimpostare la password viene inviata all'e-mail associata all'account utente IAM Identity Center. Seleziona il link fornito nell' AWS e-mail per reimpostare la password. Il link ti indirizza a una nuova pagina Web per creare una nuova password. Dopo aver creato una nuova password, riceverai la conferma che la reimpostazione della password è avvenuta con successo.

Se non hai ricevuto un'e-mail per reimpostare la password, chiedi all'amministratore di confermare quale e-mail è registrata con il tuo utente in IAM Identity Center.

Ricevo un messaggio di errore che dice «Non sei tu, siamo noi» quando provo ad accedere alla console IAM Identity Center

Questo errore indica che c'è un problema di configurazione con l'istanza di IAM Identity Center o con il provider di identità esterno (IdP) che utilizza come fonte di identità. Ti consigliamo di verificare quanto segue:

- Verifica le impostazioni di data e ora sul dispositivo che stai utilizzando per accedere. Ti consigliamo di consentire l'impostazione automatica di data e ora. Se non è disponibile, ti consigliamo di sincronizzare la data e l'ora con un server Network Time Protocol (NTP) noto.
- Verifica che il certificato IdP caricato su IAM Identity Center sia lo stesso fornito dal tuo provider di identità. Puoi controllare il certificato dalla console IAM Identity Center accedendo a Impostazioni. Nella scheda Identity Source, in Azione, scegli Gestisci autenticazione. Potrebbe essere necessario importare un nuovo certificato.
- Nel file di metadati SAML del tuo IdP, assicurati che il formato NameID sia. `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
- Se utilizzi AD Connector, verifica che le credenziali per l'account di servizio siano corrette e non siano scadute. Per ulteriori informazioni, consulta Aggiornare le credenziali dell'account del servizio AD Connector in Directory Service.

Risoluzione dei problemi relativi al AWS Builder ID

Utilizza le informazioni qui per aiutarti a risolvere i problemi che potresti avere con il tuo. ID Builder AWS

Argomenti

- Ricevo il messaggio «Non sei tu, siamo noi» quando provo ad accedere a Builder ID AWS
- La disconnessione non mi disconnette completamente
- Sto ancora cercando di risolvere il mio problema

La mia e-mail è già in uso

Se l'email che hai inserito è già in uso e la riconosci come tua, allora potresti aver già registrato un AWS Builder ID. Prova ad accedere utilizzando quell'indirizzo e-mail. Se non ricordi la password, consulta Ho dimenticato la mia password.

Non è possibile completare la verifica dell'e-mail

Se ti sei registrato a AWS Builder ID ma non hai ricevuto l'email di verifica, completa le seguenti attività di risoluzione dei problemi.

1. Controlla la cartella dello spam, della posta indesiderata e degli elementi eliminati.

   > **Note**
   >
   > Questa email di verifica proviene dall'indirizzo no-reply@signin.aws o no-reply@login.awsapps.com. Ti consigliamo di configurare il tuo sistema di posta in modo che accetti le e-mail da questi indirizzi del mittente e non le gestisca come posta indesiderata o spam.

2. Scegli Resend code (Reinvia codice), aggiorna la tua casella di posta e controlla nuovamente le cartelle dello spam, della posta indesiderata e degli elementi eliminati.
3. Se continui a non visualizzare l'email di verifica, ricontrolla l'indirizzo email del AWS Builder ID per eventuali errori di battitura. Se hai inserito l'indirizzo e-mail sbagliato, registrati nuovamente con un indirizzo e-mail di tua proprietà.

Non riesco ad accedere con Google

Se hai già un ID Builder AWS profilo con lo stesso indirizzo email del tuo account Google, usa ID Builder AWS la password per accedere al tuo account. Se non ricordi la password, consulta Ho dimenticato la mia password.

Per assistenza nell'accesso con la tua password Google, vedi Impossibile accedere al tuo account Google.

Non riesco ad accedere con Apple

Se hai già un ID Builder AWS profilo con lo stesso indirizzo email del tuo account Apple, usa ID Builder AWS la password per accedere al tuo account. Se non ricordi la password, consulta Ho dimenticato la mia password.

Per assistenza nell'accesso con la tua password Apple, vedi Se non riesci ad accedere al tuo account Apple.

