Guida per l'utente

AWS IAM Identity Center

AWS IAM Identity Center: Guida per l'utente

Table of Contents

Cos'è IAM Identity Center?

AWS IAM Identity Center è consigliato Servizio AWS per gestire l'accesso degli utenti umani alle AWS risorse. È un unico posto in cui è possibile assegnare agli utenti della forza lavoro un accesso uniforme a più applicazioni Account AWS . workforce identities IAM Identity Center è offerto senza costi aggiuntivi.

Con IAM Identity Center, puoi creare o connettere gli utenti della forza lavoro e gestire centralmente il loro accesso a tutte le loro Account AWS applicazioni. Puoi utilizzare le autorizzazioni per più account per assegnare l'accesso agli utenti della tua forza lavoro. Account AWSÈ possibile utilizzare le assegnazioni delle applicazioni per assegnare agli utenti l'accesso alle applicazioni gestite e gestite dai clienti. AWS

> **Note**
>
> Sebbene il nome del servizio AWS Single Sign-On sia stato ritirato, il termine Single Sign-On viene ancora utilizzato in questa guida per descrivere lo schema di autenticazione che consente agli utenti di accedere una sola volta per accedere a più applicazioni e siti Web.

Funzionalità di IAM Identity Center

IAM Identity Center include le seguenti funzionalità e caratteristiche principali:

Gestisci le identità della forza lavoro

Gli utenti umani che creano o gestiscono carichi di lavoro AWS sono anche noti come utenti della forza lavoro o identità della forza lavoro. Gli utenti della forza lavoro sono dipendenti o collaboratori a cui consenti l'accesso Account AWS nell'organizzazione e nelle applicazioni aziendali interne. Queste persone potrebbero essere sviluppatori che creano sistemi interni e rivolti ai clienti o utenti di sistemi e applicazioni di database interni. Puoi creare utenti e gruppi della forza lavoro in IAM Identity Center oppure connetterti e sincronizzarti con un set esistente di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni, consulta Gestisci la tua fonte di identità.

Gestisci le istanze di IAM Identity Center

IAM Identity Center supporta due tipi di istanze: istanze di organizzazione e istanze di account. Un'istanza organizzativa è la best practice. È l'unica istanza che consente di gestire l'accesso

alle applicazioni Account AWS ed è consigliata per tutti gli usi in produzione. Un'istanza dell'organizzazione viene distribuita nell'account di AWS Organizations gestione e offre un unico punto da cui gestire l'accesso degli utenti in tutto l' AWS ambiente.

Le istanze dell'account sono legate all'account Account AWS in cui sono abilitate. Utilizza le istanze di account di IAM Identity Center solo per supportare implementazioni isolate di applicazioni gestite selezionate. AWS Per ulteriori informazioni, consulta Gestisci le istanze di organizzazione e account di IAM Identity Center.

Gestisci l'accesso a più Account AWS

Con le autorizzazioni per più account, puoi pianificare e implementare centralmente le autorizzazioni su più Account AWS account contemporaneamente senza dover configurare manualmente ciascuno dei tuoi account. Puoi creare autorizzazioni basate su funzioni lavorative comuni o definire autorizzazioni personalizzate che soddisfino le tue esigenze di sicurezza. È quindi possibile assegnare tali autorizzazioni agli utenti della forza lavoro per controllare il loro accesso su account specifici.

Questa funzionalità opzionale è disponibile solo per le istanze dell'organizzazione. Se utilizzi la gestione dei ruoli IAM per account nel tuo ambiente, entrambi i sistemi possono coesistere. Se desideri provare le autorizzazioni per più account, puoi iniziare implementando questo sistema su base limitata e migrare una parte maggiore del tuo ambiente per utilizzare questo sistema nel tempo.

Gestisci l'accesso alle applicazioni

IAM Identity Center consente di semplificare la gestione degli accessi alle applicazioni. Con IAM Identity Center, puoi concedere agli utenti della tua forza lavoro in IAM Identity Center l'accesso single sign-on alle applicazioni.

AWS applicazioni gestite

AWS fornisce applicazioni come Amazon Redshift Amazon Managed Grafana e Amazon Monitron, che si integrano con IAM Identity Center. Queste applicazioni possono utilizzare IAM Identity Center per l'autenticazione, i servizi di directory e la propagazione affidabile delle identità. I tuoi utenti traggono vantaggio da un'esperienza Single Sign-On coerente e, poiché le applicazioni condividono una visione comune di utenti, gruppi e appartenenza ai gruppi, gli utenti hanno anche un'esperienza coerente quando condividono le risorse delle applicazioni con altri. Puoi configurare le applicazioni AWS gestite per funzionare con IAM Identity Center direttamente dalle console delle applicazioni pertinenti o tramite le API.

Applicazioni gestite dal cliente

Puoi concedere agli utenti della tua forza lavoro in IAM Identity Center l'accesso Single Sign-On alle applicazioni che supportano la federazione delle identità con SAML 2.0. Molte applicazioni SAML 2.0 di uso comune, come Salesforce e Microsoft 365, funzionano con IAM Identity Center e sono disponibili nel catalogo delle applicazioni nella console IAM Identity Center. Questa è una funzionalità opzionale che può essere utile se utilizzi tali applicazioni e crei utenti e gruppi in IAM Identity Center oppure utilizzi il servizio di dominio Microsoft Active Directory come fonte di identità.

Propagazione delle identità attendibili tra le applicazioni

La propagazione affidabile delle identità offre un'esperienza Single Sign-On semplificata per gli utenti di strumenti di query e applicazioni di business intelligence (BI) che richiedono l'accesso ai dati nei servizi. AWS La gestione dell'accesso ai dati si basa sull'identità dell'utente, quindi gli amministratori possono concedere l'accesso in base all'appartenenza esistente degli utenti e ai gruppi. L'accesso degli utenti ai AWS servizi e ad altri eventi viene registrato nei registri e negli CloudTrail eventi specifici del servizio, in modo che i revisori sappiano quali azioni hanno intrapreso gli utenti e a quali risorse hanno avuto accesso gli utenti.

AWS accedi all'accesso al portale per i tuoi utenti

Il portale di AWS accesso è un semplice portale web che fornisce agli utenti un accesso senza interruzioni a tutti i loro compiti Account AWS e applicazioni.

Rinomina di IAM Identity Center

Il 26 luglio 2022, AWS Single Sign-On è stato rinominato in. AWS IAM Identity Center Per i clienti esistenti, la tabella seguente ha lo scopo di descrivere alcune delle modifiche ai termini più comuni che sono state aggiornate in questa guida a seguito della ridenominazione.

Termine precedente	Termine attuale
AWS Utente SSO o utente SSO	utente o utente della forza lavoro
AWS Portale utente o portale utenti SSO	AWS portale di accesso
AWS applicazioni integrate con SSO	AWS applicazioni gestite
AWS directory SSO	Directory del Centro identità

Termine precedente	Termine attuale
AWS Archivio SSO o archivio identità AWS SSO	archivio di identità utilizzato da IAM Identity Center

La tabella seguente descrive le modifiche al nome della guida di riferimento per utenti, sviluppatori e API applicabili che hanno avuto luogo anche a seguito di questa ridenominazione.

Guida Legacy	Guida attuale
AWS Guida per l'utente Single Sign-On	Guida per l'utente di IAM Identity Center
AWS Guida per sviluppatori all'implementazione SCIM Single Sign-On	Guida per sviluppatori all'implementazione SCIM di IAM Identity Center
AWS Guida di riferimento all'API Single Sign-On	Riferimento all'API IAM Identity Center
AWS Guida di riferimento all'API Single Sign-On Identity Store	Riferimento all'API di Identity Store
AWS Guida di riferimento all'API OIDC Single Sign-On	Riferimento all'API OIDC di IAM Identity Center
AWS Guida di riferimento all'API del portale Single Sign-On	Riferimento all'API del portale IAM Identity Center

I namespace legacy rimangono gli stessi

I namespace **`sso`** e **`identitystore`** API insieme ai seguenti namespace correlati rimangono invariati per motivi di compatibilità con le versioni precedenti.

- Comandi CLI
  - `aws configure sso`
  - `identitystore`
  - `sso`

  - `sso-admin`
  - `sso-oidc`
- Policy gestite che contengono `AWSSSO` e prefissi `AWSIdentitySync`
- Endpoint di servizio contenenti e `sso identitystore`
- AWS CloudFormationrisorse contenenti `AWS::SSO` prefissi
- Ruolo collegato al servizio contenente `AWSServiceRoleForSSO`
- URL della console contenenti e `sso singlesignon`
- URL di documentazione contenenti `singlesignon`

Abilitazione AWS IAM Identity Center

Completa i seguenti passaggi per accedere AWS Management Console e abilitare un'istanza organizzativa di IAM Identity Center.

1. Effettua una delle seguenti operazioni per accedere a AWS Management Console.
   - Nuovo utente AWS (utente root): accedi come proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.
   - Già in uso AWS (credenziali IAM): accedi utilizzando le tue credenziali IAM con autorizzazioni amministrative.
2. Apri la console IAM Identity Center.
3. In Abilita IAM Identity Center, scegli Abilita con AWS Organizations.
4. Facoltativo: aggiungi i tag che desideri associare a questa istanza dell'organizzazione.
5. Facoltativo Configura l'amministrazione delegata.

> **Note**
>
> Se utilizzi un ambiente con più account, ti consigliamo di configurare l'amministrazione delegata. Con l'amministrazione delegata, puoi limitare il numero di persone che richiedono l'accesso all'account di gestione in. AWS Organizations Per ulteriori informazioni, consulta Amministrazione delegata.

> **Important**
>
> La possibilità di creare istanze di account di IAM Identity Center è abilitata per impostazione predefinita. Le istanze di account di IAM Identity Center includono un sottoinsieme di funzionalità disponibili per un'istanza dell'organizzazione. Puoi controllare se gli utenti possono accedere a questa funzionalità utilizzando una Service Control Policy.

È necessario aggiornare firewall e gateway?

Se si filtra l'accesso a AWS domini o endpoint URL specifici utilizzando una soluzione di filtraggio dei contenuti Web come i firewall di nuova generazione (NGFW) o i 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 al portale di accesso. AWS

- *[Directory ID or alias]*.awsapps.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
- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

Considerazioni sulla possibilità di inserire nella lista domini ed endpoint URL

Comprendi l'impatto dei domini Allowlisting oltre al portale di accesso. AWS

- Per accedere Account AWS alla console IAM Identity Center e alla console IAM Identity Center dal tuo portale di AWS accesso, devi consentire l'elenco di domini aggiuntivi. AWS Management Console Per un elenco di domini, consulta la sezione Risoluzione dei problemi nella Guida AWS Management Console introduttiva. AWS Management Console
- Per accedere alle applicazioni AWS gestite dal portale di AWS accesso, è necessario consentire l'elenco dei rispettivi domini. Per ulteriori informazioni, consulta la documentazione relativa al servizio.
- Queste liste di autorizzazione riguardano AWS i servizi. Se utilizzi software esterno, ad esempio esterno IdPs (ad esempio Okta eMicrosoft Entra ID), dovrai includere i relativi domini nelle tue liste di autorizzazione.

Ora sei pronto per configurare IAM Identity Center. Quando abiliti IAM Identity Center, questo viene automaticamente configurato con una directory Identity Center come fonte di identità predefinita, che

è il modo più veloce per iniziare a utilizzare IAM Identity Center. Per istruzioni, consulta Configura l'accesso degli utenti con la directory IAM Identity Center predefinita.

Se desideri saperne di più su come IAM Identity Center funziona con Organizations, fonti di identità e ruoli IAM, consulta i seguenti argomenti.

Argomenti

Prerequisiti e considerazioni

I seguenti argomenti forniscono informazioni sui prerequisiti e altre considerazioni per la configurazione di IAM Identity Center.

Considerazioni per la scelta di un Regione AWS

Puoi abilitare un'istanza IAM Identity Center in un'unica istanza, Regione AWS supportata a tua scelta. La scelta di una regione richiede una valutazione delle priorità in base ai casi d'uso e alle politiche aziendali. L'accesso alle applicazioni cloud Account AWS e dal tuo IAM Identity Center non dipendono da questa scelta; tuttavia, l'accesso alle applicazioni AWS gestite e la possibilità di utilizzarle AWS Managed Microsoft AD come fonte di identità possono dipendere da questa scelta. Per un elenco delle regioni supportate da AWS IAM Identity Center, consulta Riferimenti generali di AWS gli endpoint e le quote di IAM Identity Center nella pagina.

Considerazioni chiave per la scelta di un. Regione AWS

- Posizione geografica: quando selezioni una regione geograficamente più vicina alla maggior parte dei tuoi utenti finali, questi avranno una latenza di accesso inferiore al portale di accesso e AWS alle applicazioni AWS gestite, come Amazon. SageMaker Studio
- Disponibilità di applicazioni AWS AWS gestite: le applicazioni gestite, come Amazon SageMaker, possono funzionare solo negli ambienti Regioni AWS che supportano. Abilita IAM Identity Center in una regione supportata dalle applicazioni AWS gestite che desideri utilizzare con esso. Molte applicazioni AWS gestite possono inoltre funzionare solo nella stessa regione in cui hai abilitato IAM Identity Center.
- Sovranità digitale: le normative sulla sovranità digitale o le politiche aziendali possono imporre l'uso di un particolare. Regione AWS Rivolgiti all'ufficio legale della tua azienda.

- Origine dell'identità: se utilizzi AWS Managed Microsoft AD o AD Connector come origine dell'identità, la sua regione di origine deve corrispondere Regione AWS a quella in cui hai abilitato IAM Identity Center.
- Regioni disattivate per impostazione predefinita: AWS inizialmente erano abilitate tutte nuove Regioni AWS per l'utilizzo in modalità Account AWS predefinita, il che consentiva automaticamente agli utenti di creare risorse in qualsiasi regione. Ora, quando si AWS aggiunge una nuova regione, il suo utilizzo è disabilitato per impostazione predefinita in tutti gli account. Se distribuisci IAM Identity Center in una regione disabilitata per impostazione predefinita, devi abilitare questa regione in tutti gli account per i quali desideri gestire l'accesso a IAM Identity Center. Questa operazione è necessaria anche se non prevedi di creare risorse in quella regione in quegli account.

  Puoi abilitare una regione per gli account correnti della tua organizzazione e devi ripetere questa azione per i nuovi account che potresti aggiungere in seguito. Per istruzioni, consulta Abilitare o disabilitare una regione nella tua organizzazione nella guida AWS Organizations per l'utente. Per evitare di ripetere questi passaggi aggiuntivi, puoi scegliere di implementare il tuo IAM Identity Center in una regione abilitata per impostazione predefinita. Per riferimento, le seguenti regioni sono abilitate per impostazione predefinita:

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

  - Asia Pacifico (Osaka-Locale)
- Chiamate tra regioni: in alcune regioni, IAM Identity Center può chiamare Amazon Simple Email Service in una regione diversa per inviare e-mail. In queste chiamate interregionali, IAM Identity Center invia determinati attributi utente all'altra regione. Per ulteriori informazioni sulle regioni, consulta AWS IAM Identity Center Disponibilità regionale.

Cambio Regioni AWS

Puoi cambiare la tua regione di IAM Identity Center solo eliminando l'istanza corrente e creando una nuova istanza in un'altra regione. Se hai già abilitato un'applicazione AWS gestita con l'istanza esistente, devi eliminarla prima di eliminare il tuo IAM Identity Center. È necessario ricreare utenti, gruppi, set di autorizzazioni, applicazioni e assegnazioni nella nuova istanza. Puoi utilizzare le API di assegnazione dell'account e delle applicazioni IAM Identity Center per ottenere un'istantanea della configurazione e quindi utilizzarla per ricostruire la configurazione in una nuova regione. Potrebbe inoltre essere necessario ricreare alcune configurazioni di IAM Identity Center tramite la console di gestione della nuova istanza. Per istruzioni sull'eliminazione di IAM Identity Center, consulta. Elimina la configurazione di IAM Identity Center

Quota per i ruoli IAM creati da IAM Identity Center

IAM Identity Center crea ruoli IAM per fornire agli utenti le autorizzazioni per l'accesso alle risorse. Quando si assegna un set di autorizzazioni, IAM Identity Center crea i ruoli IAM corrispondenti controllati da IAM Identity Center in ciascun account e associa le politiche specificate nel set di autorizzazioni a tali ruoli. IAM Identity Center gestisce il ruolo e consente agli utenti autorizzati che hai definito di assumere il ruolo, utilizzando il portale di accesso o. AWS AWS CLI Man mano che modifichi il set di autorizzazioni, IAM Identity Center garantisce che le politiche e i ruoli IAM corrispondenti vengano aggiornati di conseguenza.

Se hai già configurato i ruoli IAM nel tuo Account AWS, ti consigliamo di verificare se il tuo account si sta avvicinando alla quota per i ruoli IAM. La quota predefinita per i ruoli IAM per account è di 1000 ruoli. Per ulteriori informazioni, consulta le quote degli oggetti IAM.

Se ti stai avvicinando alla quota, prendi in considerazione la possibilità di richiedere un aumento della quota. Altrimenti, potresti riscontrare problemi con IAM Identity Center quando fornisci set di autorizzazioni agli account che hanno superato la quota di ruoli IAM. Per informazioni su come richiedere un aumento della quota, vedere Richiedere un aumento della quota nella Service Quotas User Guide.

> **Note**
>
> Se stai esaminando i ruoli IAM in un account che utilizza già IAM Identity Center, potresti notare che i nomi dei ruoli iniziano con. “AWSReservedSSO_” Questi sono i ruoli che il servizio IAM Identity Center ha creato nell'account e derivano dall'assegnazione di un set di autorizzazioni all'account.

IAM Identity Center e AWS Organizations

AWS Organizations è consigliato, ma non obbligatorio, per l'uso con IAM Identity Center. Se non hai creato un'organizzazione, non è necessario. Quando abiliti IAM Identity Center, sceglierai se abilitare il servizio con AWS Organizations. Quando configuri un'organizzazione, chi configura Account AWS l'organizzazione diventa l'account di gestione dell'organizzazione. L'utente root di Account AWS è ora il proprietario dell'account di gestione dell'organizzazione. Tutti gli altri Account AWS che inviti a far parte della tua organizzazione sono account utente. L'account di gestione crea le risorse, le unità organizzative e le politiche dell'organizzazione che gestiscono gli account dei membri. Le autorizzazioni vengono delegate agli account dei membri dall'account di gestione.

> **Note**
>
> Ti consigliamo di abilitare IAM Identity Center con AWS Organizations, che crea un'istanza organizzativa di IAM Identity Center. Un'istanza organizzativa è la nostra best practice consigliata perché supporta tutte le funzionalità di IAM Identity Center e fornisce funzionalità di gestione centralizzate. Per ulteriori informazioni, consulta Gestisci le istanze di organizzazione e account di IAM Identity Center.

Se hai già configurato AWS Organizations e intendi aggiungere IAM Identity Center alla tua organizzazione, assicurati che tutte le AWS Organizations funzionalità siano abilitate. Quando si crea un'organizzazione, l'abilitazione di tutte le caratteristiche è l'impostazione predefinita. Per ulteriori informazioni, consulta la sezione Abilitazione di tutte le caratteristiche nell'organizzazione nella Guida per l'utente di AWS Organizations .

Per abilitare IAM Identity Center, devi accedere al tuo account AWS Management Console di AWS Organizations gestione come utente con credenziali amministrative o come utente root (scelta sconsigliata a meno che non esistano altri utenti amministrativi). Non puoi abilitare IAM

Identity Center dopo aver effettuato l'accesso con credenziali amministrative da un account AWS Organizations membro. Per ulteriori informazioni, consulta Creazione e gestione di un' AWS organizzazione nella Guida per l'AWS Organizations utente.

Conferma le tue fonti di identità in IAM Identity Center

La tua fonte di identità in IAM Identity Center definisce dove vengono gestiti gli utenti e i gruppi. Dopo aver abilitato IAM Identity Center, conferma che stai utilizzando la fonte di identità di tua scelta.

Conferma la tua fonte di identità

1. Apri la console IAM Identity Center.
2. Nella pagina Dashboard, sotto la sezione Passaggi di configurazione consigliati, scegli Conferma l'origine dell'identità. Puoi accedere a questa pagina anche scegliendo Impostazioni e selezionando la scheda Origine dell'identità.
3. Se desideri mantenere la fonte di identità assegnata, non è necessaria alcuna azione. Se preferisci modificarla, scegli Azioni, quindi scegli Cambia fonte di identità.

   Puoi scegliere una delle seguenti opzioni come fonte di identità:

   Directory del Centro identità

   Quando abiliti IAM Identity Center per la prima volta, viene automaticamente configurato con una directory Identity Center come fonte di identità predefinita. Se non utilizzi già un altro provider di identità esterno, puoi iniziare a creare utenti e gruppi e assegnare il loro livello di accesso alle tue Account AWS applicazioni. Per un tutorial sull'utilizzo di questa fonte di identità, consultaConfigura l'accesso degli utenti con la directory IAM Identity Center predefinita.

   Active Directory

   Se gestisci già utenti e gruppi nella tua AWS Managed Microsoft AD directory utilizzando AWS Directory Service o utilizzando la directory gestita in modo autonomoActive Directory (AD), ti consigliamo di connettere quella directory quando abiliti IAM Identity Center. Non creare utenti e gruppi nella directory predefinita di Identity Center. IAM Identity Center utilizza la connessione fornita da AWS Directory Service per sincronizzare le informazioni su utenti, gruppi e appartenenze dalla directory di origine in Active Directory all'archivio di identità IAM Identity Center. Per ulteriori informazioni, consulta Connect a una Microsoft AD directory.

> **Note**
>
> IAM Identity Center non supporta Simple AD basato su Samba4 come fonte di identità.

Provider di identità esterno

Per i provider di identità esterni (IdPs) come Okta orMicrosoft Entra ID, puoi utilizzare IAM Identity Center per autenticare le identità dallo standard Security Assertion Markup Language (SAML) 2.0. IdPs Il protocollo SAML non fornisce un modo per interrogare l'IdP per conoscere utenti e gruppi. Fai conoscere a IAM Identity Center tali utenti e gruppi inserendoli in IAM Identity Center. Puoi eseguire il provisioning automatico (sincronizzazione) delle informazioni su utenti e gruppi dal tuo IdP a IAM Identity Center utilizzando il protocollo System for Cross-domain Identity Management (SCIM) v2.0 se il tuo IdP supporta SCIM. Altrimenti, puoi effettuare manualmente il provisioning di utenti e gruppi inserendo manualmente i nomi utente, l'indirizzo e-mail e i gruppi in IAM Identity Center.

Per istruzioni dettagliate sulla configurazione della fonte di identità, consultaTutorial introduttivi.

> **Note**
>
> Se prevedi di utilizzare un provider di identità esterno, tieni presente che l'IdP esterno, non IAM Identity Center, gestisce le impostazioni di autenticazione a più fattori (MFA). L'MFA in IAM Identity Center non è supportata per l'uso da parte di utenti esterni. IdPs Per ulteriori informazioni, consulta Richiedi agli utenti l'MFA.