Non riesco ad accedere con GitHub

Se hai già un ID Builder AWS profilo con lo stesso indirizzo email del tuo GitHub account, usa ID Builder AWS la password per accedere al tuo account. Se non ricordi la password, consulta Ho dimenticato la mia password.

Per assistenza nell'accesso con GitHub la password, vedi Impossibile accedere - GitHub Support.

Non riesco ad accedere con Amazon

Se disponi di un ID Builder AWS profilo esistente con lo stesso indirizzo e-mail del tuo account Amazon, usa ID Builder AWS la password per accedere al tuo account. Se non ricordi la password, consulta Ho dimenticato la mia password.

Per assistenza nell'accesso con la tua password Amazon, consulta Aiuto per l'accesso.

Ho ricevuto un errore di accesso quando ho provato a registrarmi per ID Builder AWS utilizzare Continue with Google

Ciò significa che ne hai già uno che ID Builder AWS utilizza lo stesso indirizzo email del tuo account Google o che l'indirizzo email associato al tuo account Google non è verificato. In entrambi i casi, prova a registrarti nuovamente inserendo il tuo indirizzo email e fornendo una password.

Ho ricevuto un errore di accesso quando ho provato a registrarmi per continuare ID Builder AWS con Apple

Ciò significa che ne hai già uno che ID Builder AWS usa lo stesso indirizzo email del tuo account Apple oppure che l'indirizzo email associato al tuo account Apple non è verificato o non è gestito dalla tua azienda con Apple Business Manager o dalla tua scuola con Apple School Manager. In entrambi i casi, prova a registrarti nuovamente inserendo il tuo indirizzo email e fornendo una password.

Ho ricevuto un errore di accesso quando ho provato a registrarmi per ID Builder AWS utilizzare continue con GitHub

Ciò significa che già ID Builder AWS utilizzi lo stesso indirizzo email del tuo GitHub Account oppure che l'indirizzo email associato al tuo GitHub Account non è verificato. In entrambi i casi, prova a registrarti nuovamente inserendo il tuo indirizzo email e fornendo una password.

Ho ricevuto un errore di accesso quando ho provato a registrarmi per ID Builder AWS utilizzare continue with Amazon

Ciò significa che ne hai già uno che ID Builder AWS utilizza lo stesso indirizzo e-mail del tuo account Amazon o che l'indirizzo e-mail associato al tuo account Amazon non è verificato. In entrambi i casi, prova a registrarti nuovamente inserendo il tuo indirizzo e-mail e fornendo una password.

Ricevo un messaggio di errore che dice «Non sei tu, siamo noi» quando provo ad accedere con il mio ID Builder AWS

Se ricevi questo messaggio di errore quando tenti di accedere, potrebbe esserci un problema con le impostazioni locali o l'indirizzo email.

- Verifica le impostazioni di data e ora sul dispositivo che stai utilizzando per accedere. Ti consigliamo di consentire l'impostazione automatica di data e ora. Se non è disponibile, ti consigliamo di sincronizzare la data e l'ora con un server Network Time Protocol (NTP) noto.
- Controlla il tuo indirizzo email per eventuali errori di formattazione. I seguenti problemi restituiranno un errore quando provi ad accedere con il tuo ID Builder AWS.
  - Spazio in un indirizzo email
  - Barra (/) in un indirizzo e-mail

- Due punti (.) in un indirizzo e-mail
- Due e commerciali (@) in un indirizzo e-mail
- Virgola (,) alla fine di un indirizzo e-mail
- Parentesi (]) alla fine di un indirizzo e-mail

Ho dimenticato la mia password

Reimpostazione della password dimenticata

1. Nella pagina Accedi con AWS Builder ID, inserisci l'email che hai usato per creare il tuo ID AWS Builder in Indirizzo e-mail. Scegli Next (Successivo).
2. Seleziona Forgot Password? (Password dimenticata?). Inviamo un link all'indirizzo email associato al tuo ID AWS Builder dove puoi reimpostare la password.
3. Segui le istruzioni nell'e-mail.