La fonte di identità scelta determina dove IAM Identity Center cerca utenti e gruppi che richiedono l'accesso Single Sign-On. Dopo aver confermato o modificato la fonte dell'identità, dovrai creare o specificare un utente e assegnargli le autorizzazioni amministrative al tuo. Account AWS

> **Important**
>
> Se gestisci già utenti e gruppi in Active Directory o presso un provider di identità esterno (IdP), ti consigliamo di prendere in considerazione la possibilità di collegare questa fonte di identità quando abiliti IAM Identity Center e scegli la tua fonte di identità. Questa operazione deve essere eseguita prima di creare utenti e gruppi nella directory predefinita di Identity Center e di effettuare qualsiasi assegnazione.
> Se gestisci già utenti e gruppi in un'unica fonte di identità in IAM Identity Center, il passaggio a una fonte di identità diversa potrebbe rimuovere tutte le assegnazioni di utenti e gruppi che hai configurato in IAM Identity Center. In tal caso, tutti gli utenti, incluso l'utente amministrativo di IAM Identity Center, perderanno l'accesso Single Sign-On alle proprie Account AWS applicazioni. Per ulteriori informazioni, consulta Considerazioni sulla modifica dell'origine dell'identità.

Dopo aver configurato la fonte di identità, puoi cercare utenti o gruppi per concedere loro l'accesso Single Sign-On alle Account AWS applicazioni cloud o a entrambi.

Tutorial introduttivi

Puoi avere una fonte di identità per organizzazione, quindi è importante dedicare del tempo a testare le funzionalità di ciascuna di esse.

In questa sezione, puoi scegliere uno dei seguenti tutorial per configurare IAM Identity Center con la tua fonte di identità preferita, creare un utente amministrativo e configurare i set di autorizzazioni per consentire agli utenti di accedere alle risorse.

Prima di iniziare uno di questi tutorial, abilita IAM Identity Center. Per ulteriori informazioni, consulta Abilitazione AWS IAM Identity Center.

Argomenti

- Configura l'accesso degli utenti con la directory IAM Identity Center predefinita
- Utilizzo di Active Directory come origine di identità
- Setting up SCIM provisioning between CyberArk and IAM Identity Center
- Configura SAML e SCIM con Google Workspace IAM Identity Center
- Utilizzo di IAM Identity Center per connettersi alla tua piattaforma di JumpCloud directory
- Configura SAML e SCIM con Microsoft Entra ID IAM Identity Center
- Configura SAML e SCIM con Okta IAM Identity Center
- Configurazione del provisioning SCIM tra OneLogin e IAM Identity Center
- Utilizzo di Ping Identity prodotti con IAM Identity Center

Configura l'accesso degli utenti con la directory IAM Identity Center predefinita

Quando abiliti IAM Identity Center per la prima volta, viene automaticamente configurato con una directory Identity Center come fonte di identità predefinita, quindi non devi scegliere una fonte di identità. Se la tua organizzazione utilizza un altro provider di identità come AWS Directory Service for Microsoft Active DirectoryMicrosoft Entra ID, o Okta considera l'integrazione di tale fonte di identità con IAM Identity Center invece di utilizzare la configurazione predefinita.

Obiettivo

In questo tutorial, utilizzerai la directory predefinita come fonte di identità e configurerai e testerai l'accesso degli utenti. In questo scenario, gestisci tutti gli utenti e i gruppi in IAM Identity Center. Gli utenti accedono tramite il portale di AWS accesso. Questo tutorial è destinato agli utenti che sono nuovi AWS o che utilizzano IAM per gestire utenti e gruppi. Nei passaggi successivi, creerai quanto segue:

- Un utente amministrativo di nome *`Nikki Wolf`*
- Un gruppo chiamato *`Admin team`*
- Un set di autorizzazioni denominato *`AdminAccess`*

Per verificare che tutto sia stato creato correttamente, accederai e imposterai la password dell'utente amministrativo. Dopo aver completato questo tutorial, puoi utilizzare l'utente amministrativo per aggiungere altri utenti in IAM Identity Center, creare set di autorizzazioni aggiuntivi e configurare l'accesso organizzativo alle applicazioni.

Se non hai ancora abilitato IAM Identity Center, consultaAbilitazione AWS IAM Identity Center.

Prima di iniziare:

Effettua una delle seguenti operazioni per accedere a AWS Management Console.

- Nuovo utente AWS (utente root): accedi come proprietario dell'account scegliendo utente Account AWS root e inserendo il tuo indirizzo Account AWS e-mail. Nella pagina successiva, inserisci la password.
- Già in uso AWS (credenziali IAM): accedi utilizzando le tue credenziali IAM con autorizzazioni amministrative.

Apri la console IAM Identity Center.

Passaggio 1: aggiungi un utente

1. Nel riquadro di navigazione di IAM Identity Center, scegli Utenti, quindi seleziona Aggiungi utente.
2. Nella pagina Specificare i dettagli dell'utente, completa le seguenti informazioni:
   - Nome utente: per questo tutorial, inserisci *`nikkiw`*.

Quando crei utenti, scegli nomi utente facili da ricordare. I tuoi utenti devono ricordare il nome utente per accedere al portale di AWS accesso e non puoi modificarlo in un secondo momento.

- Password: scegli Invia un'e-mail a questo utente con le istruzioni per l'impostazione della password (scelta consigliata).

  Questa opzione invia all'utente un'e-mail indirizzata da Amazon Web Services, con l'oggetto Invito a partecipare a IAM Identity Center (successore di AWS Single Sign-On). L'e-mail proviene da o. `no-reply@signin.aws` `no-reply@login.awsapps.com` Aggiungi questi indirizzi e-mail all'elenco dei mittenti approvati.

- Indirizzo e-mail: inserisci un indirizzo e-mail per l'utente a cui puoi ricevere l'e-mail. Quindi, inseriscilo di nuovo per confermarlo. Ogni utente deve avere un indirizzo email univoco.
- Nome: inserisci il nome dell'utente. Per questo tutorial, inserisci *`Nikki`*.
- Cognome: inserisci il cognome dell'utente. Per questo tutorial, inserisci *`Wolf`*.
- Nome visualizzato: il valore predefinito è il nome e il cognome dell'utente. Se desideri modificare il nome visualizzato, puoi inserire qualcosa di diverso. Il nome visualizzato è visibile nel portale di accesso e nell'elenco degli utenti.
- Se lo desideri, completa le informazioni opzionali. Non viene utilizzato durante questo tutorial e puoi modificarlo in seguito.

3. Seleziona Successivo. Viene visualizzata la pagina Aggiungi utente ai gruppi. *`Creeremo un gruppo a cui assegnare le autorizzazioni amministrative invece di darle direttamente a Nikki.`*

   Scegli Crea gruppo

   Si apre una nuova scheda del browser per visualizzare la pagina Crea gruppo.

   a. In Dettagli del gruppo, in Nome del gruppo inserisci un nome per il gruppo. Consigliamo un nome di gruppo che identifichi il ruolo del gruppo. Per questo tutorial, inserisci il *`team di amministrazione`*.

   b. Scegli Crea gruppo

   c. Chiudi la scheda del browser Gruppi per tornare alla scheda Aggiungi browser utente

4. Nell'area Gruppi, seleziona il pulsante Aggiorna. Il gruppo del *`team di amministratori`* viene visualizzato nell'elenco.

Seleziona la casella di controllo accanto a *Team di amministrazione*, quindi scegli Avanti.

5. Nella pagina Rivedi e aggiungi utente, conferma quanto segue:

   - Le informazioni principali vengono visualizzate come previsto
   - Gruppi mostra l'utente aggiunto al gruppo che hai creato

   Se vuoi apportare modifiche, seleziona Edit (Precedente). Quando tutti i dettagli sono corretti, scegli Aggiungi utente.

   Un messaggio di notifica ti informa che l'utente è stato aggiunto.

Successivamente, aggiungerai le autorizzazioni amministrative per il gruppo del *team di amministrazione* in modo che *Nikki* abbia accesso alle risorse.

Passaggio 2: Aggiungere le autorizzazioni amministrative

1. Nel riquadro di navigazione di IAM Identity Center, in Autorizzazioni multiaccount, scegli. Account AWS
2. Nella Account AWSpagina, la struttura organizzativa mostra la tua organizzazione con i tuoi account sottostanti nella gerarchia. Seleziona la casella di controllo per il tuo account di gestione, quindi seleziona Assegna utenti o gruppi.
3. Viene visualizzato il flusso di lavoro Assegna utenti e gruppi. Consiste in tre fasi:

   a. Per il passaggio 1: Seleziona utenti e gruppi, scegli il gruppo di *team di amministrazione* che hai creato. Quindi scegli Successivo.

   b. Per il Passaggio 2: Seleziona i set di autorizzazioni, scegli Crea set di autorizzazioni per aprire una nuova scheda che illustra i tre passaggi secondari necessari per creare un set di autorizzazioni.

      i. Per la Fase 1: Seleziona il tipo di set di autorizzazioni, completa quanto segue:

         - In Tipo di set di autorizzazioni, scegli Set di autorizzazioni predefinito.
         - In Politica per il set di autorizzazioni predefinito, scegli. AdministratorAccess

         Seleziona Successivo.

ii. Per la Fase 2: Specificate i dettagli del set di autorizzazioni, mantenete le impostazioni predefinite e scegliete Avanti.

Le impostazioni predefinite creano un set di autorizzazioni denominato *AdministratorAccess*con la durata della sessione impostata su un'ora. È possibile modificare il nome del set di autorizzazioni inserendo un nuovo nome nel campo Nome del set di autorizzazioni.

iii. Per il passaggio 3: revisione e creazione, verifica che il tipo di set di autorizzazioni utilizzi la politica AWS gestita AdministratorAccess. Scegli Crea. Nella pagina Set di autorizzazioni viene visualizzata una notifica che informa che il set di autorizzazioni è stato creato. Ora puoi chiudere questa scheda nel tuo browser web.

Nella scheda Assegna utenti e gruppi del browser, sei ancora al Passaggio 2: Seleziona i set di autorizzazioni da cui hai avviato il flusso di lavoro per la creazione del set di autorizzazioni.

Nell'area Set di autorizzazioni, scegli il pulsante Aggiorna. Il set di *AdministratorAccess*autorizzazioni creato viene visualizzato nell'elenco. Seleziona la casella di controllo relativa al set di autorizzazioni, quindi scegli Avanti.

c. Nella pagina Passaggio 3: Rivedi e invia le assegnazioni, conferma che il gruppo del *team di amministrazione* sia selezionato e che il set di *AdministratorAccess*autorizzazioni sia selezionato, quindi scegli Invia.

La pagina viene aggiornata con un messaggio che indica che la tua Account AWS è in fase di configurazione. Attendi il completamento del processo.

Verrai reindirizzato alla Account AWS pagina. Un messaggio di notifica ti informa che il tuo Account AWS è stato riassegnato e che il set di autorizzazioni aggiornato è stato applicato.

> **Complimenti!**
>
> Hai configurato correttamente il primo utente, gruppo e set di autorizzazioni.

Nella parte successiva di questo tutorial testerai l'accesso di *Nikki accedendo al portale di* accesso con le AWS loro credenziali amministrative e impostando la loro password. Esci subito dalla console.

Fase 3: test dell'accesso utente

Ora che *Nikki Wolf* è un utente della tua organizzazione, può accedere e accedere alle risorse per le quali ha ottenuto l'autorizzazione in base al set di autorizzazioni. Per verificare che l'utente sia configurato correttamente, nel passaggio successivo utilizzerai le credenziali *di Nikki* per accedere e impostare la password. Quando hai aggiunto l'utente *Nikki Wolf* nel passaggio 1, hai scelto di far ricevere a *Nikki* un'e-mail con le istruzioni per l'impostazione della password. È ora di aprire quell'e-mail e fare quanto segue:

1. Nell'e-mail, seleziona il link Accetta l'invito per accettare l'invito.

   > **Note**
   >
   > L'e-mail include anche il nome utente *di Nikki* e l'URL del portale di AWS accesso che utilizzeranno per accedere all'organizzazione. Registra queste informazioni per utilizzi futuri.

   Verrai indirizzato alla pagina di registrazione di un nuovo utente dove puoi impostare la password *di Nikki*.

2. Dopo aver impostato la password *di Nikki*, si passa alla pagina di accesso. Inserisci ***nikkiw*** e scegli Avanti, quindi inserisci la password di ***Nikki*** e scegli Accedi.
3. Si apre il portale di AWS accesso che mostra l'organizzazione e le applicazioni a cui puoi accedere.

   Seleziona l'organizzazione per espanderla in un elenco Account AWS , quindi seleziona l'account per visualizzare i ruoli che puoi utilizzare per accedere alle risorse dell'account.

   Ogni set di autorizzazioni dispone di due metodi di gestione che è possibile utilizzare, ruoli o chiavi di accesso.

   - Ruolo, ad esempio *AdministratorAccess*: apre il AWS Console Home.
   - Chiavi di accesso: forniscono credenziali che è possibile utilizzare con AWS CLI or e AWS SDK. Include le informazioni per l'utilizzo di credenziali a breve termine che si aggiornano automaticamente o chiavi di accesso a breve termine. Per ulteriori informazioni, consulta Ottenere le credenziali utente di IAM Identity Center per gli SDK AWS CLI or AWS.
4. Scegli il link Ruolo per accedere a. AWS Console Home

Hai effettuato l'accesso e sei passato alla AWS Console Home pagina. Esplora la console e conferma di avere l'accesso previsto.

Passaggi successivi

Ora che hai creato un utente amministrativo in IAM Identity Center, puoi:

- Assegna applicazioni
- Aggiungi altri utenti
- Assegna utenti agli account
- Configura set di autorizzazioni aggiuntivi

> **Note**
>
> È possibile assegnare più set di autorizzazioni allo stesso utente. Per seguire la procedura ottimale di applicazione delle autorizzazioni con privilegi minimi, dopo aver creato l'utente amministrativo, create un set di autorizzazioni più restrittivo e assegnatelo allo stesso utente. In questo modo, puoi accedere solo Account AWS con le autorizzazioni necessarie, anziché con le autorizzazioni amministrative.

Dopo che gli utenti hanno accettato l'invito ad attivare il proprio account e hanno effettuato l' AWS accesso al portale di accesso, gli unici elementi che appaiono nel portale riguardano Account AWS i ruoli e le applicazioni a cui sono assegnati.

> **Important**
>
> Ti consigliamo vivamente di abilitare l'autenticazione a più fattori (MFA) per i tuoi utenti. Per ulteriori informazioni, consulta Autenticazione a più fattori per gli utenti di Identity Center.

Utilizzo di Active Directory come origine di identità

Se gestisci gli utenti nella tua AWS Managed Microsoft AD directory utilizzando AWS Directory Service o la directory gestita autonomamente in Active Directory (AD), puoi modificare la fonte di identità di IAM Identity Center per lavorare con tali utenti. Ti consigliamo di prendere in considerazione la possibilità di collegare questa fonte di identità quando abiliti IAM Identity Center

e scegli la tua fonte di identità. Questa operazione prima di creare utenti e gruppi nella directory predefinita di Identity Center ti aiuterà a evitare la configurazione aggiuntiva richiesta se modifichi la fonte di identità in un secondo momento.

Per utilizzare Active Directory come origine dell'identità, la configurazione deve soddisfare i seguenti prerequisiti:

- Se lo utilizziAWS Managed Microsoft AD, devi abilitare IAM Identity Center nello stesso Regione AWS luogo in cui è configurata la tua AWS Managed Microsoft AD directory. IAM Identity Center archivia i dati di assegnazione nella stessa regione della directory. Per amministrare IAM Identity Center, potrebbe essere necessario passare alla regione in cui è configurato IAM Identity Center. Inoltre, tieni presente che il portale di AWS accesso utilizza lo stesso URL di accesso della tua directory.
- Usa un Active Directory che risiede nell'account di gestione:

  Devi avere un AD Connector o una AWS Managed Microsoft AD directory esistente configurata in AWS Directory Service e deve risiedere nel tuo account di AWS Organizations gestione. È possibile connettere solo una directory AD Connector o una directory AWS Managed Microsoft AD alla volta. Se devi supportare più domini o foreste, usaAWS Managed Microsoft AD. Per ulteriori informazioni, consultare:

  - Connect una directory AWS Managed Microsoft AD a IAM Identity Center
  - Connect una directory autogestita in Active Directory a IAM Identity Center
- Utilizza un Active Directory che risiede nell'account amministratore delegato:

  Se prevedi di abilitare un amministratore delegato di IAM Identity Center e utilizzare Active Directory come fonte di identità IAM Identity Center, puoi utilizzare un AD Connector o una AWS Managed Microsoft AD directory esistente configurata in AWS Directory che risiede nell'account amministratore delegato.

  Se decidi di modificare l'origine dell'identità di IAM Identity Center da qualsiasi altra fonte ad Active Directory o di cambiarla da Active Directory a qualsiasi altra fonte, la directory deve risiedere (essere di proprietà di) l'account membro amministratore delegato di IAM Identity Center, se esistente; in caso contrario, deve essere nell'account di gestione.

Questo tutorial ti guida attraverso la configurazione di base per l'utilizzo di Active Directory come fonte di identità IAM Identity Center.

Passaggio 1: Connect Active Directory e specifica un utente

Se utilizzi già Active Directory, i seguenti argomenti ti aiuteranno a prepararti a connettere la tua directory a IAM Identity Center.

> **Note**
>
> Come best practice di sicurezza, ti consigliamo vivamente di abilitare l'autenticazione a più fattori. Se prevedi di connettere una AWS Managed Microsoft AD directory o una directory autogestita in Active Directory e non utilizzi RADIUS MFA AWS Directory Service con, abilita l'MFA in IAM Identity Center.

AWS Managed Microsoft AD

1. Consulta le linee guida contenute in. Connect a una Microsoft AD directory
2. Seguire la procedura riportata in Connect una directory AWS Managed Microsoft AD a IAM Identity Center.
3. Configura Active Directory per sincronizzare l'utente a cui desideri concedere le autorizzazioni amministrative in IAM Identity Center. Per ulteriori informazioni, consulta Sincronizza un utente amministrativo in IAM Identity Center.

Directory gestita automaticamente in Active Directory

1. Consulta le linee guida contenute inConnect a una Microsoft AD directory.
2. Seguire la procedura riportata in Connect una directory autogestita in Active Directory a IAM Identity Center.
3. Configura Active Directory per sincronizzare l'utente a cui desideri concedere le autorizzazioni amministrative in IAM Identity Center. Per ulteriori informazioni, consulta Sincronizza un utente amministrativo in IAM Identity Center.

Fase 2: sincronizzazione di un utente amministrativo in IAM Identity Center

Dopo aver collegato la tua directory a IAM Identity Center, puoi specificare un utente a cui vuoi concedere le autorizzazioni amministrative e quindi sincronizzare quell'utente dalla tua directory in IAM Identity Center.

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, scegli Azioni, quindi scegli Gestisci sincronizzazione.
4. Nella pagina Gestisci sincronizzazione, scegli la scheda Utenti, quindi scegli Aggiungi utenti e gruppi.
5. Nella scheda Utenti, in Utente, inserisci il nome utente esatto e scegli Aggiungi.
6. In Utenti e gruppi aggiunti, procedi come segue:
    a. Conferma che l'utente a cui desideri concedere le autorizzazioni amministrative sia specificato.
    b. Seleziona la casella di controllo a sinistra del nome utente.
    c. Seleziona Invia.
7. Nella pagina Gestisci sincronizzazione, l'utente specificato viene visualizzato nell'elenco degli ambiti Utenti sincronizzati.
8. Nel pannello di navigazione, seleziona Utenti.
9. Nella pagina Utenti, potrebbe essere necessario del tempo prima che l'utente specificato compaia nell'elenco. Scegli l'icona di aggiornamento per aggiornare l'elenco degli utenti.

A questo punto, l'utente non ha accesso all'account di gestione. Configurerai l'accesso amministrativo a questo account creando un set di autorizzazioni amministrative e assegnando l'utente a tale set di autorizzazioni. Per ulteriori informazioni, consulta Crea un set di autorizzazioni..

Setting up SCIM provisioning between CyberArk and IAM Identity Center

IAM Identity Center supporta il provisioning automatico (sincronizzazione) delle informazioni utente da CyberArk Directory Platform IAM Identity Center. Questo provisioning utilizza il protocollo System for Cross-domain Identity Management (SCIM) v2.0. Questa connessione viene configurata CyberArk utilizzando l'endpoint e il token di accesso IAM Identity Center SCIM. Quando configuri la sincronizzazione SCIM, crei una mappatura degli attributi utente agli attributi denominati in CyberArk IAM Identity Center. Ciò fa sì che gli attributi previsti corrispondano tra IAM Identity Center e. CyberArk

Questa guida è basata su CyberArk agosto 2021. I passaggi per le versioni più recenti possono variare. Questa guida contiene alcune note sulla configurazione dell'autenticazione utente tramite SAML.

> **Note**
>
> Prima di iniziare a distribuire SCIM, ti consigliamo di esaminare prima il. Considerazioni sull'utilizzo del provisioning automatico Quindi continua a esaminare le considerazioni aggiuntive nella sezione successiva.

Argomenti

Prerequisiti

Prima di iniziare, avrai bisogno di quanto segue:

- CyberArkabbonamento o prova gratuita. Per iscriverti a una prova gratuita, visita CyberArk.
- Un account abilitato per IAM Identity Center (gratuito). Per ulteriori informazioni, consulta Enable IAM Identity Center.
- Una connessione SAML dal tuo CyberArk account a IAM Identity Center, come descritto nella CyberArkdocumentazione per IAM Identity Center.
- Associa il connettore IAM Identity Center ai ruoli, agli utenti e alle organizzazioni a cui desideri consentire l'accesso Account AWS.

Considerazioni SCIM

Di seguito sono riportate le considerazioni relative all'utilizzo CyberArk della federazione per IAM Identity Center:

- Solo i ruoli mappati nella sezione Provisioning dell'applicazione verranno sincronizzati con IAM Identity Center.
- Lo script di provisioning è supportato solo nel suo stato predefinito, una volta modificato il provisioning SCIM potrebbe fallire.
  - È possibile sincronizzare un solo attributo del numero di telefono e l'impostazione predefinita è «telefono di lavoro».
- Se la mappatura dei ruoli nell'applicazione CyberArk IAM Identity Center viene modificata, è previsto il seguente comportamento:
  - Se i nomi dei ruoli vengono modificati, nessuna modifica ai nomi dei gruppi in IAM Identity Center.
  - Se i nomi dei gruppi vengono modificati, verranno creati nuovi gruppi in IAM Identity Center, i vecchi gruppi rimarranno ma non avranno membri.
- La sincronizzazione degli utenti e il comportamento di de-provisioning possono essere configurati dall'applicazione CyberArk IAM Identity Center, assicurati di impostare il comportamento giusto per la tua organizzazione. Queste sono le opzioni a tua disposizione:
  - Sovrascrivi (o meno) gli utenti nella directory di Identity Center con lo stesso nome principale.
  - Rimuovi il provisioning degli utenti da IAM Identity Center quando l'utente viene rimosso dal CyberArk ruolo.
  - Annullare il provisioning del comportamento dell'utente: disabilitazione o eliminazione.

Fase 1: abilitare il provisioning in IAM Identity Center

In questo primo passaggio, utilizzi la console IAM Identity Center per abilitare il provisioning automatico.

Per abilitare il provisioning automatico in IAM Identity Center

1. Dopo aver completato i prerequisiti, apri la console IAM Identity Center.
2. Scegli Impostazioni nel riquadro di navigazione a sinistra.

3. Nella pagina Impostazioni, individua la casella Informazioni sulla fornitura automatica, quindi scegli Abilita. Ciò abilita immediatamente il provisioning automatico in IAM Identity Center e visualizza le informazioni necessarie sull'endpoint SCIM e sul token di accesso.
4. Nella finestra di dialogo di provisioning automatico in entrata, copia ciascuno dei valori per le seguenti opzioni. Dovrai incollarli in un secondo momento quando configuri il provisioning nel tuo IdP.

   a. Endpoint SCIM

   b. Token di accesso
5. Scegli Chiudi.

Ora che hai configurato il provisioning nella console IAM Identity Center, devi completare le attività rimanenti utilizzando l'applicazione CyberArk IAM Identity Center. Questi passaggi sono descritti nella procedura seguente.

Fase 2: Configurare il provisioning in CyberArk

Utilizza la seguente procedura nell'applicazione CyberArk IAM Identity Center per abilitare il provisioning con IAM Identity Center. Questa procedura presuppone che tu abbia già aggiunto l'applicazione CyberArk IAM Identity Center alla tua console di CyberArk amministrazione in Web Apps. Se non l'hai ancora fatto, consulta e completa questa procedura per configurare il provisioning SCIM. Prerequisiti

Per configurare il provisioning in CyberArk

1. Apri l'applicazione CyberArk IAM Identity Center che hai aggiunto come parte della configurazione di SAML per CyberArk (App > Web App). Per informazioni, consulta Prerequisiti.
2. Scegli l'applicazione IAM Identity Center e vai alla sezione Provisioning.
3. Seleziona la casella Abilita il provisioning per questa applicazione e scegli la modalità Live.
4. Nella procedura precedente, hai copiato il valore dell'endpoint SCIM da IAM Identity Center. Incolla quel valore nel campo SCIM Service URL, nell'applicazione CyberArk IAM Identity Center imposta il Tipo di autorizzazione su Authorization Header. Assicurati di rimuovere la barra finale alla fine dell'URL.
5. Imposta il tipo di intestazione su Bearer Token.
6. Dalla procedura precedente hai copiato il valore del token di accesso in IAM Identity Center. Incolla quel valore nel campo Bearer Token dell'applicazione CyberArk IAM Identity Center.

7. Fai clic su Verifica per testare e applicare la configurazione.
8. In Opzioni di sincronizzazione, scegliete il comportamento giusto per il quale desiderate che il provisioning in uscita funzioniCyberArk. Puoi scegliere di sovrascrivere (o meno) gli utenti esistenti di IAM Identity Center con un nome principale simile e il comportamento di de-provisioning.
9. In Role Mapping, configura la mappatura dai CyberArk ruoli, nel campo Nome, al gruppo IAM Identity Center, nel gruppo di destinazione.
10. Una volta terminato, fai clic su Salva in basso.
11. Per verificare che gli utenti siano stati sincronizzati correttamente con IAM Identity Center, torna alla console IAM Identity Center e scegli Utenti. Gli utenti sincronizzati da CyberArk verranno visualizzati nella pagina Utenti. Questi utenti possono ora essere assegnati agli account e possono connettersi all'interno di IAM Identity Center.

(Facoltativo) Fase 3: Configurazione degli attributi utente in ABAC (CyberArkfor access control) in IAM Identity Center

Questa è una procedura facoltativa da CyberArk utilizzare se scegli di configurare gli attributi per IAM Identity Center per gestire l'accesso alle tue AWS risorse. Gli attributi che definisci CyberArk vengono passati in un'asserzione SAML a IAM Identity Center. Quindi crei un set di autorizzazioni in IAM Identity Center per gestire l'accesso in base agli attributi da cui sei passato. CyberArk

Prima di iniziare questa procedura, è necessario abilitare la Attributi per il controllo degli accessi funzionalità. Per ulteriori informazioni su come effettuare tale operazione, consulta Abilita e configura gli attributi per il controllo degli accessi.

Per configurare gli attributi utente CyberArk per il controllo degli accessi in IAM Identity Center

1. Apri l'applicazione CyberArk IAM Identity Center che hai installato come parte della configurazione di SAML per CyberArk (App > App Web).
2. Vai all'opzione SAML Response.
3. In Attributi, aggiungi gli attributi pertinenti alla tabella seguendo la logica seguente:
    a. Il nome dell'attributo è il nome dell'attributo originale diCyberArk.
    b. Il valore dell'attributo è il nome dell'attributo inviato nell'asserzione SAML a IAM Identity Center.
4. Selezionare Salva.

(Facoltativo) Passaggio di attributi per il controllo degli accessi

Facoltativamente, puoi utilizzare la Attributi per il controllo degli accessi funzionalità di IAM Identity Center per passare un `Attribute` elemento con l'`Name`attributo `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` impostato su. Questo elemento consente di passare attributi come tag di sessione nell'asserzione SAML. Per ulteriori informazioni sui tag di sessione, consulta Passing session tag AWS STSin the IAM User Guide.

Per passare gli attributi come tag di sessione, includi l'elemento `AttributeValue` che specifica il valore del tag. Ad esempio, per passare la coppia chiave-valore del tag`CostCenter = blue`, usa il seguente attributo.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Se devi aggiungere più attributi, includi un `Attribute` elemento separato per ogni tag.

Configura SAML e SCIM con Google Workspace IAM Identity Center

Se la tua organizzazione lo utilizza, Google Workspace puoi integrare utenti e gruppi da Google Workspace IAM Identity Center per consentire loro di accedere alle AWS risorse. È possibile ottenere questa integrazione modificando la fonte di identità IAM Identity Center dalla fonte di identità IAM Identity Center predefinita aGoogle Workspace.

Le informazioni utente di Google Workspace vengono sincronizzate in IAM Identity Center utilizzando il protocollo System for Cross-domain Identity Management (SCIM) v2.0. Questa connessione viene configurata Google Workspace utilizzando l'endpoint SCIM per IAM Identity Center e un token bearer IAM Identity Center. Quando configuri la sincronizzazione SCIM, crei una mappatura degli attributi utente agli attributi denominati in IAM Google Workspace Identity Center. Questa mappatura corrisponde agli attributi utente previsti tra IAM Identity Center e. Google Workspace Per fare ciò, devi configurarti Google Workspace come provider di identità IAM e provider di identità IAM Identity Center.

Obiettivo

I passaggi di questo tutorial ti aiutano a stabilire la connessione SAML tra Google Workspace e AWS. Successivamente, sincronizzerai gli utenti dall'Google Workspaceutilizzo di SCIM. Per verificare che tutto sia configurato correttamente, dopo aver completato i passaggi di configurazione, accederai come Google Workspace utente e verificherai l'accesso alle risorse. AWS Nota che questo tutorial si basa su un piccolo ambiente di test di Google Workspace directory. Le strutture di directory come i gruppi e le unità organizzative non sono incluse. Dopo aver completato questo tutorial, i tuoi utenti potranno accedere al portale di accesso con Google Workspace le tue credenziali. AWS

> **Note**
>
> Per iscriverti a una prova gratuita, Google Workspace visita il Google Workspacesito Google's web.
> Se non hai ancora abilitato IAM Identity Center, consultaAbilitazione AWS IAM Identity Center.

Considerazioni

- Prima di configurare il provisioning SCIM tra Google Workspace e IAM Identity Center, ti consigliamo di effettuare una prima revisione. Considerazioni sull'utilizzo del provisioning automatico
- La sincronizzazione automatica di SCIM Google Workspace è attualmente limitata al provisioning degli utenti. Il provisioning automatico di gruppo non è supportato in questo momento. I gruppi possono essere creati manualmente con il comando create-group di AWS CLI Identity Store o l'API AWS Identity and Access Management (IAM). CreateGroup In alternativa, puoi utilizzare ssosync per sincronizzare Google Workspace utenti e gruppi in IAM Identity Center.
- Ogni Google Workspace utente deve avere un valore specificato per nome, cognome, nome utente e nome visualizzato.
- Ogni Google Workspace utente ha un solo valore per attributo di dati, ad esempio indirizzo e-mail o numero di telefono. Tutti gli utenti con più valori non riusciranno a sincronizzarsi. Se alcuni utenti hanno più valori nei propri attributi, rimuovi gli attributi duplicati prima di tentare di eseguire il provisioning dell'utente in IAM Identity Center. Ad esempio, è possibile sincronizzare solo un attributo del numero di telefono, poiché l'attributo del numero di telefono predefinito è «telefono aziendale», utilizza l'attributo «telefono aziendale» per memorizzare il numero di telefono dell'utente, anche se il numero di telefono dell'utente è un telefono di casa o un telefono cellulare.

- Gli attributi sono ancora sincronizzati se l'utente è disabilitato in IAM Identity Center, ma è ancora attivo in. Google Workspace
- Se esiste un utente esistente nella directory di Identity Center con lo stesso nome utente e lo stesso indirizzo e-mail, l'utente verrà sovrascritto e sincronizzato utilizzando SCIM from. Google Workspace
- Quando si modifica l'origine dell'identità, sono necessarie ulteriori considerazioni. Per ulteriori informazioni, consulta the section called “Passaggio da IAM Identity Center a un IdP esterno”.

Passaggio 1Google Workspace: configurare l'applicazione SAML

1. Accedi alla tua console di Google amministrazione utilizzando un account con privilegi di super amministratore.
2. Nel pannello di navigazione a sinistra della console di Google amministrazione, scegli App, quindi scegli App Web e per dispositivi mobili.
3. Nell'elenco a discesa Aggiungi app, seleziona Cerca app.
4. Nella casella di ricerca inserisci Amazon Web Services, quindi seleziona l'app Amazon Web Services (SAML) dall'elenco.
5. Nella pagina Dettagli dell'GoogleIdentity Provider - Amazon Web Services, puoi effettuare una delle seguenti operazioni:

   a. Scarica i metadati IdP.

   b. Copia l'URL SSO, l'URL dell'Entity ID e le informazioni sul certificato.

   Avrai bisogno del file XML o delle informazioni sull'URL nel passaggio 2.
6. Prima di passare alla fase successiva della console di Google amministrazione, lascia aperta questa pagina e passa alla console IAM Identity Center.

Fase 2: IAM Identity Center eGoogle Workspace: Modifica dell'origine dell'identità IAM Identity Center e configurazione Google Workspace come provider di identità SAML

1. Accedi alla console IAM Identity Center utilizzando un ruolo con autorizzazioni amministrative.
2. Scegli Impostazioni nel riquadro di navigazione a sinistra.
3. Nella pagina Impostazioni, scegli Azioni, quindi scegli Cambia origine dell'identità.

- Se non hai abilitato IAM Identity Center, consulta Abilitazione di IAM Identity Center per ulteriori informazioni. Dopo aver abilitato e effettuato l'accesso a IAM Identity Center per la prima volta, arriverai alla Dashboard dove potrai selezionare Scegli la tua fonte di identità.

4. Nella pagina Scegli l'origine dell'identità, seleziona Provider di identità esterno, quindi scegli Avanti.
5. Viene visualizzata la pagina Configura provider di identità esterno. Per completare questa pagina e la Google Workspace pagina del passaggio 1, è necessario completare quanto segue:

   - Nella sezione dei metadati di Identity Provider nella console IAM Identity Center, dovrai eseguire una delle seguenti operazioni:

     i. Carica i metadati GoogleSAML come metadati IdP SAML nella console IAM Identity Center.

     ii. Copia e incolla l'URL GoogleSSO nel campo URL di accesso IdPGoogle, l'URL dell'emittente nel campo URL dell'emittente IdP e carica il certificato come certificato IdP. Google

6. Dopo aver fornito i Google metadati nella sezione dei metadati Identity Provider della console IAM Identity Center, copia l'URL di accesso al portale di accesso, l'URL di accesso al portale di AWS accesso, l'URL di IAM Identity Assertion Consumer Service (ACS) e l'URL dell'emittente di IAM Identity Center. Dovrai fornire questi URL nella Console di amministrazione nel passaggio successivo. Google
7. Lascia la pagina aperta con la console IAM Identity Center e torna alla Console di Google amministrazione. Dovresti trovarti nella pagina dei dettagli di Amazon Web Services - Service Provider. Seleziona Continua.
8. Nella pagina dei dettagli del fornitore di servizi, inserisci i valori URL ACS, Entity ID e Start URL. Hai copiato questi valori nel passaggio precedente e sono disponibili nella console IAM Identity Center.

   - Incolla l'URL IAM Identity Center Assertion Consumer Service (ACS) nel campo URL ACS
   - Incolla l'URL dell'emittente di IAM Identity Center nel campo Entity ID.
   - Incolla l'URL di AWS accesso al portale di accesso nel campo URL iniziale.

9. Nella pagina dei dettagli del fornitore di servizi, completa i campi sotto Nome ID come segue:

   - Per il formato Name ID, seleziona EMAIL
   - Per Name ID, seleziona Informazioni di base > Email principale

10. Scegli Continua.
11. Nella pagina Mappatura degli attributi, in Attributi, scegli AGGIUNGI MAPPATURA, quindi configura questi campi in Attributo di Googledirectory:
    - Per l'attributo **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`** dell'app, seleziona il campo Informazioni di base, Email principale dagli Google Directory attributi.
    - Per l'attributo **`https://aws.amazon.com/SAML/Attributes/Role`** dell'app, seleziona qualsiasi Google Directoryattributo. Un attributo Google Directory potrebbe essere Department.
12. Scegli Finish
13. Torna alla console IAM Identity Center e scegli Avanti. Nella pagina Rivedi e conferma, esamina le informazioni, quindi inserisci ACCEPT nell'apposito spazio. Scegli Cambia fonte di identità.

Ora sei pronto per abilitare l'app Amazon Web Services in Google Workspace modo che i tuoi utenti possano essere inseriti in IAM Identity Center.

Passaggio 3Google Workspace: abilitare le app

1. Torna alla Console di Google amministrazione e alla tua AWS IAM Identity Center applicazione, che puoi trovare in App e app Web e mobili.
2. Nel pannello Accesso utente accanto a Accesso utente, scegli la freccia rivolta verso il basso per espandere l'accesso utente e visualizzare il pannello di stato del servizio.
3. Nel pannello Stato del servizio, scegli ON per tutti, quindi scegli SALVA.

> **Note**
>
> Per contribuire a mantenere il principio del privilegio minimo, dopo aver completato questo tutorial, ti consigliamo di modificare lo stato del servizio su OFF per tutti. Solo gli utenti che devono accedere a AWS devono avere il servizio abilitato. Puoi utilizzare Google Workspace gruppi o unità organizzative per concedere l'accesso utente a un particolare sottoinsieme dei tuoi utenti.

Fase 4: IAM Identity Center: configurazione del provisioning automatico di IAM Identity Center

1. Torna alla console IAM Identity Center.
2. Nella pagina Impostazioni, individua la casella Informazioni sul provisioning automatico, quindi scegli Abilita. Ciò abilita immediatamente il provisioning automatico in IAM Identity Center e visualizza le informazioni necessarie sull'endpoint SCIM e sul token di accesso.
3. Nella finestra di dialogo di provisioning automatico in entrata, copia ciascuno dei valori per le seguenti opzioni. Nel passaggio 5 di questo tutorial, inserirete questi valori per configurare il provisioning automatico. Google Workspace

   - Endpoint SCIM
   - Token di accesso

   > **Warning**
   >
   > Questa è l'unica volta in cui è possibile ottenere l'endpoint SCIM e il token di accesso. Assicurati di copiare questi valori prima di andare avanti.

4. Scegli Chiudi.

   Ora che hai configurato il provisioning nella console IAM Identity Center, nel passaggio successivo configurerai il provisioning automatico in. Google Workspace

Fase 5Google Workspace: Configurazione del provisioning automatico

1. Torna alla Console di Google amministrazione e alla tua AWS IAM Identity Center applicazione, che puoi trovare in App e app Web e mobili. Nella sezione Provisioning automatico, scegli Configura il provisioning automatico.
2. Nella procedura precedente, hai copiato il valore del token di accesso nella console IAM Identity Center. Incolla quel valore nel campo del token di accesso e scegli Continua. Inoltre, nella procedura precedente, hai copiato il valore dell'endpoint SCIM nella console IAM Identity Center. Incolla quel valore nel campo URL dell'endpoint. Assicurati di rimuovere la barra finale alla fine dell'URL e scegli Continua.

3. Verifica che tutti gli attributi obbligatori di IAM Identity Center (quelli contrassegnati con *) siano mappati agli attributi. Google Cloud Directory In caso contrario, scegli la freccia rivolta verso il basso e associa l'attributo appropriato. Scegli Continua.
4. Nella sezione Provisioning scope, puoi scegliere un gruppo con la tua Google Workspace directory per fornire l'accesso all'app Amazon Web Services. Salta questo passaggio e seleziona Continua.
5. Nella sezione Deprovisioning, puoi scegliere come rispondere a diversi eventi che rimuovono l'accesso a un utente. Per ogni situazione è possibile specificare il periodo di tempo prima che inizi il deprovisioning per:

   - entro 24 ore
   - dopo un giorno
   - dopo sette giorni
   - dopo 30 giorni

   In ogni situazione è previsto un orario in cui sospendere l'accesso di un account e quando eliminare l'account.

   > **Tip**
   >
   > Imposta sempre più tempo prima di eliminare l'account di un utente piuttosto che sospendere l'account di un utente.

6. Scegli Fine. Verrai reindirizzato alla pagina dell'app Amazon Web Services.
7. Nella sezione Provisioning automatico, attiva l'interruttore a levetta per modificarlo da Inattivo a Attivo.

   > **Note**
   >
   > Il cursore di attivazione è disabilitato se IAM Identity Center non è attivato per gli utenti. Scegli Accesso utente e attiva l'app per abilitare lo slider.

8. Nella finestra di dialogo di conferma, scegli Attiva.
9. Per verificare che gli utenti siano sincronizzati correttamente con IAM Identity Center, torna alla console IAM Identity Center e scegli Utenti. La pagina Utenti elenca gli utenti della tua Google Workspace directory che sono stati creati da SCIM. Se gli utenti non sono ancora elencati, è

possibile che il provisioning sia ancora in corso. Il provisioning può richiedere fino a 24 ore, anche se nella maggior parte dei casi viene completato in pochi minuti. Assicurati di aggiornare la finestra del browser ogni pochi minuti.

Seleziona un utente e visualizzane i dettagli. Le informazioni devono corrispondere a quelle contenute nella Google Workspace directory.

> **Complimenti!**
>
> Hai impostato correttamente una connessione SAML tra Google Workspace e AWS e hai verificato che il provisioning automatico funzioni. Ora puoi assegnare questi utenti ad account e applicazioni in IAM Identity Center. Per questo tutorial, nel passaggio successivo designiamo uno degli utenti come amministratore di IAM Identity Center concedendo loro le autorizzazioni amministrative per l'account di gestione.

Fase 6: IAM Identity Center: concedere Google Workspace agli utenti l'accesso agli account

1. Torna alla console IAM Identity Center. Nel pannello di navigazione di IAM Identity Center, in Autorizzazioni multiaccount, scegli. Account AWS
2. Nella Account AWSpagina, la struttura organizzativa mostra la radice dell'organizzazione con gli account sottostanti nella gerarchia. Seleziona la casella di controllo per il tuo account di gestione, quindi seleziona Assegna utenti o gruppi.
3. Viene visualizzato il flusso di lavoro Assegna utenti e gruppi. Consiste in tre fasi:

    a. Per il passaggio 1: Seleziona utenti e gruppi scegli l'utente che svolgerà la funzione di amministratore. Quindi scegli Successivo.

    b. Per il Passaggio 2: Seleziona i set di autorizzazioni, scegli Crea set di autorizzazioni per aprire una nuova scheda che illustra i tre passaggi secondari necessari per creare un set di autorizzazioni.

        i. Per la Fase 1: Seleziona il tipo di set di autorizzazioni, completa quanto segue:

        - In Tipo di set di autorizzazioni, scegli Set di autorizzazioni predefinito.
        - In Politica per il set di autorizzazioni predefinito, scegli. AdministratorAccess

Seleziona Successivo.

ii. Per la Fase 2: Specificate i dettagli del set di autorizzazioni, mantenete le impostazioni predefinite e scegliete Avanti.

Le impostazioni predefinite creano un set di autorizzazioni denominato *AdministratorAccess*con la durata della sessione impostata su un'ora.

iii. Per il passaggio 3: revisione e creazione, verifica che il tipo di set di autorizzazioni utilizzi la politica AWS gestita AdministratorAccess. Scegli Crea. Nella pagina Set di autorizzazioni viene visualizzata una notifica che informa che il set di autorizzazioni è stato creato. Ora puoi chiudere questa scheda nel tuo browser web.

iv. Nella scheda Assegna utenti e gruppi del browser, sei ancora al Passaggio 2: Seleziona i set di autorizzazioni da cui hai avviato il flusso di lavoro per la creazione del set di autorizzazioni.

v. Nell'area dei set di autorizzazioni, scegli il pulsante Aggiorna. Il set di *AdministratorAccess*autorizzazioni creato viene visualizzato nell'elenco. Seleziona la casella di controllo relativa al set di autorizzazioni, quindi scegli Avanti.

c. Per il passaggio 3: revisione e invio, esamina l'utente e il set di autorizzazioni selezionati, quindi scegli Invia.

La pagina si aggiorna con un messaggio che indica Account AWS che stai configurando. Attendi il completamento del processo.

Verrai reindirizzato alla Account AWS pagina. Un messaggio di notifica ti informa che il tuo Account AWS è stato riassegnato e che il set di autorizzazioni aggiornato è stato applicato. Una volta effettuato l'accesso, l'utente avrà la possibilità di scegliere il ruolo. *AdministratorAccess*

> **Note**
>
> La sincronizzazione automatica di SCIM supporta Google Workspace solo gli utenti di provisioning. Il provisioning automatico di gruppo non è supportato in questo momento. Non puoi creare gruppi per i tuoi Google Workspace utenti utilizzando. AWS Management Console Dopo aver assegnato il provisioning agli utenti, puoi creare gruppi utilizzando il comando create-group di AWS CLI Identity Store o l'API IAM. CreateGroup

Passaggio 7Google Workspace: Conferma dell'accesso Google Workspace degli utenti alle risorse AWS

1. Accedi per Google utilizzare un account utente di prova. Per informazioni su come aggiungere utenti aGoogle Workspace, consulta Google Workspacela documentazione.
2. Seleziona l'icona di Google apps avvio (waffle).
3. Scorri fino alla fine dell'elenco delle app in cui si trovano le Google Workspace app personalizzate. Vengono visualizzate due app: Amazon Web Services e il portale di AWS accesso.
4. Seleziona l'app del portale di AWS accesso. Hai effettuato l'accesso al portale e puoi vedere l' Account AWS icona. Espandi l'icona per visualizzare l'elenco a Account AWS cui l'utente può accedere. In questo tutorial hai utilizzato solo un account, quindi espandendo l'icona viene visualizzato solo un account.

   > **Note**
   >
   > Se selezioni l'app Amazon Web Services, riceverai un errore SAML. Tale app viene utilizzata per Google Workspace gli utenti che sono stati assegnati come utenti IAM e questo tutorial prevede il provisioning Google Workspace degli utenti come utenti in IAM Identity Center.