Non riesco a impostare una nuova password

Per motivi di sicurezza, devi seguire questi requisiti ogni volta che imposti o modifichi la password:

- Le password distinguono tra maiuscole e minuscole.
- La lunghezza delle password deve essere compresa tra 8 e 64 caratteri.
- Le password devono contenere almeno un carattere per ognuna delle quattro categorie seguenti:
  - Lettere minuscole (a-z)
  - Lettere maiuscole (A-Z)
  - Numeri (0-9)
  - Caratteri non alfanumerici (~!@#$%^portale di gestione*_-+=`|\(){}[]:;'"<>,.?/)
- Le ultime tre password non possono essere riutilizzate.
- Le password che sono note pubblicamente attraverso un set di dati divulgato da terze parti non possono essere utilizzate.

La mia password non funziona

Se ricordi la password, ma non funziona quando accedi con AWS Builder ID, assicurati che:

- Il blocco delle maiuscole sia disattivato.
- Non stai utilizzando una password più vecchia.
- Stai usando la tua password AWS Builder ID e non una password per un. Account AWS

Se verifichi che la password up-to-date sia stata inserita correttamente, ma continua a non funzionare, segui le istruzioni Ho dimenticato la mia password per reimpostare la password.

La mia password non funziona e non riesco più ad accedere alle e-mail inviate al mio indirizzo e-mail AWS Builder ID

Se riesci ancora ad accedere al tuo AWS Builder ID, usa la pagina Profilo per aggiornare l'email del tuo AWS Builder ID con il tuo nuovo indirizzo email. Dopo aver completato la verifica dell'email, potrai accedere AWS e ricevere comunicazioni al tuo nuovo indirizzo email.

Se hai utilizzato un indirizzo e-mail aziendale o universitario e hai lasciato l'azienda o la scuola e non riesci a ricevere alcuna e-mail inviata a quell'indirizzo, contatta l'amministratore del sistema di posta elettronica. Potrebbero essere in grado di inoltrare la tua e-mail a un nuovo indirizzo, concederti un accesso temporaneo o condividere contenuti dalla tua casella di posta.

Non riesco ad abilitare l'MFA

Per abilitare l'autenticazione a più fattori, aggiungi uno o più dispositivi MFA al tuo profilo seguendo i passaggi riportati in Gestione dell' ID Builder AWS autenticazione a più fattori (MFA).

Non riesco ad aggiungere un'app di autenticazione come dispositivo MFA

Se non riesci ad aggiungere un altro dispositivo MFA, potresti aver raggiunto il limite di dispositivi MFA che puoi registrare in quell'applicazione. Prova a rimuovere un dispositivo MFA inutilizzato o a utilizzare un'altra app di autenticazione.

Non riesco a rimuovere un dispositivo MFA

Se desideri disabilitare l'autenticazione a più fattori, procedi con la rimozione del dispositivo MFA seguendo i passaggi riportati in Eliminare il dispositivo MFA. Tuttavia, se desideri lasciare l'MFA

abilitata, prima di provare a eliminare un dispositivo MFA esistente dovrai aggiungere un altro dispositivo MFA. Per ulteriori informazioni sull'aggiunta di un altro dispositivo MFA, consulta Gestione dell' ID Builder AWS autenticazione a più fattori (MFA).

Ricevo il messaggio "An unexpected error has occurred" (Si è verificato un errore imprevisto) quando provo a registrarmi o accedere con un'app di autenticazione

Un sistema di password monouso (TOTP) basato sul tempo, come quello utilizzato da AWS Builder ID in combinazione con un'app di autenticazione basata su codice, si basa sulla sincronizzazione temporale tra il client e il server. Assicurati che il dispositivo su cui è installata l'app di autenticazione sia sincronizzato correttamente con una fonte temporale affidabile oppure imposta manualmente l'ora sul dispositivo in modo che corrisponda a una fonte affidabile, come NIST o altri equivalenti. local/ regional

Ricevo il messaggio «Non sei tu, siamo noi» quando provo ad accedere a Builder ID AWS

Verifica le impostazioni di data e ora sul dispositivo che stai utilizzando per accedere. Ti consigliamo di impostare la data e l'ora in modo che vengano impostate automaticamente. Se non è disponibile, ti consigliamo di sincronizzare la data e l'ora con un server Network Time Protocol (NTP) noto.

La disconnessione non mi disconnette completamente

Il sistema è progettato per disconnettersi immediatamente, ma la disconnessione completa può richiedere fino a un'ora.