5. Seleziona l'account per visualizzare i set di autorizzazioni disponibili per l'utente. In questo tutorial hai creato il set di AdministratorAccessautorizzazioni.
6. Accanto al set di autorizzazioni ci sono i link relativi al tipo di accesso disponibile per quel set di autorizzazioni. Quando è stato creato il set di autorizzazioni, è stato specificato che sia la console di gestione che l'accesso programmatico fossero abilitati, quindi queste due opzioni sono presenti. Seleziona Console di gestione per aprire. AWS Management Console
7. L'utente ha effettuato l'accesso alla console.

(Facoltativo) Passaggio di attributi per il controllo degli accessi

Facoltativamente, puoi utilizzare la Attributi per il controllo degli accessi funzionalità di IAM Identity Center per passare un `Attribute` elemento con l'`Name`attributo `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` impostato su. Questo elemento consente di passare attributi come tag di sessione nell'asserzione SAML. Per ulteriori informazioni sui tag di sessione, consulta Passing session tag AWS STS in the IAM User Guide.

Per passare gli attributi come tag di sessione, includi l'elemento `AttributeValue` che specifica il valore del tag. Ad esempio, per passare la coppia chiave-valore del tag`CostCenter = blue`, usa il seguente attributo.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Se devi aggiungere più attributi, includi un `Attribute` elemento separato per ogni tag.

Passaggi successivi

Ora che ti sei configurato Google Workspace come provider di identità e hai assegnato il provisioning agli utenti in IAM Identity Center, puoi:

- Utilizza il comando create-group di AWS CLI Identity Store o l'API IAM CreateGroupper creare gruppi per i tuoi utenti.

  I gruppi sono utili per assegnare l'accesso a Account AWS applicazioni e applicazioni. Anziché assegnare ogni utente singolarmente, concedi le autorizzazioni a un gruppo. Successivamente, quando aggiungi o rimuovi utenti da un gruppo, l'utente ottiene o perde dinamicamente l'accesso agli account e alle applicazioni che hai assegnato al gruppo.
- Configura le autorizzazioni in base alle funzioni lavorative, vedi Creare un set di autorizzazioni.

  I set di autorizzazioni definiscono il livello di accesso di utenti e gruppi a un Account AWS. I set di autorizzazioni sono archiviati in IAM Identity Center e possono essere assegnati a uno o più Account AWS. Puoi assegnare più set di autorizzazioni a un utente.

> **Note**
>
> In qualità di amministratore di IAM Identity Center, a volte dovrai sostituire i vecchi certificati IdP con quelli più recenti. Ad esempio, potrebbe essere necessario sostituire un certificato IdP quando si avvicina la data di scadenza del certificato. Il processo di sostituzione di un certificato precedente con uno più recente viene definito rotazione dei certificati. Assicurati di leggere come gestire i certificati SAML per. Google Workspace

Utilizzo di IAM Identity Center per connettersi alla tua piattaforma di JumpCloud directory

IAM Identity Center supporta il provisioning automatico (sincronizzazione) delle informazioni degli utenti da JumpCloud Directory Platform a IAM Identity Center. Questo provisioning utilizza il protocollo System for Cross-domain Identity Management (SCIM) v2.0. Questa connessione viene configurata JumpCloud utilizzando l'endpoint e il token di accesso IAM Identity Center SCIM. Quando configuri la sincronizzazione SCIM, crei una mappatura degli attributi utente agli attributi denominati in JumpCloud IAM Identity Center. Ciò fa sì che gli attributi previsti corrispondano tra IAM Identity Center e. JumpCloud

Questa guida è basata su JumpCloud giugno 2021. I passaggi per le versioni più recenti possono variare. Questa guida contiene alcune note sulla configurazione dell'autenticazione utente tramite SAML.

I passaggi seguenti illustrano come abilitare il provisioning automatico di utenti e gruppi da JumpCloud IAM Identity Center utilizzando il protocollo SCIM.

> **Note**
>
> Prima di iniziare a distribuire SCIM, ti consigliamo di esaminare prima il. Considerazioni sull'utilizzo del provisioning automatico Quindi continua a esaminare le considerazioni aggiuntive nella sezione successiva.

Argomenti

Prerequisiti

Prima di iniziare, avrai bisogno di quanto segue:

- JumpCloudabbonamento o prova gratuita. Per iscriverti a una prova gratuita, visita JumpCloud.
- Un account abilitato per IAM Identity Center (gratuito). Per ulteriori informazioni, consulta Enable IAM Identity Center.
- Una connessione SAML dal tuo JumpCloud account a IAM Identity Center, come descritto nella JumpClouddocumentazione per IAM Identity Center.
- Associa il connettore IAM Identity Center ai gruppi a cui desideri consentire l'accesso agli AWS account.

Considerazioni SCIM

Di seguito sono riportate alcune considerazioni sull'utilizzo JumpCloud della federazione per IAM Identity Center.

- Solo i gruppi associati al connettore AWS Single Sign-On JumpCloud verranno sincronizzati con SCIM.
- È possibile sincronizzare un solo attributo del numero di telefono e l'impostazione predefinita è «telefono aziendale».
- Gli utenti nella JumpCloud directory devono avere nome e cognome configurati per la sincronizzazione con IAM Identity Center con SCIM.
- Gli attributi sono ancora sincronizzati se l'utente è disabilitato in IAM Identity Center ma continua ad attivarsi in. JumpCloud
- Puoi scegliere di abilitare la sincronizzazione SCIM solo per le informazioni sugli utenti deselezionando «Abilita la gestione dei gruppi di utenti e l'appartenenza ai gruppi» nel connettore.
- Se esiste un utente esistente nella directory di Identity Center con lo stesso nome utente e lo stesso indirizzo e-mail, l'utente verrà sovrascritto e sincronizzato con SCIM da. JumpCloud

Fase 1: abilitare il provisioning in IAM Identity Center

In questo primo passaggio, utilizzi la console IAM Identity Center per abilitare il provisioning automatico.

Per abilitare il provisioning automatico in IAM Identity Center

1. Dopo aver completato i prerequisiti, apri la console IAM Identity Center.
2. Scegli Impostazioni nel riquadro di navigazione a sinistra.
3. Nella pagina Impostazioni, individua la casella Informazioni sulla fornitura automatica, quindi scegli Abilita. Ciò abilita immediatamente il provisioning automatico in IAM Identity Center e visualizza le informazioni necessarie sull'endpoint SCIM e sul token di accesso.
4. Nella finestra di dialogo di provisioning automatico in entrata, copia ciascuno dei valori per le seguenti opzioni. Dovrai incollarli in un secondo momento quando configuri il provisioning nel tuo IdP.

   a. Endpoint SCIM

   b. Token di accesso
5. Scegli Chiudi.

Ora che hai configurato il provisioning nella console IAM Identity Center, devi completare le attività rimanenti utilizzando il connettore JumpCloud IAM Identity Center. Questi passaggi sono descritti nella procedura seguente.

Fase 2: Configurare il provisioning in JumpCloud

Utilizza la seguente procedura nel connettore JumpCloud IAM Identity Center per abilitare il provisioning con IAM Identity Center. Questa procedura presuppone che tu abbia già aggiunto il connettore JumpCloud IAM Identity Center al portale e ai JumpCloud gruppi di amministrazione. Se non l'hai ancora fatto, consulta e completa questa procedura per Prerequisiti configurare il provisioning SCIM.

Per configurare il provisioning in JumpCloud

1. Apri il connettore JumpCloud IAM Identity Center che hai installato come parte della configurazione di SAML per JumpCloud (Autenticazione utente > IAM Identity Center). Per informazioni, consulta Prerequisiti.
2. Scegli il connettore IAM Identity Center, quindi scegli la terza scheda Identity Management.
3. Seleziona la casella Abilita la gestione dei gruppi di utenti e l'appartenenza ai gruppi in questa applicazione se desideri sincronizzare i gruppi con SCIM.
4. Fai clic su Configura.

5. Nella procedura precedente, hai copiato il valore dell'endpoint SCIM in IAM Identity Center. Incolla quel valore nel campo Base URL del connettore JumpCloud IAM Identity Center. Assicurati di rimuovere la barra finale alla fine dell'URL.
6. Dalla procedura precedente hai copiato il valore del token di accesso in IAM Identity Center. Incolla quel valore nel campo Token Key del connettore JumpCloud IAM Identity Center.
7. Fai clic su Attiva per applicare la configurazione.
8. Assicurati di avere un indicatore verde accanto a Single Sign-On attivato.
9. Passa alla quarta scheda Gruppi di utenti e seleziona i gruppi a cui desideri assegnare SCIM.
10. Una volta terminato, fai clic su Salva in basso.
11. Per verificare che gli utenti siano stati sincronizzati correttamente con IAM Identity Center, torna alla console IAM Identity Center e scegli Utenti. Gli utenti sincronizzati JumpCloud vengono visualizzati nella pagina Utenti. Questi utenti possono ora essere assegnati agli account all'interno di IAM Identity Center.

(Facoltativo) Fase 3: Configurazione degli attributi utente JumpCloud per il controllo degli accessi in IAM Identity Center

Questa è una procedura facoltativa da JumpCloud utilizzare se scegli di configurare gli attributi per IAM Identity Center per gestire l'accesso alle tue AWS risorse. Gli attributi che definisci JumpCloud vengono passati in un'asserzione SAML a IAM Identity Center. Quindi crei un set di autorizzazioni in IAM Identity Center per gestire l'accesso in base agli attributi da cui sei passato. JumpCloud

Prima di iniziare questa procedura, è necessario abilitare la funzione Attributi per il controllo degli accessi. Per ulteriori informazioni su come eseguire questa operazione, consulta Abilitare e configurare gli attributi per il controllo degli accessi.

Per configurare gli attributi utente JumpCloud per il controllo degli accessi in IAM Identity Center

1. Apri il connettore JumpCloud IAM Identity Center che hai installato come parte della configurazione di SAML per JumpCloud (Autenticazione utente > IAM Identity Center).
2. Scegli il connettore IAM Identity Center. Quindi, scegli la seconda scheda IAM Identity Center.
3. Nella parte inferiore di questa scheda trovi User Attribute Mapping, scegli Aggiungi nuovo attributo, quindi procedi come segue: Devi eseguire questi passaggi per ogni attributo che aggiungerai per utilizzarlo in IAM Identity Center per il controllo degli accessi.

a. Nel campo Service Provide Attribute Name, inserisci `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**`.` Replace **`AttributeName`** con il nome dell'attributo che ti aspetti in IAM Identity Center. Ad esempio, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**.

b. Nel campo JumpCloudAttribute Name, scegli gli attributi utente dalla tua JumpCloud directory. Ad esempio, Email (Work).

4. Selezionare Salva.

(Facoltativo) Passaggio di attributi per il controllo degli accessi

Facoltativamente, puoi utilizzare la Attributi per il controllo degli accessi funzionalità di IAM Identity Center per passare un `Attribute` elemento con l'`Name`attributo `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** impostato su. Questo elemento consente di passare attributi come tag di sessione nell'asserzione SAML. Per ulteriori informazioni sui tag di sessione, consulta Passing session tag AWS STS in the IAM User Guide.

Per passare gli attributi come tag di sessione, includi l'elemento `AttributeValue` che specifica il valore del tag. Ad esempio, per passare la coppia chiave-valore del tag`CostCenter = blue`, usa il seguente attributo.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Se devi aggiungere più attributi, includi un `Attribute` elemento separato per ogni tag.

Configura SAML e SCIM con Microsoft Entra ID IAM Identity Center

AWS IAM Identity Centersupporta l'integrazione con Security Assertion Markup Language (SAML) 2.0 e il provisioning automatico (sincronizzazione) di informazioni su utenti e gruppi da Microsoft Entra ID (precedentemente noto come Azure Active Directory or) in IAM Identity Center utilizzando il protocollo System for Cross-domain Identity Management (SCIMAzure AD) 2.0.

Obiettivo

In questo tutorial, configurerai un laboratorio di test e configurerai una connessione SAML e il provisioning SCIM tra Microsoft Entra ID e IAM Identity Center. Durante le fasi iniziali di preparazione, creerai un utente di prova (Nikki Wolf) sia Microsoft Entra ID in IAM Identity Center che utilizzerai per testare la connessione SAML in entrambe le direzioni. Successivamente, come parte dei passaggi SCIM, creerai un utente di test diverso (Richard Roe) per verificare che i nuovi attributi Microsoft Entra ID si sincronizzino con IAM Identity Center come previsto.

Prerequisiti

Prima di iniziare con questo tutorial, devi prima configurare quanto segue:

- Un Microsoft Entra ID inquilino. Per ulteriori informazioni, consulta Quickstart: configurare un tenant sul sito Web di Microsoft.
- Un account AWS IAM Identity Center abilitato. Per ulteriori informazioni, consulta Enable IAM Identity Center nella Guida per l'AWS IAM Identity Centerutente.

Fase 1: Preparare il tenant Microsoft

In questo passaggio, spiegherai come installare e configurare l'applicazione AWS IAM Identity Center aziendale e assegnare l'accesso a un utente di Microsoft Entra ID prova appena creato.

Step 1.1 >

Passaggio 1.1: Configurare l'applicazione AWS IAM Identity Center aziendale in Microsoft Entra ID

In questa procedura, si installa l'applicazione AWS IAM Identity Center aziendale inMicrosoft Entra ID. Questa applicazione ti servirà in seguito per configurare la tua connessione SAML conAWS.

1. Accedi all'interfaccia di amministrazione di Microsoft Entra come almeno amministratore di applicazioni cloud.
2. Passa a Identità > Applicazioni > Applicazioni aziendali, quindi scegli Nuova applicazione.
3. Nella pagina Browse Microsoft Entra Gallery, inserisci **`AWS IAM Identity Center`**nella casella di ricerca.
4. Seleziona AWS IAM Identity Centerdall'area dei risultati.
5. Scegli Crea.

Step 1.2 >

Passaggio 1.2: Creare un utente di prova in Microsoft Entra ID

Nikki Wolf è il nome del tuo utente di Microsoft Entra ID test che creerai in questa procedura.

1. Nella console dell'interfaccia di amministrazione Microsoft Entra, vai a Identità > Utenti > Tutti gli utenti.
2. Seleziona Nuovo utente, quindi scegli Crea nuovo utente nella parte superiore dello schermo.
3. In Nome principale utente, inserisci **`NikkiWolf`**, quindi seleziona il dominio e l'estensione preferiti. Ad esempio, NikkiWolf@ *`example.org`*.
4. In Nome visualizzato, immettere. **`NikkiWolf`**
5. In Password, inserisci una password sicura o seleziona l'icona a forma di occhio per mostrare la password generata automaticamente e copia o annota il valore visualizzato.
6. Scegli Proprietà, in Nome, inserisci **`Nikki`**. In Cognome, immettere **`Wolf`**.
7. Scegliete Review + create, quindi scegliete Crea.

Step 1.3

Passaggio 1.3: Metti alla prova l'esperienza di Nikki prima di assegnarle le autorizzazioni a AWS IAM Identity Center

In questa procedura, verificherai a cosa Nikki può accedere correttamente al suo portale Microsoft My Account.

1. Nello stesso browser, apri una nuova scheda, vai alla pagina di accesso al portale My Account e inserisci l'indirizzo email completo di Nikki. Ad esempio, NikkiWolf@ *`example.org`*.
2. Quando richiesto, inserisci la password di Nikki, quindi scegli Accedi. Se si tratta di una password generata automaticamente, ti verrà richiesto di cambiarla.
3. Nella pagina Azione richiesta, scegli Chiedi più tardi per ignorare la richiesta di metodi di sicurezza aggiuntivi.
4. Nella pagina Il mio account, nel menu di navigazione a sinistra, scegli Le mie app. Tieni presente che, oltre ai componenti aggiuntivi, al momento non viene visualizzata alcuna app. Aggiungerai un'AWS IAM Identity Centerapp che verrà visualizzata qui in un passaggio successivo.

Step 1.4

Passaggio 1.4: Assegna le autorizzazioni a Nikki in Microsoft Entra ID

Ora che hai verificato che Nikki può accedere correttamente al portale Il mio account, usa questa procedura per assegnare il suo utente all'app. AWS IAM Identity Center

1. Nella console dell'interfaccia di amministrazione Microsoft Entra, accedi a Identità > Applicazioni > Applicazioni aziendali, quindi scegli AWS IAM Identity Centerdall'elenco.
2. A sinistra, scegli Utenti e gruppi.
3. Scegli Add user/group (Aggiungi utente/gruppo). Puoi ignorare il messaggio che indica che i gruppi non sono disponibili per l'assegnazione. Questo tutorial non utilizza i gruppi per le assegnazioni.
4. Nella pagina Aggiungi assegnazione, in Utenti, scegli Nessuno selezionato.
5. Seleziona NikkiWolf, quindi scegli Seleziona.
6. Nella pagina Aggiungi assegnazione, scegli Assegna. NikkiWolf ora appare nell'elenco degli utenti assegnati all'AWS IAM Identity Centerapp.

Passaggio 2: prepara il tuo AWS account

In questo passaggio, spiegherai come configurare le autorizzazioni di accesso (tramite set di autorizzazioni), creare manualmente un utente Nikki Wolf corrispondente e assegnargli le autorizzazioni necessarie per amministrare le risorse. IAM Identity CenterAWS

Step 2.1 >

Passaggio 2.1: Creare un set di autorizzazioni in RegionalAdmin IAM Identity Center

Questo set di autorizzazioni verrà utilizzato per concedere a Nikki le autorizzazioni AWS dell'account necessarie per gestire le regioni dalla pagina Account all'interno di. AWS Management Console Tutte le altre autorizzazioni per visualizzare o gestire qualsiasi altra informazione relativa all'account di Nikki sono negate per impostazione predefinita.

1. Apri la console IAM Identity Center.
2. In Autorizzazioni per più account, scegli Set di autorizzazioni.
3. Scegli Create permission set (Crea set di autorizzazioni).
4. Nella pagina Seleziona il tipo di set di autorizzazioni, seleziona Set di autorizzazioni personalizzato, quindi scegli Avanti.

5. Seleziona Criterio in linea per espanderlo, quindi crea un criterio per il set di autorizzazioni utilizzando i seguenti passaggi:

   a. Scegli Aggiungi nuova dichiarazione per creare una dichiarazione politica.

   b. In Modifica rendiconto, seleziona Account dall'elenco, quindi scegli le seguenti caselle di controllo.

      - **`ListRegions`**
      - **`GetRegionOptStatus`**
      - **`DisableRegion`**
      - **`EnableRegion`**

   c. Vicino a Aggiungi una risorsa, scegli Aggiungi.

   d. Nella pagina Aggiungi risorsa, in Tipo di risorsa, seleziona Tutte le risorse, quindi scegli Aggiungi risorsa. Verifica che la tua politica sia simile alla seguente:

```
{
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "account:ListRegions",
                "account:DisableRegion",
                "account:EnableRegion",
                "account:GetRegionOptStatus"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. Seleziona Avanti.

7. Nella pagina Specificare i dettagli del set di autorizzazioni, in Nome del set di autorizzazioni **`RegionalAdmin`**, immettere e quindi scegliere Avanti.

8. Nella pagina Review and create (Rivedi e crea), scegliere Create (Crea). Dovresti essere RegionalAdminvisualizzato nell'elenco dei set di autorizzazioni.

Step 2.2 >

Passaggio 2.2: Creare un NikkiWolf utente corrispondente in IAM Identity Center

Poiché il protocollo SAML non fornisce un meccanismo per interrogare l'IdP Microsoft Entra ID () e creare automaticamente gli utenti qui in IAM Identity Center, utilizza la seguente procedura per creare manualmente un utente in IAM Identity Center che rispecchi gli attributi principali dell'utente Nikki Wolfs in. Microsoft Entra ID

1. Apri la console IAM Identity Center.
2. Scegli Utenti, scegli Aggiungi utente, quindi fornisci le seguenti informazioni:
   a. Sia per il nome utente che per l'indirizzo e-mail: inserisci la stessa **NikkiWolf@*yourcompanydomain.extension*** che hai usato durante la creazione dell'utente. Microsoft Entra ID *Ad esempio, @ example.org. NikkiWolf*
   b. Conferma l'indirizzo e-mail: inserisci nuovamente l'indirizzo e-mail del passaggio precedente
   c. Nome: immettere **Nikki**
   d. Cognome: immettere **Wolf**
   e. Nome visualizzato: immettere **Nikki Wolf**
3. Scegli Avanti due volte, quindi scegli Aggiungi utente.
4. Seleziona Close (Chiudi).

Step 2.3

Passaggio 2.3: Assegna Nikki all' RegionalAdmin autorizzazione impostata in IAM Identity Center

Qui si individuano le regioni Account AWS in cui Nikki amministrerà le regioni e quindi si assegnano le autorizzazioni necessarie per accedere correttamente al portale di accesso. AWS

1. Apri la console IAM Identity Center.
2. In Autorizzazioni multiaccount, scegli. Account AWS
3. Seleziona la casella di controllo accanto al nome dell'account (ad esempio, *Sandbox*) a cui desideri concedere a Nikki l'accesso alla gestione delle regioni, quindi scegli Assegna utenti e gruppi.
4. Nella pagina Assegna utenti e gruppi, scegli la scheda Utenti, trova e seleziona la casella accanto a Nikki, quindi scegli Avanti.

Passaggio 3: configura e verifica la tua connessione SAML

In questo passaggio, configuri la connessione SAML utilizzando l'applicazione AWS IAM Identity Center aziendale Microsoft Entra ID insieme alle impostazioni IdP esterne in IAM Identity Center.

Step 3.1 >

Fase 3.1: Raccolta dei metadati richiesti del fornitore di servizi da IAM Identity Center

In questo passaggio, avvierai la procedura guidata Change identity source dalla console IAM Identity Center e recupererai il file di metadati e l'URL di accesso AWS specifico che dovrai inserire durante la configurazione della connessione nel passaggio successivo. Microsoft Entra ID

1. Nella console IAM Identity Center, scegli Impostazioni.
2. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, quindi scegli Azioni > Modifica l'origine dell'identità.
3. Nella pagina Scegli l'origine dell'identità, seleziona Provider di identità esterno, quindi scegli Avanti.
4. Nella pagina Configura provider di identità esterno, in Metadati del provider di servizi, scegli Scarica il file di metadati per scaricarlo sul tuo sistema.
5. Nella stessa sezione, individua il valore dell'URL di AWS accesso al portale di accesso e copialo. Dovrai inserire questo valore quando richiesto nel passaggio successivo.
6. Lasciate aperta questa pagina e passate al passaggio successivo (**`Step 3.2`**) per configurare l'applicazione AWS IAM Identity Center aziendale inMicrosoft Entra ID. Successivamente, tornerai a questa pagina per completare il processo.

Step 3.2 >

Passaggio 3.2: Configurare l'applicazione AWS IAM Identity Center aziendale in Microsoft Entra ID

Questa procedura stabilisce metà della connessione SAML sul lato Microsoft utilizzando i valori del file di metadati e dell'URL di accesso ottenuti nell'ultimo passaggio.

1. Nella console dell'interfaccia di amministrazione Microsoft Entra, accedi a Identità > Applicazioni > Applicazioni aziendali, quindi scegli AWS IAM Identity Center.
2. A sinistra, scegli Single Sign-on.

3. Nella pagina Configura Single Sign-On con SAML, scegli Carica file di metadati, scegli l'icona della cartella, seleziona il file di metadati del fornitore di servizi che hai scaricato nel passaggio precedente, quindi scegli Aggiungi.
4. Nella pagina Configurazione SAML di base, verifica che entrambi i valori Identifier e Reply URL puntino ora agli endpoint con. AWS `https://<REGION>.signin.aws.amazon.com/platform/saml/`
5. In URL di accesso (opzionale), incolla il valore dell'URL di AWS accesso al portale di accesso che hai copiato nel passaggio precedente (**`Step 3.1`**), scegli Salva, quindi scegli X per chiudere la finestra.
6. Se ti viene richiesto di testare il Single Sign-On conAWS IAM Identity Center, scegli No. Proverò più tardi. Effettuerai questa verifica in un passaggio successivo.
7. Nella pagina Configura Single Sign-On con SAML, nella sezione Certificati SAML, accanto a Federation Metadata XML, scegli Scarica per salvare il file di metadati sul tuo sistema. Dovrai caricare questo file quando richiesto nel passaggio successivo.

Step 3.3 **>**

Passaggio 3.3: Configurazione dell'IdP Microsoft Entra ID esterno in AWS IAM Identity Center

Qui tornerai alla procedura guidata Change identity source nella console IAM Identity Center per completare la seconda metà della connessione SAML. AWS

1. Torna alla sessione del browser da cui hai lasciato aperta **`Step 3.1`**nella console IAM Identity Center.
2. Nella pagina Configura provider di identità esterno, nella sezione Metadati del provider di identità, in Metadati SAML IdP, scegli il pulsante Scegli file e seleziona il file di metadati del provider di identità Microsoft Entra ID da cui hai scaricato nel passaggio precedente, quindi scegli Apri.
3. Seleziona Avanti.
4. Dopo aver letto la dichiarazione di non responsabilità e aver iniziato a procedere, inserisci. **`ACCEPT`**
5. Scegli Cambia origine identità per applicare le modifiche.

Step 3.4 **>**

Passaggio 3.4: Verifica che Nikki venga reindirizzata al portale di accesso AWS

In questa procedura, testerai la connessione SAML accedendo al portale My Account di Microsoft con le credenziali di Nikki. Una volta autenticata, selezionerai l'AWS IAM Identity Centerapplicazione che reindirizzerà Nikki al portale di accesso. AWS

1. Vai alla pagina di accesso al portale Il mio account e inserisci l'indirizzo email completo di Nikki. Ad esempio, ***NikkiWolf***@ *example.org*.
2. Quando richiesto, inserisci la password di Nikki, quindi scegli Accedi.
3. Nella pagina Il mio account, nel menu di navigazione a sinistra, scegli Le mie app.
4. Nella pagina Le mie app, seleziona l'app denominata AWS IAM Identity Center. Questo dovrebbe richiedere un'autenticazione aggiuntiva.
5. Nella pagina di accesso di Microsoft, scegli NikkiWolf le tue credenziali. Se ti viene richiesta una seconda volta l'autenticazione, scegli nuovamente NikkiWolf le tue credenziali. Questo dovrebbe reindirizzarti automaticamente al portale di accesso. AWS

   > **Tip**
   >
   > Se non vieni reindirizzato correttamente, verifica che il valore dell'URL di AWS accesso al portale di accesso che hai inserito **`Step 3.2`**corrisponda al valore da cui hai copiato. **`Step 3.1`**

6. Verifica che sia visualizzata l'icona AWSdell'account.

   > **Tip**
   >
   > Se la pagina è vuota e non viene visualizzata l'icona AWSdell'account, conferma che Nikki è stata assegnata correttamente al set di RegionalAdminautorizzazioni (vedi **`Step 2.3`**).

Step 3.5

Passaggio 3.5: Verifica il livello di accesso di Nikki per gestirla Account AWS

In questo passaggio, controllerai il livello di accesso di Nikki per gestire le impostazioni della regione per lei. Account AWS Nikki dovrebbe avere solo i privilegi di amministratore sufficienti per gestire le regioni dalla pagina Account.

1. Nel portale di AWS accesso, scegli l'icona AWSAccount

   per espandere l'elenco degli account. Dopo aver scelto l'icona, vengono visualizzati i nomi degli account, gli ID degli account e gli indirizzi e-mail associati a tutti gli account in cui sono stati definiti i set di autorizzazioni.
2. Scegli il nome dell'account (ad esempio, *Sandbox*) a cui hai applicato il set di autorizzazioni (vedi **`Step 2.3`**). Questo amplierà l'elenco dei set di autorizzazioni tra cui Nikki può scegliere per gestire il suo account.
3. Quindi RegionalAdminscegli Console di gestione per assumere il ruolo definito nel set di RegionalAdminautorizzazioni. Questo ti reindirizzerà alla AWS Management Console home page.
4. Nell'angolo in alto a destra della console, scegli il nome del tuo account, quindi scegli Account. Verrai reindirizzato alla pagina Account. Nota che in tutte le altre sezioni di questa pagina viene visualizzato un messaggio che indica che non disponi delle autorizzazioni necessarie per visualizzare o modificare tali impostazioni.
5. Nella pagina Account, scorri verso il basso fino alla sezione AWSRegioni. Seleziona una casella di controllo per ogni regione disponibile nella tabella. Nota che Nikki dispone delle autorizzazioni necessarie per abilitare o disabilitare l'elenco delle regioni per il suo account, come previsto.

> Ben fatto!
>
> I passaggi da 1 a 3 ti hanno aiutato a implementare e testare con successo la tua connessione SAML. Ora, per completare il tutorial, ti invitiamo a passare alla Fase 4 per implementare il provisioning automatico.

Fase 4: Configurare e testare la sincronizzazione SCIM

In questo passaggio, configurerai il provisioning automatico (sincronizzazione) delle informazioni utente da Microsoft Entra ID IAM Identity Center utilizzando il protocollo SCIM v2.0. Questa connessione viene configurata Microsoft Entra ID utilizzando l'endpoint SCIM per IAM Identity Center e un token bearer creato automaticamente da IAM Identity Center.

Quando configuri la sincronizzazione SCIM, crei una mappatura degli attributi utente agli attributi denominati in IAM Microsoft Entra ID Identity Center. Ciò fa sì che gli attributi previsti corrispondano tra IAM Identity Center e. Microsoft Entra ID

I seguenti passaggi illustrano come abilitare il provisioning automatico degli utenti che risiedono principalmente in Microsoft Entra ID IAM Identity Center utilizzando l'app IAM Identity Center in. Microsoft Entra ID

Step 4.1 >

Passaggio 4.1: Creare un secondo utente di prova in Microsoft Entra ID

A scopo di test, creerai un nuovo utente (Richard Roe) inMicrosoft Entra ID. Successivamente, dopo aver impostato la sincronizzazione SCIM, verificherai che questo utente e tutti gli attributi pertinenti siano stati sincronizzati correttamente con IAM Identity Center.

1. Nella console dell'interfaccia di amministrazione Microsoft Entra, vai a Identità > Utenti > Tutti gli utenti.
2. Seleziona Nuovo utente, quindi scegli Crea nuovo utente nella parte superiore dello schermo.
3. In Nome principale utente, inserisci **`RichRoe`**, quindi seleziona il dominio e l'estensione preferiti. Ad esempio, RichRoe@ *`example.org`*.
4. In Nome visualizzato, immettere. **`RichRoe`**
5. In Password, inserisci una password sicura o seleziona l'icona a forma di occhio per mostrare la password generata automaticamente e copia o annota il valore visualizzato.
6. Scegli Proprietà, quindi fornisci i seguenti valori:
   - Nome - Invio **`Richard`**
   - Cognome - Invio **`Roe`**
   - Job title - Enter **`Marketing Lead`**
   - Dipartimento - Entra **`Sales`**
   - ID dipendente: inserisci **`12345`**
7. Scegli Revisione+crea, quindi scegli Crea.

Step 4.2 >

Fase 4.2: Abilita il provisioning automatico in IAM Identity Center

In questa procedura, utilizzerai la console IAM Identity Center per abilitare il provisioning automatico di utenti e gruppi provenienti da Microsoft Entra ID IAM Identity Center.

1. Apri la console IAM Identity Center e scegli Impostazioni nel riquadro di navigazione a sinistra.
2. Nella pagina Impostazioni, nella scheda Identity source, nota che il metodo di provisioning è impostato su Manuale.
3. Individua la casella Informazioni sul provisioning automatico, quindi scegli Abilita. Ciò abilita immediatamente il provisioning automatico in IAM Identity Center e visualizza le informazioni necessarie sull'endpoint SCIM e sul token di accesso.
4. Nella finestra di dialogo di provisioning automatico in entrata, copia ciascuno dei valori per le seguenti opzioni. Sarà necessario incollarli nel passaggio successivo quando si configura il provisioning in. Microsoft Entra ID

   a. Endpoint SCIM: ad esempio, https://scim. *us-east-2 .amazonaws.com/ 111-2222-3333-4444-5555 /scim/v2/*

   b. Token di accesso: scegli Mostra token per copiare il valore.
5. Scegli Chiudi.
6. Nella scheda Identity source, notate che il metodo Provisioning è ora impostato su SCIM.

Step 4.3 >

Passaggio 4.3: Configurare il provisioning automatico in Microsoft Entra ID

Ora che hai installato l'utente di RichRoe prova e hai abilitato SCIM in IAM Identity Center, puoi procedere con la configurazione delle impostazioni di sincronizzazione SCIM in. Microsoft Entra ID

1. Nella console dell'interfaccia di amministrazione Microsoft Entra, accedi a Identità > Applicazioni > Applicazioni aziendali, quindi scegli AWS IAM Identity Center.
2. Scegli Provisioning, in Gestisci, scegli nuovamente Provisioning.
3. In Provisioning Mode, seleziona Automatico.
4. In Admin Credentials, in Tenant URL incolla il valore dell'URL dell'endpoint SCIM che hai copiato in precedenza. **`Step 4.1`** In Secret Token, incolla il valore del token di accesso.

5. Scegli Test Connection (Connessione di prova). Dovresti visualizzare un messaggio che indica che le credenziali testate sono state autorizzate correttamente per abilitare il provisioning.
6. Selezionare Salva.
7. In Gestisci, scegli Utenti e gruppi, quindi scegli Aggiungi utente/gruppo.
8. Nella pagina Aggiungi assegnazione, in Utenti, scegli Nessuno selezionato.
9. Seleziona RichRoe, quindi scegli Seleziona.
10. Nella pagina Add Assignment (Aggiungi assegnazione), scegli Assign (Assegna).
11. Scegli Panoramica, quindi scegli Avvia provisioning.

Step 4.4

Passaggio 4.4: Verifica che la sincronizzazione sia avvenuta

In questa sezione, verificherai che il provisioning dell'utente di Richard sia stato eseguito correttamente e che tutti gli attributi siano visualizzati in IAM Identity Center.

1. Nella console IAM Identity Center, scegli Utenti.
2. Nella pagina Utenti, dovresti vedere il tuo RichRoeutente visualizzato. Notate che nella colonna Creato da il valore è impostato su SCIM.
3. Scegliete RichRoe, in Profilo, verificate che i seguenti attributi siano stati copiati da. Microsoft Entra ID

   - Nome - **`Richard`**
   - Cognome - **`Roe`**
   - Dipartimento - **`Sales`**
   - Titolo - **`Marketing Lead`**
   - Numero del dipendente - **`12345`**

   Ora che l'utente di Richard è stato creato in IAM Identity Center, puoi assegnarlo a qualsiasi set di autorizzazioni in modo da controllare il livello di accesso che ha alle tue AWS risorse. Ad esempio, puoi RichRoeassegnare al set di **`RegionalAdmin`** autorizzazioni che hai usato in precedenza per concedere a Nikki le autorizzazioni per gestire le regioni (vedi **`Step 2.3`**) e poi testare il suo livello di accesso utilizzando. **`Step 3.5`**

> **Complimenti!**
>
> Hai configurato correttamente una connessione SAML tra Microsoft e AWS e hai verificato che il provisioning automatico funzioni per mantenere tutto sincronizzato. Ora puoi applicare ciò che hai imparato per configurare più agevolmente il tuo ambiente di produzione.

Considerazioni sull'utilizzo di SCIM Microsoft Entra ID in un ambiente di produzione

Di seguito sono riportate importanti considerazioni in merito Microsoft Entra ID che possono influire sul modo in cui si prevede di implementare il provisioning automatico con IAM Identity Center nell'ambiente di produzione utilizzando il protocollo SCIM v2.

> **Note**
>
> Prima di iniziare a distribuire SCIM, ti consigliamo di effettuare una prima revisione. Considerazioni sull'utilizzo del provisioning automatico

Attributi per il controllo degli accessi

Gli attributi per il controllo degli accessi vengono utilizzati nelle politiche di autorizzazione che determinano chi nell'identità dell'utente può accedere alle AWS risorse. Se un attributo viene rimosso da un utente inMicrosoft Entra ID, tale attributo non verrà rimosso dall'utente corrispondente in IAM Identity Center. Si tratta di una limitazione nota inMicrosoft Entra ID. Se un attributo viene modificato in un valore diverso (non vuoto) su un utente, tale modifica verrà sincronizzata con IAM Identity Center.

Gruppi annidati

Il servizio di provisioning Microsoft Entra ID degli utenti non è in grado di leggere o effettuare il provisioning degli utenti nei gruppi nidificati. Solo gli utenti che sono membri immediati di un gruppo assegnato in modo esplicito possono essere letti e assegnati. Microsoft Entra IDnon decomprime in modo ricorsivo le appartenenze ai gruppi di utenti o gruppi assegnati indirettamente (utenti o gruppi membri di un gruppo assegnato direttamente). Per ulteriori informazioni, consulta l'ambito basato sulle assegnazioni nella documentazione. Microsoft Entra ID

Gruppi dinamici

Il servizio di provisioning Microsoft Entra ID degli utenti può leggere ed effettuare il provisioning degli utenti in gruppi dinamici. Di seguito è riportato un esempio che mostra la struttura di utenti e gruppi durante l'utilizzo di gruppi dinamici e come vengono visualizzati in IAM Identity Center. Il provisioning di questi utenti e gruppi è stato effettuato da Microsoft Entra ID IAM Identity Center tramite SCIM

Ad esempio, se Microsoft Entra ID la struttura per i gruppi dinamici è la seguente:

1. Gruppo A con membri ua1, ua2
2. Gruppo B con membri ub1
3. Gruppo C con membri uc1
4. Gruppo K con una regola per includere i membri del Gruppo A, B, C
5. Gruppo L con una regola per includere i membri dei gruppi B e C

Dopo aver fornito le informazioni su utenti e Microsoft Entra ID gruppi da IAM Identity Center tramite SCIM, la struttura sarà la seguente:

1. Gruppo A con membri ua1, ua2
2. Gruppo B con membri ub1
3. Gruppo C con membri uc1
4. Gruppo K con membri ua1, ua2, ub1, uc1
5. Gruppo L con membri ub1, uc1

Quando configuri il provisioning automatico utilizzando gruppi dinamici, tieni presenti le seguenti considerazioni.

- Un gruppo dinamico può includere un gruppo annidato. Tuttavia, il servizio di Microsoft Entra ID provisioning non appiattisce il gruppo nidificato. Ad esempio, se si dispone della seguente Microsoft Entra ID struttura per i gruppi dinamici:
  - Il gruppo A è un genitore del gruppo B.
  - Il gruppo A ha ua1 come membro.
  - Il gruppo B ha ub1 come membro.

Il gruppo dinamico che include il gruppo A includerà solo i membri diretti del gruppo A (ovvero ua1). Non includerà ricorsivamente i membri del gruppo B.

- I gruppi dinamici non possono contenere altri gruppi dinamici. Per ulteriori informazioni, consulta Limitazioni dell'anteprima nella Microsoft Entra ID documentazione.

Risoluzione dei problemi SCIM con Microsoft Entra ID

Se riscontri problemi con Microsoft Entra ID gli utenti che non si sincronizzano con IAM Identity Center, ciò potrebbe essere dovuto a un problema di sintassi che IAM Identity Center ha segnalato quando viene aggiunto un nuovo utente a IAM Identity Center. Puoi confermarlo controllando i registri di Microsoft Entra ID controllo per verificare la presenza di eventi non riusciti, ad esempio un. `'Export'` Il motivo dello stato di questo evento indicherà:

```
{"schema":["urn:ietf:params:scim:api:messages:2.0:Error"],"detail":"Request is
 unparsable, syntactically incorrect, or violates schema.","status":"400"}
```

Puoi anche verificare la presenza AWS CloudTrail di un evento non riuscito. Questo può essere fatto effettuando una ricerca nella console Event History o CloudTrail utilizzando il seguente filtro:

```
"eventName":"CreateUser"
```

L'errore nell' CloudTrail evento indicherà quanto segue:

```
"errorCode": "ValidationException",
        "errorMessage": "Currently list attributes only allow single item“
```

In definitiva, questa eccezione significa che uno dei valori trasmessi Microsoft Entra ID conteneva più valori del previsto. La soluzione in questo caso consiste nel rivedere gli attributi dell'utente inMicrosoft Entra ID, assicurandosi che nessuno contenga valori duplicati. Un esempio comune di valori duplicati è la presenza di più valori per numeri di contatto come cellulare, ufficio e fax. Sebbene siano valori separati, vengono tutti passati a IAM Identity Center con l'attributo genitore singolo phoneNumbers.

Per suggerimenti generali sulla risoluzione dei problemi SCIM, consulta. Risoluzione dei problemi relativi a IAM Identity Center

Fase 5: (Facoltativo) Configurare ABAC

Ora che hai configurato correttamente SAML e SCIM, puoi scegliere facoltativamente di configurare il controllo degli accessi basato sugli attributi (ABAC). ABAC è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi.

ConMicrosoft Entra ID, puoi utilizzare uno dei due metodi seguenti per configurare ABAC da utilizzare con IAM Identity Center.

Method 1

Metodo 1: configura gli attributi utente Microsoft Entra ID per il controllo degli accessi in IAM Identity Center

Nella procedura seguente, determinerai quali attributi Microsoft Entra ID devono essere utilizzati da IAM Identity Center per gestire l'accesso alle tue AWS risorse. Una volta definiti, Microsoft Entra ID invia questi attributi a IAM Identity Center tramite asserzioni SAML. Dovrai quindi accedere Crea un set di autorizzazioni. a IAM Identity Center per gestire l'accesso in base agli attributi da cui sei passato. Microsoft Entra ID

Prima di iniziare questa procedura, devi prima abilitare la Attributi per il controllo degli accessi funzionalità. Per ulteriori informazioni su come effettuare tale operazione, consulta Abilita e configura gli attributi per il controllo degli accessi.

1. Nella console dell'interfaccia di amministrazione Microsoft Entra, accedi a Identità > Applicazioni > Applicazioni aziendali, quindi scegli AWS IAM Identity Center.
2. Scegli Single Sign-On.
3. Nella sezione Attributi e reclami, scegli Modifica.
4. Nella pagina Attributi e rivendicazioni, procedi come segue:
    a. Scegli Aggiungi nuovo reclamo
    b. Per Nome, immetti `AccessControl:`*`AttributeName`*. Sostituiscilo *`AttributeName`*con il nome dell'attributo che ti aspetti in IAM Identity Center. Ad esempio, `AccessControl:`**`Department`**.
    c. Per Namespace (Spazio dei nomi), immettere **`https://aws.amazon.com/SAML/Attributes`**.
    d. In Source (Origine), scegliere Attribute (Attributo).
    e. Per l'attributo Source, utilizza l'elenco a discesa per scegliere gli Microsoft Entra ID attributi utente. Ad esempio, `user.`**`department`**.
5. Ripeti il passaggio precedente per ogni attributo da inviare a IAM Identity Center nell'asserzione SAML.
6. Selezionare Salva.

Method 2

Metodo 2: configura ABAC utilizzando IAM Identity Center

Con questo metodo, si utilizza la Attributi per il controllo degli accessi funzionalità di IAM Identity Center per passare un `Attribute` elemento con l'`Name`attributo `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` impostato su. Puoi utilizzare questo elemento per passare gli attributi come tag di sessione nell'asserzione SAML. Per ulteriori informazioni sui tag di sessione, consulta Passing session tag AWS STS in the IAM User Guide.

Per passare gli attributi come tag di sessione, includi l'elemento `AttributeValue` che specifica il valore del tag. Ad esempio, per passare la coppia chiave-valore del tag`CostCenter = blue`, usa il seguente attributo:

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/
AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Se devi aggiungere più attributi, includi un `Attribute` elemento separato per ogni tag.

Configura SAML e SCIM con Okta IAM Identity Center

Puoi fornire (sincronizzare) automaticamente le informazioni su utenti e gruppi da Okta IAM Identity Center utilizzando il protocollo System for Cross-domain Identity Management (SCIM) v2.0. Per configurare questa connessioneOkta, si utilizza l'endpoint SCIM per IAM Identity Center e un token bearer creato automaticamente da IAM Identity Center. Quando configuri la sincronizzazione SCIM, crei una mappatura degli attributi utente agli attributi denominati in IAM Okta Identity Center. Questa mappatura corrisponde agli attributi utente previsti tra IAM Identity Center e il tuo. Okta

Oktasupporta le seguenti funzionalità di provisioning quando è connesso a IAM Identity Center tramite SCIM:

- Crea utenti: gli utenti assegnati all'applicazione IAM Identity Center in Okta vengono forniti in IAM Identity Center.

- Aggiorna gli attributi utente: le modifiche agli attributi per gli utenti assegnati all'applicazione IAM Identity Center Okta vengono aggiornate in IAM Identity Center.
- Disattiva utenti: gli utenti non assegnati dall'applicazione IAM Identity Center Okta sono disabilitati in IAM Identity Center.
- Push di gruppo: i gruppi (e i relativi membri) Okta vengono sincronizzati con IAM Identity Center.

> **Note**
>
> Per ridurre al minimo il sovraccarico amministrativo Okta sia per IAM Identity Center che per IAM, consigliamo di assegnare e inviare gruppi anziché singoli utenti.

Se non hai ancora abilitato IAM Identity Center, consulta. Abilitazione AWS IAM Identity Center

Obiettivo

In questo tutorial, illustrerai come configurare una connessione SAML con Okta IAM Identity Center. Successivamente, sincronizzerai gli utenti daOkta, utilizzando SCIM. In questo scenario, gestisci tutti gli utenti e i gruppi in. Okta Gli utenti accedono tramite il Okta portale. Per verificare che tutto sia configurato correttamente, dopo aver completato i passaggi di configurazione, accederai come Okta utente e verificherai l'accesso alle AWS risorse.

> **Note**
>
> Puoi registrare un Okta account (prova gratuita) su cui è installata l'applicazione Okta's IAM Identity Center. Per Okta i prodotti a pagamento, potrebbe essere necessario confermare che la Okta licenza supporti la gestione del ciclo di vita o funzionalità simili che abilitano il provisioning in uscita. Queste funzionalità potrebbero essere necessarie per configurare SCIM da Okta IAM Identity Center.

Prima di iniziare

Prima di configurare il provisioning SCIM tra Okta e IAM Identity Center, ti consigliamo di esaminarlo prima. Considerazioni sull'utilizzo del provisioning automatico

Conferma i seguenti elementi prima di iniziare:

- Ogni Okta utente deve avere un valore specificato per nome, cognome, nome utente e nome visualizzato.
- Ogni Okta utente ha un solo valore per attributo di dati, ad esempio indirizzo e-mail o numero di telefono. Tutti gli utenti con più valori non riusciranno a sincronizzarsi. Se alcuni utenti hanno più valori nei propri attributi, rimuovi gli attributi duplicati prima di tentare di eseguire il provisioning dell'utente in IAM Identity Center. Ad esempio, è possibile sincronizzare solo un attributo del numero di telefono, poiché l'attributo del numero di telefono predefinito è «telefono aziendale», utilizza l'attributo «telefono aziendale» per memorizzare il numero di telefono dell'utente, anche se il numero di telefono dell'utente è un telefono di casa o un telefono cellulare.
- Se aggiorni l'indirizzo di un utente, devi aver specificato streetAddress, city, state, zipCode e il valore CountryCode. Se uno di questi valori non è specificato per l'Oktautente al momento della sincronizzazione, all'utente (o alle modifiche apportate all'utente) non verrà assegnato il provisioning.

> **Note**
>
> Le autorizzazioni e gli attributi dei ruoli non sono supportati e non possono essere sincronizzati con IAM Identity Center.
> L'utilizzo dello stesso Okta gruppo sia per le assegnazioni che per i push di gruppo non è attualmente supportato. Per mantenere coerenti le appartenenze ai gruppi tra IAM Identity Center Okta e IAM, crea un gruppo separato e configuralo per inviare i gruppi a IAM Identity Center.

Passaggio 1: ottieni i metadati SAML dal tuo account Okta

1. Accedi aOkta admin dashboard, espandi Applicazioni, quindi seleziona Applicazioni.
2. Nella pagina Applications (Applicazioni), scegli Browse App Catalog (Sfoglia catalogo app).
3. Nella casella di ricerca AWS IAM Identity Center, digita e seleziona l'app per aggiungere l'app IAM Identity Center.
4. Seleziona la scheda Accedi.
5. In Certificati di firma SAML, seleziona Azioni, quindi seleziona Visualizza metadati IdP. Si apre una nuova scheda del browser che mostra l'albero dei documenti di un file XML. Seleziona tutto il codice XML da `<md:EntityDescriptor>` a `</md:EntityDescriptor>` e copialo in un file di testo.

6. Salva il file di testo come`metadata.xml`.

Lascia Okta admin dashboard aperto, continuerai a utilizzare quella console nei passaggi successivi.

Passaggio 2: configura Okta come fonte di identità per IAM Identity Center

1. Apri la console IAM Identity Center come utente con privilegi amministrativi.
2. Scegli Impostazioni nel riquadro di navigazione a sinistra.
3. Nella pagina Impostazioni, scegli Azioni, quindi scegli Cambia origine dell'identità.
4. In Scegli l'origine dell'identità, seleziona Provider di identità esterno, quindi scegli Avanti.
5. In Configura provider di identità esterno, procedi come segue:

   a. In Metadati del fornitore di servizi, scegli Scarica il file di metadati per scaricare il file di metadati IAM Identity Center e salvarlo sul tuo sistema. Fornirai il file di metadati SAML di IAM Identity Center più avanti in questo Okta tutorial.

      Copia i seguenti elementi in un file di testo per accedervi facilmente:

      - URL dell'IAM Identity Center Assertion Consumer Service (ACS)
      - URL emittente di IAM Identity Center

      Questi valori ti serviranno più avanti in questo tutorial.

   b. In Metadati del provider di identità, in IdP SAML meta seleziona Scegli file, quindi seleziona `metadata.xml` il file creato nel passaggio precedente.

   c. Seleziona Successivo.
6. Dopo aver letto il disclaimer e aver iniziato a procedere, inserisci ACCEPT.
7. Scegli Cambia fonte di identità.

   Lascia la AWS console aperta, continuerai a usarla nel passaggio successivo.
8. Torna alla scheda Accedi dell' AWS IAM Identity Center app Okta admin dashboard e seleziona, quindi fai clic su Modifica.
9. In Impostazioni di accesso avanzate inserisci quanto segue:

   - Per l'URL ACS, inserisci il valore che hai copiato per l'URL di IAM Identity Center Assertion Consumer Service (ACS)

- Per l'URL dell'emittente, inserisci il valore che hai copiato per l'URL dell'emittente di IAM Identity Center
- Per il formato del nome utente dell'applicazione, seleziona una delle opzioni dal menu a discesa.

  Assicurati che il valore che scegli sia unico per ogni utente. Per questo tutorial, seleziona il nome utente Okta

10. Selezionare Salva.

Ora sei pronto per effettuare il provisioning degli utenti da Okta IAM Identity Center. Lascia Okta admin dashboard aperto e torna alla console IAM Identity Center per il passaggio successivo.

Fase 3: Eseguire il provisioning degli utenti da Okta

1. Nella console IAM Identity Center, nella pagina Impostazioni, individua la casella Informazioni sul provisioning automatico, quindi scegli Abilita. Ciò consente il provisioning automatico in IAM Identity Center e visualizza le informazioni necessarie sull'endpoint SCIM e sul token di accesso.
2. Nella finestra di dialogo di provisioning automatico in entrata, copia ciascuno dei valori per le seguenti opzioni:

   - Endpoint SCIM
   - Token di accesso

   Più avanti in questo tutorial inserirai questi valori per configurare il provisioning. Okta
3. Scegli Chiudi.
4. Torna all'app IAM Identity Center Okta admin dashboard e accedi all'app IAM Identity Center.
5. Nella pagina dell'app IAM Identity Center, scegli la scheda Provisioning, quindi nella barra di navigazione a sinistra in Impostazioni, scegli Integrazione.
6. Scegli Modifica, quindi seleziona la casella di controllo accanto a Abilita l'integrazione delle API per abilitare il provisioning.
7. Esegui la configurazione Okta con i valori di provisioning SCIM di IAM Identity Center che hai copiato in precedenza in questo tutorial:

   a. Nel campo Base URL, inserisci il valore dell'endpoint SCIM. Assicurati di rimuovere la barra finale alla fine dell'URL.

b. Nel campo Token API, inserisci il valore del token di accesso.

8. Scegli Test API Credentials per verificare che le credenziali inserite siano valide.

   Il messaggio AWS IAM Identity Center è stato verificato con successo! visualizza.

9. Selezionare Salva. Si passa all'area Impostazioni, con l'opzione Integrazione selezionata.
10. In Impostazioni, scegli All'app, quindi seleziona la casella di controllo Abilita per ciascuna delle funzionalità di Provisioning to App che desideri abilitare. Per questo tutorial, seleziona tutte le opzioni.
11. Selezionare Salva.

Ora sei pronto per sincronizzare i tuoi utenti Okta con IAM Identity Center.

Fase 4: Sincronizzazione degli utenti Okta con IAM Identity Center

Per impostazione predefinita, nessun gruppo o utente viene assegnato all'app Okta IAM Identity Center. I gruppi di provisioning forniscono il provisioning agli utenti che sono membri del gruppo. Completa i seguenti passaggi per sincronizzare gruppi e utenti con IAM Identity Center.

1. Nella pagina dell'app Okta IAM Identity Center, scegli la scheda Assegnazioni. Puoi assegnare sia persone che gruppi all'app IAM Identity Center.

   a. Per assegnare persone:

      - Nella pagina Assegnazioni, scegli Assegna, quindi scegli Assegna a persone.
      - Scegli gli Okta utenti a cui desideri che abbiano accesso all'app IAM Identity Center. Scegli Assegna, scegli Salva e torna indietro, quindi scegli Fine.

      Questo avvia il processo di provisioning degli utenti in IAM Identity Center.

   b. Per assegnare gruppi:

      - Nella pagina Assegnazioni, scegli Assegna, quindi scegli Assegna ai gruppi.
      - Scegli i Okta gruppi a cui desideri che abbiano accesso all'app IAM Identity Center. Scegli Assegna, scegli Salva e torna indietro, quindi scegli Fine.

      Questo avvia il processo di provisioning degli utenti del gruppo in IAM Identity Center.

> **Note**
>
> Potrebbe esserti richiesto di specificare attributi aggiuntivi per il gruppo se non sono presenti in tutti i record degli utenti. Gli attributi specificati per il gruppo sovrascriveranno i valori dei singoli attributi.

2. Scegliete la scheda Push Groups. Scegli il Okta gruppo che contiene tutti i gruppi che hai assegnato all'app IAM Identity Center. Selezionare Salva.

   Lo stato del gruppo cambia in Attivo dopo che il gruppo e i suoi membri sono stati trasferiti a IAM Identity Center.

3. Torna alla scheda Assegnazioni.

4. Se hai utenti che non sono membri dei gruppi che hai inviato a IAM Identity Center, aggiungili singolarmente utilizzando i seguenti passaggi:

   Nella pagina Assegnazioni, scegli Assegna, quindi scegli Assegna a persone.

5. Scegli gli Okta utenti a cui desideri che abbiano accesso all'app IAM Identity Center. Scegli Assegna, scegli Salva e torna indietro, quindi scegli Fine.

   Questo avvia il processo di provisioning dei singoli utenti in IAM Identity Center.

   > **Note**
   >
   > Puoi anche assegnare utenti e gruppi all' AWS IAM Identity Center app, dalla pagina Applicazioni di. Okta admin dashboard Per fare ciò, seleziona l'icona Impostazioni, quindi scegli Assegna a utenti o Assegna a gruppi, quindi specifica l'utente o il gruppo.

6. Torna alla console IAM Identity Center. Nella barra di navigazione a sinistra, seleziona Utenti, dovresti vedere l'elenco degli utenti popolato dai tuoi Okta utenti.

> **Complimenti!**
>
> Hai configurato correttamente una connessione SAML tra Okta e AWS e hai verificato che il provisioning automatico funzioni. Ora puoi assegnare questi utenti ad account e applicazioni in IAM Identity Center. Per questo tutorial, nel passaggio successivo designiamo uno

degli utenti come amministratore di IAM Identity Center concedendo loro le autorizzazioni amministrative per l'account di gestione.

Passaggio 5: concedere Okta agli utenti l'accesso agli account

1. Nel pannello di navigazione di IAM Identity Center, in Autorizzazioni multiaccount, scegli. Account AWS
2. Nella Account AWSpagina, la struttura organizzativa mostra la radice dell'organizzazione con gli account sottostanti nella gerarchia. Seleziona la casella di controllo per il tuo account di gestione, quindi seleziona Assegna utenti o gruppi.
3. Viene visualizzato il flusso di lavoro Assegna utenti e gruppi. Consiste in tre fasi:

    a. Per il passaggio 1: Seleziona utenti e gruppi scegli l'utente che svolgerà la funzione di amministratore. Quindi scegli Successivo.

    b. Per il Passaggio 2: Seleziona i set di autorizzazioni, scegli Crea set di autorizzazioni per aprire una nuova scheda che illustra i tre passaggi secondari necessari per creare un set di autorizzazioni.

        i. Per la Fase 1: Seleziona il tipo di set di autorizzazioni, completa quanto segue:

            - In Tipo di set di autorizzazioni, scegli Set di autorizzazioni predefinito.
            - In Politica per il set di autorizzazioni predefinito, scegli. AdministratorAccess

            Seleziona Successivo.

        ii. Per la Fase 2: Specificate i dettagli del set di autorizzazioni, mantenete le impostazioni predefinite e scegliete Avanti.

            Le impostazioni predefinite creano un set di autorizzazioni denominato *`AdministratorAccess`*con la durata della sessione impostata su un'ora.

        iii. Per il passaggio 3: revisione e creazione, verifica che il tipo di set di autorizzazioni utilizzi la politica AWS gestita AdministratorAccess. Scegli Crea. Nella pagina Set di autorizzazioni viene visualizzata una notifica che informa che il set di autorizzazioni è stato creato. Ora puoi chiudere questa scheda nel tuo browser web.

Nella scheda Assegna utenti e gruppi del browser, sei ancora al Passaggio 2: Seleziona i set di autorizzazioni da cui hai avviato il flusso di lavoro per la creazione del set di autorizzazioni.

Nell'area Set di autorizzazioni, scegli il pulsante Aggiorna. Il set di *AdministratorAccess*autorizzazioni creato viene visualizzato nell'elenco. Seleziona la casella di controllo relativa al set di autorizzazioni, quindi scegli Avanti.

c. Per il passaggio 3: revisione e invio, esamina l'utente e il set di autorizzazioni selezionati, quindi scegli Invia.

   La pagina si aggiorna con un messaggio che indica Account AWS che stai configurando. Attendi il completamento del processo.

   Verrai reindirizzato alla Account AWS pagina. Un messaggio di notifica ti informa che il tuo Account AWS è stato riassegnato e che il set di autorizzazioni aggiornato è stato applicato. Quando l'utente accede, avrà la possibilità di scegliere il ruolo. *AdministratorAccess*

   > **Note**
   >
   > La sincronizzazione automatica di SCIM supporta Okta solo il provisioning degli utenti; i gruppi non vengono assegnati automaticamente. Non è possibile creare gruppi per gli utenti utilizzandoOkta. AWS Management Console Dopo aver assegnato il provisioning agli utenti, puoi creare gruppi utilizzando un'operazione CLI o API

Fase 6: Conferma l'accesso Okta degli utenti alle risorse AWS

1. Accedi Okta dashboard utilizzando un account utente di prova.
2. In Le mie app seleziona l'AWS IAM Identity Centericona.
3. Hai effettuato l'accesso al portale e puoi vedere l' Account AWS icona. Espandi l'icona per visualizzare l'elenco a Account AWS cui l'utente può accedere. In questo tutorial hai utilizzato solo un account, quindi espandendo l'icona viene visualizzato solo un account.
4. Seleziona l'account per visualizzare i set di autorizzazioni disponibili per l'utente. In questo tutorial hai creato il set di AdministratorAccessautorizzazioni.

5. Accanto al set di autorizzazioni ci sono i link relativi al tipo di accesso disponibile per quel set di autorizzazioni. Quando è stato creato il set di autorizzazioni, è stato specificato che sia la console di gestione che l'accesso programmatico fossero abilitati, quindi queste due opzioni sono presenti. Seleziona Console di gestione per aprire. AWS Management Console
6. L'utente ha effettuato l'accesso alla console.

(Facoltativo) Passaggio di attributi per il controllo degli accessi

Facoltativamente, puoi utilizzare la Attributi per il controllo degli accessi funzionalità di IAM Identity Center per passare un `Attribute` elemento con l'`Name`attributo `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` impostato su. Questo elemento consente di passare attributi come tag di sessione nell'asserzione SAML. Per ulteriori informazioni sui tag di sessione, consulta Passing session tag AWS STS in the IAM User Guide.

Per passare gli attributi come tag di sessione, includi l'elemento `AttributeValue` che specifica il valore del tag. Ad esempio, per passare la coppia chiave-valore del tag`CostCenter = blue`, usa il seguente attributo.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Se devi aggiungere più attributi, includi un `Attribute` elemento separato per ogni tag.

Passaggi successivi

Ora che ti sei configurato Okta come provider di identità e hai assegnato il provisioning agli utenti in IAM Identity Center, puoi:

- Concedi l'accesso a Account AWS, vediAssegna l'accesso utente a Account AWS.
- Concedi l'accesso alle applicazioni cloud, vediAssegna l'accesso degli utenti alle applicazioni nella console IAM Identity Center.
- Configura le autorizzazioni in base alle funzioni lavorative, vedi Creare un set di autorizzazioni

Configurazione del provisioning SCIM tra OneLogin e IAM Identity Center

IAM Identity Center supporta il provisioning automatico (sincronizzazione) di informazioni su utenti e gruppi da OneLogin IAM Identity Center utilizzando il protocollo System for Cross-domain Identity Management (SCIM) v2.0. Puoi configurare questa connessione inOneLogin, utilizzando il tuo endpoint SCIM per IAM Identity Center e un token bearer creato automaticamente da IAM Identity Center. Quando configuri la sincronizzazione SCIM, crei una mappatura degli attributi utente agli attributi denominati in IAM OneLogin Identity Center. Ciò fa sì che gli attributi previsti corrispondano tra IAM Identity Center e. OneLogin

I passaggi seguenti illustrano come abilitare il provisioning automatico di utenti e gruppi da OneLogin IAM Identity Center utilizzando il protocollo SCIM.

> **Note**
>
> Prima di iniziare a distribuire SCIM, ti consigliamo di esaminare prima il. Considerazioni sull'utilizzo del provisioning automatico

Argomenti

Prerequisiti

Avrai bisogno di quanto segue prima di iniziare:

- Un OneLogin account. Se non disponi di un account esistente, potresti ottenere una versione di prova gratuita o un account sviluppatore dal OneLoginsito web.

- Un account abilitato per IAM Identity Center (gratuito). Per ulteriori informazioni, consulta Enable IAM Identity Center.
- Una connessione SAML dal tuo OneLogin account a IAM Identity Center. Per ulteriori informazioni, consulta Enabling Single Sign-On tra OneLogin e AWS sul blog AWS Partner Network.

Fase 1: abilitare il provisioning in IAM Identity Center

In questo primo passaggio, utilizzi la console IAM Identity Center per abilitare il provisioning automatico.

Per abilitare il provisioning automatico in IAM Identity Center

1. Dopo aver completato i prerequisiti, apri la console IAM Identity Center.
2. Scegli Impostazioni nel riquadro di navigazione a sinistra.
3. Nella pagina Impostazioni, individua la casella Informazioni sulla fornitura automatica, quindi scegli Abilita. Ciò abilita immediatamente il provisioning automatico in IAM Identity Center e visualizza le informazioni necessarie sull'endpoint SCIM e sul token di accesso.
4. Nella finestra di dialogo di provisioning automatico in entrata, copia ciascuno dei valori per le seguenti opzioni. Dovrai incollarli in un secondo momento quando configuri il provisioning nel tuo IdP.
   a. Endpoint SCIM
   b. Token di accesso
5. Scegli Chiudi.

Ora hai configurato il provisioning nella console IAM Identity Center. Ora devi eseguire le attività rimanenti utilizzando la console di OneLogin amministrazione come descritto nella procedura seguente.

Passaggio 2: configurare il provisioning in OneLogin

Utilizza la seguente procedura nella console di OneLogin amministrazione per abilitare l'integrazione tra IAM Identity Center e l'app IAM Identity Center. Questa procedura presuppone che tu abbia già configurato l'applicazione AWS Single Sign-On OneLogin per l'autenticazione SAML. Se non hai ancora creato questa connessione SAML, fallo prima di procedere e poi torna qui per completare il

processo di provisioning SCIM. Per ulteriori informazioni sulla configurazione di SAML conOneLogin, consulta Enabling Single Sign-On Between and on the Partner Network blog. OneLogin AWS AWS

Per configurare il provisioning in OneLogin

1. Accedi aOneLogin, quindi vai su Applicazioni > Applicazioni.
2. Nella pagina Applicazioni, cerca l'applicazione che hai creato in precedenza per creare la tua connessione SAML con IAM Identity Center. Sceglila e poi scegli Configurazione dalla barra di navigazione a sinistra.
3. Nella procedura precedente, hai copiato il valore dell'endpoint SCIM in IAM Identity Center. Incolla quel valore nel campo SCIM Base URL di. OneLogin Assicurati di rimuovere la barra finale alla fine dell'URL. Inoltre, nella procedura precedente hai copiato il valore del token di accesso in IAM Identity Center. Incolla quel valore nel campo SCIM Bearer Token di. OneLogin