> **Note**
>
> Quando utilizzi un account di accesso social come Google o Apple, l'eliminazione delle ID Builder AWS sessioni attive non ti disconnetterà dal tuo account di accesso social.

Sto ancora cercando di risolvere il mio problema

Puoi compilare il modulo di feedback per l'assistenza. Nella sezione Richiedi informazioni, sotto Come possiamo aiutarti, indica che stai utilizzando AWS Builder ID. Fornisci il maggior numero di dettagli possibile in modo che possiamo risolvere il problema nel modo più efficiente.

AWS politiche gestite per Accedi ad AWS

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i propri casi d'uso.

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

Per ulteriori informazioni, consultare Policy gestite da AWS nella Guida per l'utente di IAM.

AWS politica gestita: AmazonManagedSignUpServicePolicy

La `AmazonManagedSignUpServicePolicy` politica concede le autorizzazioni necessarie per completare i processi di registrazione AWS dell'account.

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

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- Verifica del cliente: consente di creare, recuperare e aggiornare i dettagli di verifica del cliente e lo stato di idoneità, inclusa la creazione di URL di caricamento per i documenti di verifica.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta AmazonManagedSignUpServicePolicy nella Guida di riferimento alle policy gestite da AWS .

AWS politica gestita: ApplicationProvisioningPolicy

La ApplicationProvisioningPolicy policy concede autorizzazioni complete per le operazioni di provisioning delle applicazioni e di gestione delle identità, tra cui la gestione dei ruoli e delle policy IAM, la configurazione SSO e le operazioni di archiviazione delle identità.

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

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- Gestione IAM: consente operazioni IAM complete, tra cui la creazione, l'aggiornamento e l'eliminazione di ruoli e policy, la gestione degli allegati dei ruoli e la creazione di ruoli collegati ai servizi.
- Studio di ricerca e ingegneria su AWS- Consente tutte le operazioni sulle risorse. Studio di ricerca e ingegneria su AWS
- Passaggio di ruoli: consente di passare i ruoli IAM ad altri servizi.
- IAM Identity Center: consente di gestire istanze, applicazioni, assegnazioni, concessioni e metodi di autenticazione di IAM Identity Center.
- Identity Store: consente di leggere le informazioni su utenti e gruppi dall'Identity Store.
- IAM Identity Center OAuth: consente l'autenticazione delle sessioni IAM tramite IAM Identity Center OAuth.
- Profilo utente e directory: consente di gestire i connettori, i profili utente e le configurazioni delle directory di IAM Identity Center, inclusa la configurazione del provider di identità esterno.
- Sottoscrizioni utente: consente di elencare le sottoscrizioni degli utenti.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta ApplicationProvisioningPolicy nella Guida di riferimento alle policy gestite da AWS .

AWS politica gestita: SignInLocalDevelopmentAccess

La `SignInLocalDevelopmentAccess` policy concede le autorizzazioni per l'accesso programmatico all' AWS utilizzo delle credenziali della console.

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

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- Autorizzazione dell'accesso OAuth2: concede l'autorizzazione all'autenticazione tramite un browser e all'ottenimento di un codice di autorizzazione OAuth 2.0 per lo scambio di credenziali
- Creazione di token OAuth2: concede l'autorizzazione a scambiare un codice di autorizzazione per il token di accesso e il token di aggiornamento OAuth 2.0 che può essere utilizzato per accedere ai servizi da strumenti e applicazioni di sviluppo AWS

> **Note**
>
> L'aggiunta di questa policy AWS gestita consente l'autorizzazione sia per l'autenticazione sullo stesso dispositivo che per quella su più dispositivi. Questa politica autorizza azioni sulle seguenti risorse:
>
> - `arn:aws:signin:region:account-id:oauth2/public-client/localhost`— Utilizzato per l'autenticazione sullo stesso dispositivo con. `aws login`
> - `arn:aws:signin:region:account-id:oauth2/public-client/remote`— Utilizzato per l'autenticazione tra dispositivi con. `aws login --remote`
>
> Per controllare l'accesso a entrambi i metodi di autenticazione, è possibile creare una politica gestita o una politica di controllo del servizio (SCP) personalizzata. Utilizza questi ARN di risorse per consentire o negare l'accesso programmatico ad AWS utilizzando le credenziali della console.