4. Accanto a Connessione API, fai clic su Abilita, quindi su Salva per completare la configurazione.
5. Nella barra di navigazione a sinistra, scegli Provisioning.
6. Seleziona le caselle di controllo Abilita provisioning, Crea utente, Elimina utente e Aggiorna utente, quindi scegli Salva.
7. Nella barra di navigazione a sinistra, scegli Utenti.
8. Fai clic su Altre azioni e scegli Sincronizza accessi. Dovresti ricevere il messaggio Sincronizzazione degli utenti con AWS Single Sign-On.
9. Fai nuovamente clic su Altre azioni, quindi scegli Riapplica le mappature dei diritti. Dovresti ricevere il messaggio Le mappature vengono riapplicate.
10. A questo punto, dovrebbe iniziare il processo di approvvigionamento. Per confermare ciò, accedi ad Attività > Eventi e monitora i progressi. Gli eventi di provisioning riusciti, così come gli errori, dovrebbero apparire nel flusso degli eventi.
11. Per verificare che tutti gli utenti e i gruppi siano stati sincronizzati correttamente con IAM Identity Center, torna alla console IAM Identity Center e scegli Utenti. I tuoi utenti sincronizzati OneLogin vengono visualizzati nella pagina Utenti. È inoltre possibile visualizzare i gruppi sincronizzati nella pagina Gruppi.
12. Per sincronizzare automaticamente le modifiche degli utenti su IAM Identity Center, accedi alla pagina Provisioning, individua la sezione Richiedi l'approvazione dell'amministratore prima che questa azione venga eseguita, deseleziona Crea utente, Elimina utente e/o Aggiorna utente e fai clic su Salva.

(Facoltativo) Passaggio 3: configura gli attributi utente OneLogin per il controllo degli accessi in IAM Identity Center

Questa è una procedura opzionale OneLogin se scegli di configurare gli attributi che utilizzerai in IAM Identity Center per gestire l'accesso alle tue AWS risorse. Gli attributi che definisci OneLogin vengono passati in un'asserzione SAML a IAM Identity Center. Creerai quindi un set di autorizzazioni in IAM Identity Center per gestire l'accesso in base agli attributi da cui sei passato. OneLogin

Prima di iniziare questa procedura, devi prima abilitare la Attributi per il controllo degli accessi funzionalità. Per ulteriori informazioni su come effettuare tale operazione, consulta Abilita e configura gli attributi per il controllo degli accessi.

Per configurare gli attributi utente OneLogin per il controllo degli accessi in IAM Identity Center

1. Accedi aOneLogin, quindi vai su Applicazioni > Applicazioni.
2. Nella pagina Applicazioni, cerca l'applicazione che hai creato in precedenza per creare la tua connessione SAML con IAM Identity Center. Sceglila, quindi scegli Parametri dalla barra di navigazione a sinistra.
3. Nella sezione Parametri richiesti, procedi come segue per ogni attributo che desideri utilizzare in IAM Identity Center:
   a. Scegli +.
   b. In Nome campo`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**, inserisci e sostituisci **`AttributeName`** con il nome dell'attributo che ti aspetti in IAM Identity Center. Ad esempio, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**.
   c. In Flags, seleziona la casella accanto a Includi nell'asserzione SAML e scegli Salva.
   d. Nel campo Valore, utilizza l'elenco a discesa per scegliere gli attributi utente. OneLogin Ad esempio, Dipartimento.
4. Selezionare Salva.

(Facoltativo) Passaggio di attributi per il controllo degli accessi

Facoltativamente, puoi utilizzare la Attributi per il controllo degli accessi funzionalità di IAM Identity Center per passare un `Attribute` elemento con l'`Name`attributo `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** impostato su. Questo elemento consente di

passare attributi come tag di sessione nell'asserzione SAML. Per ulteriori informazioni sui tag di sessione, consulta Passing session tag AWS STS in the IAM User Guide.

Per passare gli attributi come tag di sessione, includi l'elemento `AttributeValue` che specifica il valore del tag. Ad esempio, per passare la coppia chiave-valore del tag`CostCenter = blue`, usa il seguente attributo.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Se devi aggiungere più attributi, includi un `Attribute` elemento separato per ogni tag.

Risoluzione dei problemi

Quanto segue può aiutarti a risolvere alcuni problemi comuni che potresti riscontrare durante la configurazione del provisioning automatico con. OneLogin

I gruppi non vengono assegnati a IAM Identity Center

Per impostazione predefinita, non è possibile effettuare il provisioning dei gruppi OneLogin da IAM Identity Center. Assicurati di aver abilitato il provisioning di gruppo per la tua applicazione IAM Identity Center in. OneLogin Per fare ciò, accedi alla console di OneLogin amministrazione e verifica che l'opzione Includi nel provisioning degli utenti sia selezionata nelle proprietà dell'applicazione IAM Identity Center (applicazione IAM Identity Center > Parametri > Gruppi). Per maggiori dettagli su come creare gruppi inOneLogin, incluso come sincronizzare i OneLogin ruoli come gruppi in SCIM, consulta il sito Web. OneLogin

Niente viene sincronizzato da OneLogin IAM Identity Center, nonostante tutte le impostazioni siano corrette

Oltre alla nota precedente relativa all'approvazione dell'amministratore, sarà necessario riapplicare le mappature delle autorizzazioni per rendere effettive molte modifiche alla configurazione. È possibile trovarlo in Applicazioni > Applicazioni > Applicazione IAM Identity Center > Altre azioni. Puoi visualizzare i dettagli e i registri per la maggior parte delle azioniOneLogin, inclusi gli eventi di sincronizzazione, in Attività > Eventi.

Ho eliminato o disabilitato un gruppo inOneLogin, ma appare ancora in IAM Identity Center

OneLoginattualmente non supporta l'operazione SCIM DELETE per i gruppi, il che significa che il gruppo continua a esistere in IAM Identity Center. È quindi necessario rimuovere il gruppo direttamente da IAM Identity Center per garantire che tutte le autorizzazioni corrispondenti in IAM Identity Center per quel gruppo vengano rimosse.

Ho eliminato un gruppo in IAM Identity Center senza prima eliminarlo da esso OneLogin e ora ho problemi di sincronizzazione utente/gruppo

Per porre rimedio a questa situazione, assicurati innanzitutto di non avere regole o configurazioni ridondanti di provisioning di gruppo. OneLogin Ad esempio, un gruppo assegnato direttamente a un'applicazione insieme a una regola di pubblicazione nello stesso gruppo. Quindi, elimina tutti i gruppi indesiderati in IAM Identity Center. Infine, inOneLogin, aggiorna le autorizzazioni (app IAM Identity Center > Provisioning > Entitlements), quindi riapplica le mappature delle autorizzazioni (app IAM Identity Center > Altre azioni). Per evitare questo problema in futuro, apporta innanzitutto la modifica per interrompere il provisioning del gruppoOneLogin, quindi elimina il gruppo da IAM Identity Center.

Utilizzo di Ping Identity prodotti con IAM Identity Center

I seguenti Ping Identity prodotti sono stati testati con IAM Identity Center.

Argomenti

PingFederate

IAM Identity Center supporta il provisioning automatico (sincronizzazione) delle informazioni su utenti e gruppi provenienti dal PingFederate prodotto Ping Identity (di seguito «Ping») in IAM Identity Center. Questo provisioning utilizza il protocollo System for Cross-domain Identity Management (SCIM) v2.0. Questa connessione viene configurata PingFederate utilizzando l'endpoint e il token di accesso IAM Identity Center SCIM. Quando configuri la sincronizzazione SCIM, crei una mappatura degli attributi utente agli attributi denominati in PingFederate IAM Identity Center. Ciò fa sì che gli attributi previsti corrispondano tra IAM Identity Center e. PingFederate

Questa guida si basa sulla PingFederate versione 10.2. I passaggi per le altre versioni possono variare. Contatta Ping per ulteriori informazioni su come configurare il provisioning a IAM Identity Center per altre versioni diPingFederate.

I passaggi seguenti illustrano come abilitare il provisioning automatico di utenti e gruppi da PingFederate IAM Identity Center utilizzando il protocollo SCIM.

> **Note**
>
> Prima di iniziare a distribuire SCIM, ti consigliamo di esaminare prima il. Considerazioni sull'utilizzo del provisioning automatico Quindi continua a esaminare le considerazioni aggiuntive nella sezione successiva.

Argomenti

Prerequisiti

Prima di iniziare, avrai bisogno di quanto segue:

- Un PingFederate server funzionante. Se non disponi di un PingFederate server esistente, potresti ottenere una versione di prova gratuita o un account sviluppatore dal sito Web di Ping Identity. La versione di prova include licenze e download di software e documentazione associata.
- Una copia del software PingFederate IAM Identity Center Connector installato sul PingFederate server. Per ulteriori informazioni su come ottenere questo software, consulta IAM Identity Center Connector sul ing Identity sito Web P.
- Un account abilitato per IAM Identity Center (gratuito). Per ulteriori informazioni, consulta Enable IAM Identity Center.
- Una connessione SAML dalla tua PingFederate istanza a IAM Identity Center. Per istruzioni su come configurare questa connessione, consulta la PingFederate documentazione. In sintesi, il percorso consigliato consiste nell'utilizzare IAM Identity Center Connector per configurare «Browser SSO» inPingFederate, utilizzando le funzionalità di «download» e «importazione»

dei metadati su entrambe le estremità per lo scambio di metadati SAML tra IAM Identity Center PingFederate e IAM Identity Center.

Ulteriori considerazioni

Di seguito sono riportate importanti considerazioni in merito PingFederate che possono influire sul modo in cui si implementa il provisioning con IAM Identity Center.

- Se un attributo (come un numero di telefono) viene rimosso da un utente nel data store configurato inPingFederate, tale attributo non verrà rimosso dall'utente corrispondente in IAM Identity Center. Questa è una limitazione nota nell'implementazione del PingFederate’s provisioner. Se un attributo viene modificato in un valore diverso (non vuoto) su un utente, tale modifica verrà sincronizzata con IAM Identity Center.

Fase 1: abilitare il provisioning in IAM Identity Center

In questo primo passaggio, utilizzi la console IAM Identity Center per abilitare il provisioning automatico.

Per abilitare il provisioning automatico in IAM Identity Center

1. Dopo aver completato i prerequisiti, apri la console IAM Identity Center.
2. Scegli Impostazioni nel riquadro di navigazione a sinistra.
3. Nella pagina Impostazioni, individua la casella Informazioni sulla fornitura automatica, quindi scegli Abilita. Ciò abilita immediatamente il provisioning automatico in IAM Identity Center e visualizza le informazioni necessarie sull'endpoint SCIM e sul token di accesso.
4. Nella finestra di dialogo di provisioning automatico in entrata, copia ciascuno dei valori per le seguenti opzioni. Dovrai incollarli in un secondo momento quando configuri il provisioning nel tuo IdP.
    a. Endpoint SCIM
    b. Token di accesso
5. Scegli Chiudi.

Ora che hai configurato il provisioning nella console IAM Identity Center, devi completare le attività rimanenti utilizzando la console di PingFederate amministrazione., I passaggi sono descritti nella procedura seguente.

Fase 2: Configurare il provisioning in PingFederate

Utilizza la seguente procedura nella console PingFederate amministrativa per abilitare l'integrazione tra IAM Identity Center e IAM Identity Center Connector. Questa procedura presuppone che tu abbia già installato il software IAM Identity Center Connector. Se non l'hai ancora fatto, consulta e completa questa procedura per Prerequisiti configurare il provisioning SCIM.

> **Important**
>
> Se il PingFederate server non è stato precedentemente configurato per il provisioning SCIM in uscita, potrebbe essere necessario apportare una modifica al file di configurazione per abilitare il provisioning. Per ulteriori informazioni, consulta la documentazione. Ping In sintesi, è necessario modificare l'`pf.provisioner.mode`impostazione nel pingfederate-<version>/pingfederate/bin/run.propertiesfile con un valore diverso da `OFF` (impostazione predefinita) e riavviare il server se attualmente in esecuzione. Ad esempio, puoi scegliere di utilizzare `STANDALONE` se attualmente non disponi di una configurazione ad alta disponibilità conPingFederate.

Per configurare il provisioning in PingFederate

1. Accedere alla console di PingFederate amministrazione.
2. Seleziona Applicazioni nella parte superiore della pagina, quindi fai clic su Connessioni SP.
3. Individua l'applicazione che hai creato in precedenza per creare la tua connessione SAML con IAM Identity Center e fai clic sul nome della connessione.
4. Seleziona Tipo di connessione dai titoli di navigazione scuri nella parte superiore della pagina. Dovresti vedere Browser SSO già selezionato nella configurazione precedente di SAML. In caso contrario, devi prima completare questi passaggi prima di poter continuare.
5. Seleziona la casella di controllo Outbound Provisioning, scegli IAM Identity Center Cloud Connector come tipo e fai clic su Salva. Se IAM Identity Center Cloud Connector non appare come opzione, assicurati di aver installato IAM Identity Center Connector e di aver riavviato il server. PingFederate

6. Fai clic su Avanti più volte fino ad arrivare alla pagina Outbound Provisioning, quindi fai clic sul pulsante Configure Provisioning.
7. Nella procedura precedente, hai copiato il valore dell'endpoint SCIM in IAM Identity Center. Incolla quel valore nel campo URL SCIM nella console. PingFederate Assicurati di rimuovere la barra finale alla fine dell'URL. Inoltre, nella procedura precedente hai copiato il valore del token di accesso in IAM Identity Center. Incolla quel valore nel campo Access Token della PingFederate console. Fai clic su Save (Salva).
8. Nella pagina Configurazione dei canali (Configura canali), fai clic su Crea.
9. Immettete un nome di canale per questo nuovo canale di provisioning (ad esempio**`AWSIAMIdentityCenterchannel`**) e fate clic su Avanti.
10. Nella pagina di origine, scegli l'Active Data Store che desideri utilizzare per la connessione a IAM Identity Center e fai clic su Avanti.

> **Note**
>
> Se non hai ancora configurato un'origine dati, devi farlo ora. Consulta la documentazione Ping del prodotto per informazioni su come scegliere e configurare un'origine dati inPingFederate.

11. Nella pagina Impostazioni sorgente, verifica che tutti i valori siano corretti per l'installazione, quindi fai clic su Avanti.
12. Nella pagina Posizione di origine, inserisci le impostazioni appropriate all'origine dati, quindi fai clic su Avanti. Ad esempio, se utilizzi Active Directory come directory LDAP:
    a. Inserisci il DN di base della tua foresta AD (ad esempio**`DC=myforest,DC=mydomain,DC=com`**).
    b. In Utenti > DN di gruppo, specifica un singolo gruppo che contenga tutti gli utenti di cui desideri effettuare il provisioning a IAM Identity Center. Se non esiste un gruppo singolo di questo tipo, crea quel gruppo in AD, torna a questa impostazione e inserisci il DN corrispondente.
    c. Specificate se effettuare la ricerca nei sottogruppi (Nested Search) e qualsiasi filtro LDAP richiesto.
    d. In Gruppi > DN di gruppo, specifica un singolo gruppo che contenga tutti i gruppi che desideri fornire a IAM Identity Center. In molti casi, questo può essere lo stesso DN specificato nella sezione Utenti. Immettete i valori Nested Search e Filter come richiesto.

13. Nella pagina Mappatura degli attributi, verifica quanto segue, quindi fai clic su Avanti:

    a. Il campo UserName deve essere mappato su un attributo formattato come e-mail (user@domain.com). Deve inoltre corrispondere al valore che l'utente utilizzerà per accedere a Ping. Questo valore a sua volta viene inserito nel `nameId` claim SAML durante l'autenticazione federata e utilizzato per la corrispondenza con l'utente in IAM Identity Center. Ad esempio, quando si utilizza Active Directory, è possibile scegliere di specificare `UserPrincipalName` come UserName.

    b. Gli altri campi con il suffisso * devono essere mappati ad attributi diversi da nulli per gli utenti.

14. Nella pagina Attivazione e riepilogo, imposta lo stato del canale su Attivo per avviare la sincronizzazione immediatamente dopo il salvataggio della configurazione.
15. Conferma che tutti i valori di configurazione nella pagina siano corretti e fai clic su Fine.
16. Nella pagina Gestisci canali, fai clic su Salva.
17. A questo punto, inizia il provisioning. Per confermare l'attività, puoi visualizzare il file provisioner.log, che si trova per impostazione predefinita nella pingfederate-<version>/pingfederate/logdirectory del tuo PingFederate server.
18. Per verificare che utenti e gruppi siano stati sincronizzati correttamente con IAM Identity Center, torna alla console IAM Identity Center e scegli Utenti. Gli utenti sincronizzati PingFederate vengono visualizzati nella pagina Utenti. È inoltre possibile visualizzare i gruppi sincronizzati nella pagina Gruppi.

(Facoltativo) Fase 3: Configurazione degli attributi utente in base alla frequenza per PingFed il controllo degli accessi in IAM Identity Center

Questa è una procedura opzionale PingFederate se scegli di configurare gli attributi che utilizzerai in IAM Identity Center per gestire l'accesso alle tue AWS risorse. Gli attributi definiti PingFederate vengono passati in un'asserzione SAML a IAM Identity Center. Creerai quindi un set di autorizzazioni in IAM Identity Center per gestire l'accesso in base agli attributi da cui sei passato. PingFederate

Prima di iniziare questa procedura, devi prima abilitare la Attributi per il controllo degli accessi funzionalità. Per ulteriori informazioni su come effettuare tale operazione, consulta Abilita e configura gli attributi per il controllo degli accessi.

Per configurare gli attributi utente PingFederate per il controllo degli accessi in IAM Identity Center

1. Accedi alla console di PingFederate amministrazione.

2. Scegli Applicazioni nella parte superiore della pagina, quindi fai clic su Connessioni SP.
3. Individua l'applicazione che hai creato in precedenza per creare la tua connessione SAML con IAM Identity Center e fai clic sul nome della connessione.
4. Scegli Browser SSO dai titoli di navigazione scuri nella parte superiore della pagina. Quindi fai clic su Configure Browser SSO.
5. Nella pagina Configure Browser SSO, scegli Assertion Creation, quindi fai clic su Configure Assertion Creation.
6. Nella pagina Configura la creazione di asserzioni, scegli Attribute Contract.
7. Nella pagina Contratto di attributo, nella sezione Estendi il contratto, aggiungi un nuovo attributo effettuando le seguenti operazioni:

   a. Nella casella di testo, inserisci`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**, sostituisci **`AttributeName`** con il nome dell'attributo che ti aspetti in IAM Identity Center. Ad esempio, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**.

   b. Per Attribute Name Format, scegli urn:oasis:names:tc:SAML:2.0:attrname-format:uri.

   c. Scegliete Aggiungi, quindi scegliete Avanti.
8. Nella pagina Authentication Source Mapping, scegli l'istanza dell'adattatore configurata con la tua applicazione.
9. Nella pagina Attribute Contract Fulfillment, scegli Source (data store) e Value (attributo data store) per l'Attribute Contract. `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**

   > **Note**
   >
   > Se non hai ancora configurato un'origine dati, dovrai farlo ora. Consulta la documentazione Ping del prodotto per informazioni su come scegliere e configurare un'origine dati inPingFederate.

10. Fai clic su Avanti più volte fino ad arrivare alla pagina Attivazione e riepilogo, quindi fai clic su Salva.

(Facoltativo) Passaggio di attributi per il controllo degli accessi

Facoltativamente, puoi utilizzare la Attributi per il controllo degli accessi funzionalità di IAM Identity Center per passare un `Attribute` elemento con l'`Name`attributo `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` impostato su. Questo elemento consente di passare attributi come tag di sessione nell'asserzione SAML. Per ulteriori informazioni sui tag di sessione, consulta Passing session tag AWS STS in the IAM User Guide.

Per passare gli attributi come tag di sessione, includi l'elemento `AttributeValue` che specifica il valore del tag. Ad esempio, per passare la coppia chiave-valore del tag`CostCenter = blue`, usa il seguente attributo.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Se devi aggiungere più attributi, includi un `Attribute` elemento separato per ogni tag.

PingOne

IAM Identity Center supporta il provisioning automatico (sincronizzazione) delle informazioni utente dal PingOne prodotto Ping Identity (di seguito «Ping») in IAM Identity Center. Questo provisioning utilizza il protocollo System for Cross-domain Identity Management (SCIM) v2.0. Questa connessione viene configurata PingOne utilizzando l'endpoint e il token di accesso IAM Identity Center SCIM. Quando configuri la sincronizzazione SCIM, crei una mappatura degli attributi utente agli attributi denominati in PingOne IAM Identity Center. Ciò fa sì che gli attributi previsti corrispondano tra IAM Identity Center e. PingOne

Questa guida è basata su PingOne ottobre 2020. I passaggi per le versioni più recenti possono variare. Contatta Ping per ulteriori informazioni su come configurare il provisioning a IAM Identity Center per altre versioni di. PingOne Questa guida contiene anche alcune note sulla configurazione dell'autenticazione utente tramite SAML.

I passaggi seguenti illustrano come abilitare il provisioning automatico degli utenti da PingOne IAM Identity Center utilizzando il protocollo SCIM.

> **Note**
>
> Prima di iniziare a distribuire SCIM, ti consigliamo di esaminare prima il. Considerazioni sull'utilizzo del provisioning automatico Quindi continua a esaminare le considerazioni aggiuntive nella sezione successiva.

Argomenti

Prerequisiti

Prima di iniziare, avrai bisogno di quanto segue:

- Un PingOne abbonamento o una prova gratuita, con funzionalità di autenticazione e provisioning federate. Per ulteriori informazioni su come ottenere una prova gratuita, consulta il Ping Identitysito Web.
- Un account abilitato per IAM Identity Center (gratuito). Per ulteriori informazioni, consulta Enable IAM Identity Center.
- L'applicazione PingOne IAM Identity Center aggiunta al tuo portale di PingOne amministrazione. È possibile ottenere l'applicazione PingOne IAM Identity Center dall'PingOneApplication Catalog. Per informazioni generali, consulta Aggiungere un'applicazione dal catalogo delle applicazioni sul Ping Identity sito Web.
- Una connessione SAML dall'PingOneistanza a IAM Identity Center. Dopo aver aggiunto l'applicazione PingOne IAM Identity Center al tuo portale di PingOne amministrazione, devi utilizzarla per configurare una connessione SAML dall'PingOneistanza a IAM Identity Center. Utilizza la funzionalità di «download» e «importazione» dei metadati su entrambe le estremità per scambiare metadati SAML tra PingOne e IAM Identity Center. Per istruzioni su come configurare questa connessione, consulta la documentazione. PingOne

Ulteriori considerazioni

Di seguito sono riportate importanti considerazioni in merito PingOne che possono influire sul modo in cui si implementa il provisioning con IAM Identity Center.

- A ottobre 2020, non PingOne supporta il provisioning di gruppi tramite SCIM. Contatta Ping per le informazioni più recenti sul supporto di gruppo in SCIM for. PingOne
- È possibile continuare a ricevere il provisioning degli utenti PingOne dopo aver disabilitato il provisioning nel portale di amministrazione. PingOne Se devi interrompere immediatamente il provisioning, elimina il token BEARER SCIM pertinente e/o disabilitalo in IAM Identity Center. Provisioning automatico
- Se un attributo per un utente viene rimosso dal data store configurato inPingOne, tale attributo non verrà rimosso dall'utente corrispondente in IAM Identity Center. Questa è una limitazione nota nell'implementazione del PingOne's provisioner. Se un attributo viene modificato, la modifica verrà sincronizzata con IAM Identity Center.
- Di seguito sono riportate note importanti relative alla configurazione SAML in: PingOne
  - IAM Identity Center supporta solo `emailaddress` come `NameId` formato. Ciò significa che devi scegliere un attributo utente univoco all'interno della tua directory inPingOne, non nullo e formattato come email/UPN (ad esempio, user@domain.com) per la mappatura SAML_SUBJECT. PingOne Email (Work) è un valore ragionevole da utilizzare per le configurazioni di test con la directory integrata. PingOne
  - Gli utenti PingOne con un indirizzo e-mail contenente un carattere + potrebbero non essere in grado di accedere a IAM Identity Center, a causa di errori come `'SAML_215' o'Invalid input'`. Per risolvere questo problemaPingOne, scegli l'opzione Avanzata per la mappatura SAML_SUBJECT in Attribute Mappings. Quindi imposta Name ID Format da inviare a SP: to nel menu a discesa. urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

Passaggio 1: abilitare il provisioning in IAM Identity Center

In questo primo passaggio, utilizzi la console IAM Identity Center per abilitare il provisioning automatico.

Per abilitare il provisioning automatico in IAM Identity Center

1. Dopo aver completato i prerequisiti, apri la console IAM Identity Center.
2. Scegli Impostazioni nel riquadro di navigazione a sinistra.