Per ulteriori informazioni, consulta Accedi con le credenziali della console (consigliato). Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta SignInLocalDevelopmentAccess nella Guida di riferimento alle policy gestite da AWS .

AWS politica gestita: AWSSignInResourcePolicyManagement

La `AWSSignInResourcePolicyManagement` politica concede le autorizzazioni per gestire la configurazione delle autorizzazioni della console e le dichiarazioni di autorizzazione delle risorse per. AWS Sign-In

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

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `signin:PutConsoleAuthorizationConfiguration`— Creare o aggiornare le impostazioni di autorizzazione della console.
- `signin:GetConsoleAuthorizationConfiguration`— Recupera la configurazione di autorizzazione corrente della console.
- `signin:DeleteConsoleAuthorizationConfiguration`— Rimuovere la configurazione di autorizzazione della console.
- `signin:PutResourcePermissionStatement`— Creare o aggiornare le dichiarazioni di autorizzazione delle risorse.
- `signin:DeleteResourcePermissionStatement`— Rimuovere le dichiarazioni di autorizzazione delle risorse.
- `signin:ListResourcePermissionStatements`— Elenca le dichiarazioni di autorizzazione delle risorse per l'account.
- `signin:GetResourcePolicy`— Recupera la politica consolidata basata sulle risorse.

Di seguito è riportata la politica JSON:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "signin:PutConsoleAuthorizationConfiguration",
                "signin:GetConsoleAuthorizationConfiguration",
                "signin:DeleteConsoleAuthorizationConfiguration",
                "signin:PutResourcePermissionStatement",
                "signin:DeleteResourcePermissionStatement",
                "signin:ListResourcePermissionStatements",
                "signin:GetResourcePolicy"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Allega questa policy ai responsabili IAM (utenti o ruoli) che gestiscono le policy basate sulle risorse per. AWS Sign-In Ciò include gli amministratori di sicurezza responsabili della configurazione dei controlli di accesso basati sulla rete, i responsabili della conformità che devono verificare le politiche di accesso alla console e i team operativi che gestiscono le configurazioni di accesso per il ripristino di emergenza.

> **Important**
>
> Questa politica garantisce l'accesso amministrativo ai controlli di autorizzazione della console. Applica il principio del privilegio minimo nell'assegnazione di questa politica. Prendi in considerazione l'utilizzo delle condizioni IAM per limitare ulteriormente quando e come queste autorizzazioni possono essere utilizzate.

Per visualizzare ulteriori dettagli sulla policy, inclusa la versione più recente del documento di policy JSON, consulta AWSSignInResourcePolicyManagement nella Guida di riferimento alle policy gestite da AWS .

Accedi ad AWS aggiornamenti a AWS policy gestite

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

Modifica	Descrizione	Data
AWSSignInResourcePolicyManagement: nuova policy	È stata aggiunta una nuova politica AWS gestita che concede le autorizzazioni per gestire la configurazione delle autorizzazioni della console e le dichiarazioni di autorizzazione delle risorse per. AWS Sign-In	10 giugno 2026

Modifica	Descrizione	Data
SignInLocalDevelopmentAccess: nuova policy	È stata aggiunta una nuova policy AWS gestita che concede le autorizzazioni per l'accesso programmatico all' AWS utilizzo delle credenziali della console esistenti.	19 novembre 2025
ApplicationProvisioningPolicy: nuova policy	È stata aggiunta una nuova policy AWS gestita che concede autorizzazioni complete per le operazioni di provisioning delle applicazioni e di gestione delle identità, tra cui la gestione dei ruoli e delle policy IAM, la configurazione di IAM Identity Center e le operazioni di Identity Store.	30 settembre 2025
AmazonManagedSignUpServicePolicy: nuova policy	È stata aggiunta una nuova policy AWS gestita che concede le autorizzazioni necessarie per i processi di registrazione AWS dell'account, comprese le operazioni di verifica dei clienti e di configurazione dei pagamenti.	30 settembre 2025
Accedi ad AWS ha iniziato a tenere traccia delle modifiche	Accedi ad AWS ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	30 settembre 2025

Cronologia dei documenti

La tabella seguente descrive importanti aggiunte alla AWS Sign-In documentazione. Inoltre, aggiorniamo frequentemente la documentazione tenendo conto dei feedback ricevuti.

- Ultimo aggiornamento importante della documentazione: 10 giugno 2026

Modifica	Descrizione	Data
Support per politiche Sign-in basate sulle risorse e politiche di controllo delle risorse	È stata aggiunta la documentazione per il controllo degli Console di gestione AWS accessi utilizzando politiche Sign-in basate sulle risorse e politiche di controllo delle risorse (RCP), un nuovo riferimento alle chiavi di condizione, la politica gestita e la relativa risoluzione dei problemi. `AWSSignInResourcePolicyManagement`	10 giugno 2026
Support per Sign in with GitHub e Amazon	Accedi ad AWS ora supporta Accedi con GitHub e Accedi con Amazon in modo da poter creare un account ID Builder AWS utilizzando il tuo account GitHub o Amazon.	10 marzo 2026
Support per l'accesso con Apple	Accedi ad AWS ora supporta l'accesso con Apple, quindi puoi crearne uno ID Builder AWS utilizzando il tuo account Apple. ID Builder AWS argomenti aggiornati e nuovi	5 febbraio 2026

	argomenti per la risoluzione dei problemi aggiunti a Risoluzione dei ID Builder AWS problemi.	
Nuova politica gestita	Accedi ad AWS ha rilasciato una nuova politica gestita. `SignInLocalDevelopmentAccess` concede le autorizzazioni per l'accesso programmatico per l'accesso programmatico all' AWS utilizzo delle credenziali della console esistenti. Per informazioni, consulta Accedi ad AWS gli aggiornamenti delle politiche gestite. AWS	19 novembre 2025
Support per l'accesso con Google	Accedi ad AWS ora supporta l'accesso con Google, quindi puoi crearne uno ID Builder AWS utilizzando il tuo account Google. ID Builder AWS argomenti aggiornati e nuovi argomenti per la risoluzione dei problemi aggiunti a Risoluzione dei ID Builder AWS problemi.	30 settembre 2025

Nuove policy gestite	Accedi ad AWS ha rilasciato due nuove politiche gestite. `AmazonManagedSignUpServicePolicy` concede le autorizzazioni necessarie per completare i processi di registrazione AWS dell'account. `ApplicationProvisioningPolicy` concede autorizzazioni complete per le operazioni di fornitura delle applicazioni e di gestione delle identità. Per informazioni, consulta Accedi ad AWS gli aggiornamenti delle politiche gestite. AWS	30 settembre 2025
Argomenti aggiornati per la risoluzione	Sono stati aggiunti nuovi argomenti di risoluzione dei problemi relativi all'accesso a ID Builder AWS e al Console di gestione AWS.	27 febbraio 2024
Sono stati aggiornati diversi argomenti per l'organizzazione	Tipi di utente aggiornati, rimossi Determina il tipo di utente e ne ha incorporato il contenuto nei tipi di utente, Come accedere a AWS	15 maggio 2023
Sono stati aggiornati diversi argomenti e il banner principale	Tipi di utenti aggiornati, Determina il tipo di utente , come accedere AWS, Cos'è AWS Sign-in? . Sono state inoltre aggiornate le procedure di accesso per utenti root e utenti IAM.	3 marzo 2023

Paragrafo introduttivo aggiornato per l' Console di gestione AWS accesso	È stato spostato Determine del tipo di utente nella parte superiore della pagina e ha rimosso la nota esistente in Account root user.	27 febbraio 2023
Aggiunto ID Builder AWS	ID Builder AWS Argomenti aggiunti alla Guida per AWS Sign-In l'utente e contenuti integrati negli argomenti esistenti.	31 gennaio 2023
Aggiornamento organizzativo	In base al feedback dei clienti, il sommario è stato aggiornat o per essere più chiaro sui metodi di accesso. Sono stati aggiornati i tutorial di accesso. Terminologia aggiornata e determinazione del tipo di utente. Collegamento incrociat o migliorato per definire termini come utente IAM e utente root.	22 dicembre 2022
Nuova guida	Questa è la prima versione della Guida per l' AWS Sign-In utente.	31 agosto 2022

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.