3. Nella pagina Impostazioni, individua la casella Informazioni sulla fornitura automatica, quindi scegli Abilita. Ciò abilita immediatamente il provisioning automatico in IAM Identity Center e visualizza le informazioni necessarie sull'endpoint SCIM e sul token di accesso.
4. Nella finestra di dialogo di provisioning automatico in entrata, copia ciascuno dei valori per le seguenti opzioni. Dovrai incollarli in un secondo momento quando configuri il provisioning nel tuo IdP.

   a. Endpoint SCIM
   b. Token di accesso
5. Scegli Chiudi.

Ora che hai configurato il provisioning nella console IAM Identity Center, devi completare le attività rimanenti utilizzando l'applicazione PingOne IAM Identity Center. Questi passaggi sono descritti nella procedura seguente.

Fase 2: Configurare il provisioning in PingOne

Utilizza la seguente procedura nell'applicazione PingOne IAM Identity Center per abilitare il provisioning con IAM Identity Center. Questa procedura presuppone che tu abbia già aggiunto l'applicazione PingOne IAM Identity Center al tuo portale di PingOne amministrazione. Se non l'hai ancora fatto, consulta e completa questa procedura per Prerequisiti configurare il provisioning SCIM.

Per configurare il provisioning in PingOne

1. Apri l'applicazione PingOne IAM Identity Center che hai installato come parte della configurazione di SAML per PingOne (Applicazioni > Le mie applicazioni). Per informazioni, consulta Prerequisiti.
2. Scorri fino alla fine della pagina. In User Provisioning, scegli il link completo per accedere alla configurazione di provisioning degli utenti della tua connessione.
3. Nella pagina Istruzioni per il provisioning, scegli Continua con il passaggio successivo.
4. Nella procedura precedente, hai copiato il valore dell'endpoint SCIM in IAM Identity Center. Incolla quel valore nel campo SCIM URL nell'applicazione PingOne IAM Identity Center. Assicurati di rimuovere la barra finale alla fine dell'URL. Inoltre, nella procedura precedente hai copiato il valore del token di accesso in IAM Identity Center. Incolla quel valore nel campo ACCESS_TOKEN dell'applicazione PingOne IAM Identity Center.
5. Per REMOVE_ACTION, scegli Disabilitato o Eliminato (consulta il testo della descrizione nella pagina per maggiori dettagli).

6. Nella pagina Mappatura degli attributi, scegliete un valore da utilizzare per l'asserzione SAML_SUBJECT (`NameId`), seguendo le indicazioni fornite in precedenza in questa pagina. Ulteriori considerazioni Quindi scegli Continua al passaggio successivo.
7. Nella pagina Personalizzazione dell'PingOneapp - IAM Identity Center, apporta le modifiche di personalizzazione desiderate (opzionale) e fai clic su Continua con il passaggio successivo.
8. Nella pagina Group Access, scegli i gruppi contenenti gli utenti che desideri abilitare per il provisioning e il single sign-on su IAM Identity Center. Scegli Continua al passaggio successivo.
9. Scorri fino alla fine della pagina e scegli Fine per iniziare il provisioning.
10. Per verificare che gli utenti siano stati sincronizzati correttamente con IAM Identity Center, torna alla console IAM Identity Center e scegli Utenti. Gli utenti sincronizzati da PingOne verranno visualizzati nella pagina Utenti. Questi utenti possono ora essere assegnati ad account e applicazioni all'interno di IAM Identity Center.

    Ricorda che non PingOne supporta la fornitura di gruppi o l'appartenenza a gruppi tramite SCIM. Contattateci Ping per ulteriori informazioni.

(Facoltativo) Fase 3: Configurazione degli attributi utente PingOne per il controllo degli accessi in IAM Identity Center

Questa è una procedura facoltativa da PingOne utilizzare se scegli di configurare gli attributi per IAM Identity Center per gestire l'accesso alle tue AWS risorse. Gli attributi definiti in vengono passati in PingOne un'asserzione SAML a IAM Identity Center. Quindi crei un set di autorizzazioni in IAM Identity Center per gestire l'accesso in base agli attributi da cui sei passato. PingOne

Prima di iniziare questa procedura, è necessario abilitare la Attributi per il controllo degli accessi funzionalità. Per ulteriori informazioni su come effettuare tale operazione, consulta Abilita e configura gli attributi per il controllo degli accessi.

Per configurare gli attributi utente PingOne per il controllo degli accessi in IAM Identity Center

1. Apri l'applicazione PingOne IAM Identity Center che hai installato come parte della configurazione di SAML per PingOne (Applicazioni > Le mie applicazioni).
2. Scegli Modifica, quindi scegli Continua con il passaggio successivo fino ad arrivare alla pagina Mappature degli attributi.
3. Nella pagina Mappature degli attributi, scegli Aggiungi nuovo attributo, quindi procedi come segue. È necessario eseguire questi passaggi per ogni attributo che verrà aggiunto per l'utilizzo in IAM Identity Center per il controllo degli accessi.

a. Nel campo Application Attribute, inserisci`https://aws.amazon.com/SAML/Attributes/AccessControl:`*`AttributeName`*. Sostituisci *`AttributeName`*con il nome dell'attributo che ti aspetti in IAM Identity Center. Ad esempio, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**.

b. Nel campo Identity Bridge Attribute o Literal Value, scegli gli attributi utente dalla tua PingOne directory. Ad esempio, Email (Work).

4. Scegli Avanti alcune volte, quindi scegli Fine.

(Facoltativo) Passaggio di attributi per il controllo degli accessi

Facoltativamente, puoi utilizzare la Attributi per il controllo degli accessi funzionalità di IAM Identity Center per passare un `Attribute` elemento con l'`Name`attributo `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** impostato su. Questo elemento consente di passare attributi come tag di sessione nell'asserzione SAML. Per ulteriori informazioni sui tag di sessione, consulta Passing session tag AWS STS in the IAM User Guide.

Per passare gli attributi come tag di sessione, includi l'elemento `AttributeValue` che specifica il valore del tag. Ad esempio, per passare la coppia chiave-valore del tag`CostCenter = blue`, usa il seguente attributo.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Se devi aggiungere più attributi, includi un `Attribute` elemento separato per ogni tag.

Inizia con le attività più comuni in IAM Identity Center

Se sei un nuovo utente di IAM Identity Center, il flusso di lavoro di base per iniziare a utilizzare il servizio è:

1. Accedi alla console del tuo account di gestione se utilizzi un'istanza organizzativa di IAM Identity Center o Account AWS se utilizzi un'istanza di account di IAM Identity Center e accedi alla console IAM Identity Center.
2. Seleziona la directory che utilizzi per archiviare le identità dei tuoi utenti e gruppi dalla console IAM Identity Center. Per impostazione predefinita, IAM Identity Center ti fornisce una directory che puoi utilizzare per configurare l'accesso degli utenti. Se preferisci utilizzare un'altra fonte di identità, puoi connettere la tua Active Directory o un provider di identità esterno.
3. Per le istanze organizzative, assegna l'accesso degli utenti Account AWS selezionando gli account all'interno dell'organizzazione, quindi selezionando gli utenti o i gruppi dalla tua directory e le autorizzazioni che desideri concedere loro.
4. Offri agli utenti l'accesso alle applicazioni tramite:
   a. Configura le applicazioni SAML 2.0 gestite dal cliente selezionando una delle applicazioni preintegrate dal catalogo delle applicazioni o aggiungendo la tua applicazione SAML 2.0.
   b. Configura le proprietà dell'applicazione.
   c. Assegna agli utenti l'accesso all'applicazione. Si consiglia di assegnare l'accesso agli utenti tramite l'appartenenza al gruppo anziché aggiungere le autorizzazioni dei singoli utenti. Con i gruppi puoi concedere o negare le autorizzazioni a gruppi di utenti, anziché applicare tali autorizzazioni a ogni individuo. Se un utente passa a un'organizzazione diversa, è sufficiente spostarlo in un gruppo diverso. L'utente riceve quindi automaticamente le autorizzazioni necessarie per la nuova organizzazione.
5. Se utilizzi la directory IAM Identity Center predefinita, spiega ai tuoi utenti come AWS accedere al portale di accesso. I nuovi utenti in IAM Identity Center devono attivare le proprie credenziali utente prima di poterle utilizzare per accedere al portale di AWS accesso. Per ulteriori informazioni, consulta Accedere al portale di AWS accesso nella Guida per l'Accedi ad AWS utente

Gli argomenti di questa sezione aiutano a familiarizzare con le attività comuni eseguite dopo aver completato la configurazione iniziale di IAM Identity Center.

Se non hai ancora abilitato IAM Identity Center, consulta. Abilitazione AWS IAM Identity Center

Argomenti

Crea un set di autorizzazioni.

I set di autorizzazioni sono archiviati in IAM Identity Center e definiscono il livello di accesso che utenti e gruppi hanno a un Account AWS. Il primo set di autorizzazioni creato è il set di autorizzazioni amministrative. Se ne hai completato uno, Tutorial introduttivi hai già creato il set di autorizzazioni amministrative. Utilizza questa procedura per creare set di autorizzazioni come descritto nell'argomento Politiche AWS gestite per le funzioni lavorative nella Guida per l'utente IAM.

1. Effettua una delle seguenti operazioni per accedere a AWS Management Console.
   - Nuovo utente AWS (utente root): accedi come proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.
   - Già in uso AWS (credenziali IAM): accedi utilizzando le tue credenziali IAM con autorizzazioni amministrative.
2. Apri la console IAM Identity Center.
3. Nel pannello di navigazione di IAM Identity Center, in Autorizzazioni multiaccount, scegli Set di autorizzazioni.
4. Scegli Create permission set (Crea set di autorizzazioni).
   a. Nella pagina Seleziona il tipo di set di autorizzazioni, nella sezione Tipo di set di autorizzazioni, scegli Set di autorizzazioni predefinito.
   b. Nella sezione Politica per il set di autorizzazioni predefinito, scegli una delle seguenti opzioni:
      - AdministratorAccess
      - Fatturazione
      - DatabaseAdministrator

- DataScientist
- NetworkAdministrator
- PowerUserAccess
- ReadOnlyAccess
- SecurityAudit
- SupportUser
- SystemAdministrator
- ViewOnlyAccess

5. Nella pagina Specificare i dettagli del set di autorizzazioni, mantieni le impostazioni predefinite e scegli Avanti. L'impostazione predefinita limita la sessione a un'ora.
6. Nella pagina Rivedi e crea, conferma quanto segue:
    1. Per il passaggio 1: Seleziona il tipo di set di autorizzazioni, visualizza il tipo di set di autorizzazioni scelto.
    2. Per la Fase 2: Definizione dei dettagli del set di autorizzazioni, visualizza il nome del set di autorizzazioni scelto.
    3. Scegli Crea.

Crea un set di autorizzazioni che applichi le autorizzazioni con privilegi minimi

Per seguire la procedura ottimale di applicazione delle autorizzazioni con privilegi minimi, dopo aver creato un set di autorizzazioni amministrative, è necessario creare un set di autorizzazioni più restrittivo e assegnarlo a uno o più utenti. I set di autorizzazioni creati nella procedura precedente forniscono un punto di partenza per valutare la quantità di accesso alle risorse di cui gli utenti hanno bisogno. Per passare alle autorizzazioni con privilegi minimi, puoi eseguire IAM Access Analyzer per monitorare i principali con policy gestite. AWS Dopo aver appreso quali autorizzazioni stanno utilizzando, puoi scrivere una policy personalizzata o generare una policy con solo le autorizzazioni richieste per il tuo team.

Con IAM Identity Center, puoi assegnare più set di autorizzazioni allo stesso utente. Al tuo utente amministrativo dovrebbero inoltre essere assegnati set di autorizzazioni aggiuntivi e più restrittivi. In questo modo, possono accedere al tuo solo Account AWS con le autorizzazioni richieste, anziché utilizzare sempre le proprie autorizzazioni amministrative.

Ad esempio, se sei uno sviluppatore, dopo aver creato il tuo utente amministrativo in IAM Identity Center, puoi creare un nuovo set di autorizzazioni che concede le autorizzazioni e quindi assegnare quel set di `PowerUserAccess` autorizzazioni a te stesso. A differenza del set di autorizzazioni amministrative, che utilizza `AdministratorAccess` le autorizzazioni, il set di autorizzazioni non consente la gestione di `PowerUserAccess` utenti e gruppi IAM. Quando accedi al portale di AWS accesso per accedere al tuo AWS account, puoi scegliere `PowerUserAccess` invece di `AdministratorAccess` eseguire attività di sviluppo nell'account.

Tieni a mente le seguenti considerazioni:

- Per iniziare rapidamente a creare un set di autorizzazioni più restrittivo, utilizza un set di autorizzazioni predefinito anziché un set di autorizzazioni personalizzato.

  Con un set di autorizzazioni predefinito, che utilizza autorizzazioni predefinite, puoi scegliere una singola politica AWS gestita da un elenco di politiche disponibili. Ogni politica concede un livello specifico di accesso a AWS servizi e risorse o autorizzazioni per una funzione lavorativa comune. Per informazioni su ciascuna di queste politiche, consulta le politiche AWS gestite per le funzioni lavorative.
- È possibile configurare la durata della sessione per un set di autorizzazioni per controllare la durata dell'accesso di un utente a Account AWS.

  Quando gli utenti si federano Account AWS e utilizzano la console di AWS gestione o l'interfaccia a riga di AWS comando (AWS CLI), IAM Identity Center utilizza l'impostazione della durata della sessione nel set di autorizzazioni per controllare la durata della sessione. Per impostazione predefinita, il valore della durata della sessione, che determina il periodo di tempo in cui un utente può accedere e Account AWS prima AWS di disconnetterlo dalla sessione, è impostato su un'ora. È possibile specificare un valore massimo di 12 ore. Per ulteriori informazioni, consulta Imposta la durata della sessione.
- È inoltre possibile configurare la durata della sessione del portale di AWS accesso per controllare il periodo di tempo in cui un utente della forza lavoro è connesso al portale.

  Per impostazione predefinita, il valore di Durata massima della sessione, che determina il periodo di tempo in cui un utente della forza lavoro può accedere al portale di AWS accesso prima di dover effettuare nuovamente l'autenticazione, è di otto ore. È possibile specificare un valore massimo di 90 giorni. Per ulteriori informazioni, consulta Configura la durata della sessione del portale di AWS accesso e delle applicazioni integrate in IAM Identity Center.
- Quando accedi al portale di AWS accesso, scegli il ruolo che fornisce le autorizzazioni con privilegi minimi.

Ogni set di autorizzazioni creato e assegnato all'utente viene visualizzato come ruolo disponibile nel portale di accesso. AWS Quando accedi al portale come utente, scegli il ruolo che corrisponde al set di autorizzazioni più restrittivo che puoi utilizzare per eseguire attività nell'account, anziché. `AdministratorAccess`

- Puoi aggiungere altri utenti a IAM Identity Center e assegnare set di autorizzazioni esistenti o nuovi a tali utenti.

  Per informazioni, consulta,Assegna l'accesso Account AWS ai gruppi.

Assegna Account AWS l'accesso a un utente IAM Identity Center

Per configurare Account AWS l'accesso per un utente IAM Identity Center, devi assegnare l'utente al set di autorizzazioni Account AWS and.

1. Effettua una delle seguenti operazioni per accedere a. AWS Management Console

   - Nuovo utente AWS (utente root): accedi come proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.
   - Già in uso AWS (credenziali IAM): accedi utilizzando le tue credenziali IAM con autorizzazioni amministrative.
2. Apri la console IAM Identity Center.
3. Nel riquadro di navigazione, in Autorizzazioni multiaccount, scegli. Account AWS
4. Nella Account AWSpagina viene visualizzato un elenco ad albero della tua organizzazione. Seleziona la casella di controllo accanto Account AWS alla quale desideri assegnare l'accesso. Se stai configurando l'accesso amministrativo per IAM Identity Center, seleziona la casella di controllo accanto all'account di gestione.
5. Scegli Assegna utenti o gruppi.
6. Per il Passaggio 1: Seleziona utenti e gruppi, nella pagina Assegna utenti e gruppi a "***`Account AWS nome`***", procedi come segue:

   1. Nella scheda Utenti, seleziona l'utente a cui desideri concedere le autorizzazioni amministrative.

      Per filtrare i risultati, inizia a digitare il nome dell'utente che desideri nella casella di ricerca.
   2. Dopo aver confermato che è selezionato l'utente corretto, scegli Avanti.

7. Per il passaggio 2: Seleziona i set di autorizzazioni, nella pagina Assegna i set di autorizzazioni a "***Account AWS nome***», in Set di autorizzazioni, seleziona un set di autorizzazioni per definire il livello di accesso degli utenti e dei gruppi a tale Account AWS scopo.
8. Seleziona Successivo.
9. Per la Fase 3: Revisione e invio, nella pagina Rivedi e invia le assegnazioni a "***Account AWS nome***", procedi come segue:

    1. Rivedi l'utente e il set di autorizzazioni selezionati.
    2. Dopo aver confermato che l'utente corretto è assegnato al set di autorizzazioni, scegli Invia.

    > **Important**
    >
    > Il completamento del processo di assegnazione degli utenti potrebbe richiedere alcuni minuti. Lascia aperta questa pagina fino al completamento del processo.

10. Se si verifica una delle seguenti condizioni, segui i passaggi Richiedi agli utenti l'MFA per abilitare l'MFA per IAM Identity Center:

    - Stai utilizzando la directory predefinita di Identity Center come fonte di identità.
    - Stai usando una AWS Managed Microsoft AD directory o una directory autogestita in Active Directory come origine di identità e non stai usando RADIUS AWS Directory Service MFA con.

    > **Note**
    >
    > Se utilizzi un provider di identità esterno, tieni presente che l'IdP esterno, non IAM Identity Center, gestisce le impostazioni MFA. L'MFA in IAM Identity Center non è supportata per l'uso da parte di utenti esterni. IdPs

Quando si configura l'accesso all'account per l'utente amministrativo, il Centro identità IAM crea un ruolo IAM corrispondente. Questo ruolo, controllato da IAM Identity Center, viene creato nell'area pertinente Account AWS e le politiche specificate nel set di autorizzazioni sono allegate al ruolo.

Accedi al portale di AWS accesso con le tue credenziali IAM Identity Center

Il portale di AWS accesso fornisce agli utenti di IAM Identity Center l'accesso Single Sign-On a tutte le applicazioni assegnate Account AWS e a tutte le applicazioni tramite un portale web.

Completa i seguenti passaggi per confermare che l'utente IAM Identity Center possa accedere al portale di AWS accesso e accedere a. Account AWS

1. Effettua una delle seguenti operazioni per accedere a AWS Management Console.
   - Nuovo utente AWS (utente root): accedi come proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.
   - Stai già utilizzando AWS (credenziali IAM): accedi con le tue credenziali IAM e seleziona un ruolo di amministratore.
2. Apri la console IAM Identity Center.
3. Nel pannello di navigazione seleziona Pannello di controllo.
4. Nella pagina Dashboard, in Riepilogo delle impostazioni, scegli l'URL del portale di AWS accesso.
5. Accedi utilizzando uno dei seguenti metodi:
   - Se utilizzi Active Directory o un provider di identità (IdP) esterno come origine dell'identità, accedi utilizzando le credenziali dell'utente Active Directory o IdP.
   - Se utilizzi la directory predefinita di Identity Center come origine dell'identità, accedi utilizzando il nome utente specificato al momento della creazione dell'utente e la nuova password specificata per l'utente.

1. Nella scheda Account, individua il tuo Account AWS ed espandilo.
2. Vengono visualizzati i ruoli a tua disposizione. Ad esempio, se ti vengono assegnati sia il set di AdministratorAccessautorizzazioni che il set di autorizzazioni di fatturazione, tali ruoli vengono visualizzati nel portale di AWS accesso. Scegli il nome del ruolo IAM che desideri utilizzare per la sessione.
3. Se vieni reindirizzato alla console di AWS gestione, hai completato con successo la configurazione dell' Account AWS accesso a.

> **Note**
>
> Se non ne vedi nessuna Account AWSnell'elenco, è probabile che all'utente non sia ancora stato assegnato un set di autorizzazioni per quell'account. Per istruzioni sull'assegnazione degli utenti a un set di autorizzazioni, consultaAssegna l'accesso utente a Account AWS.

Ora che hai confermato di poter accedere utilizzando le credenziali di IAM Identity Center, passa al browser che hai usato per accedere AWS Management Console e disconnettiti dall'utente root o dalle credenziali utente IAM.

> **Important**
>
> Ti consigliamo vivamente di utilizzare le credenziali dell'utente amministrativo di IAM Identity Center quando accedi al portale di AWS accesso per eseguire attività amministrative invece di utilizzare le credenziali dell'utente IAM o dell'utente root. Conservare le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per consentire ad altri utenti di accedere ai tuoi account e alle tue applicazioni e per amministrare IAM Identity Center, crea e assegna set di autorizzazioni solo tramite IAM Identity Center.

Assegna l'accesso Account AWS ai gruppi

Dopo aver creato un utente amministrativo in IAM Identity Center e creato set di autorizzazioni aggiuntivi da utilizzare per eseguire attività con autorizzazioni con privilegi minimi, puoi fornire l'accesso ai tuoi gruppi di utenti. Account AWS

Ti consigliamo di assegnare l'accesso direttamente ai gruppi anziché ai singoli utenti. Ad esempio, se si creano gruppi e set di autorizzazioni basati su unità organizzative, se un utente si sposta in un'unità organizzativa diversa, è sufficiente spostare quell'utente in un gruppo diverso e riceverà automaticamente le autorizzazioni necessarie per la nuova unità organizzativa e perderà le autorizzazioni dell'unità organizzativa precedente.

Per assegnare l'accesso a un gruppo di utenti a Account AWS

1. Apri la console IAM Identity Center.

> **Note**
>
> Se la tua fonte di identità è, AWS Managed Microsoft AD assicurati che la console IAM Identity Center utilizzi la regione in cui si trova la AWS Managed Microsoft AD directory prima di passare alla fase successiva.

2. Nel pannello di navigazione, in Autorizzazioni multiaccount, scegli. Account AWS
3. Nella Account AWSpagina viene visualizzato un elenco ad albero della tua organizzazione. Seleziona la casella di controllo accanto a una o più Account AWS a cui desideri assegnare l'accesso Single Sign-On.

> **Note**
>
> Puoi selezionarne fino a 10 Account AWS per set di autorizzazioni.

4. Scegli Assegna utenti o gruppi.
5. Per il Passaggio 1: Seleziona utenti e gruppi, nella pagina Assegna utenti e gruppi a "***AWS-account-name***", seleziona la scheda Gruppi, quindi scegli uno o più gruppi.

   Per filtrare i risultati, inizia a digitare il nome del gruppo che desideri nella casella di ricerca.

   Per visualizzare i gruppi selezionati, scegli il triangolo laterale accanto a Utenti e gruppi selezionati.

   Dopo aver confermato che i gruppi corretti sono selezionati, scegli Avanti.
6. Per il passaggio 2: Seleziona i set di autorizzazioni, nella pagina Assegna i set di autorizzazioni a "***AWS-account-name***", seleziona uno o più set di autorizzazioni

> **Note**
>
> Se non hai creato il set di autorizzazioni desiderato prima di iniziare questa procedura, scegli Crea set di autorizzazioni e segui i passaggi indicati. Crea un set di autorizzazioni. Dopo aver creato i set di autorizzazioni da applicare, nella console IAM Identity Center, torna Account AWSe segui le istruzioni fino a raggiungere la Fase 2: Seleziona i set di autorizzazioni. Una volta raggiunto questo passaggio, seleziona i nuovi set di autorizzazioni che hai creato e procedi al passaggio successivo di questa procedura.

Dopo aver confermato che sono stati selezionati i set di autorizzazioni corretti, scegli Avanti.

7. Per la Fase 3: Revisione e invio, nella pagina Rivedi e invia le assegnazioni a "***AWS-account-name***", procedi come segue:

   1. Rivedi i gruppi e i set di autorizzazioni selezionati.
   2. Dopo aver verificato che i gruppi e i set di autorizzazioni corretti siano selezionati, scegli Invia.

> **Important**
>
> Il completamento del processo di assegnazione al gruppo potrebbe richiedere alcuni minuti. Lascia aperta questa pagina fino al completamento del processo.

> **Note**
>
> Potrebbe essere necessario concedere a utenti o gruppi le autorizzazioni per operare nell'account di AWS Organizations gestione. Poiché si tratta di un account altamente privilegiato, ulteriori restrizioni di sicurezza richiedono che tu disponga della FullAccess policy IAM o di autorizzazioni equivalenti prima di poterlo configurare. Queste restrizioni di sicurezza aggiuntive non sono richieste per nessuno degli account membri dell'organizzazione. AWS

In alternativa, è possibile utilizzare AWS CloudFormationper creare e assegnare set di autorizzazioni e assegnare utenti a tali set di autorizzazioni. Gli utenti possono quindi accedere al portale di AWS accesso o utilizzare i comandi AWS Command Line Interface (AWS CLI).

Configura l'accesso Single Sign-On alle tue applicazioni

IAM Identity Center supporta due tipi di applicazioni: applicazioni gestite e applicazioni AWS gestite dal cliente.

AWS le applicazioni gestite vengono configurate direttamente dall'interno delle console applicative pertinenti o tramite le API dell'applicazione.

Le applicazioni gestite dal cliente devono essere aggiunte alla console IAM Identity Center e configurate con i metadati appropriati sia per IAM Identity Center che per il fornitore di servizi. Puoi scegliere tra un catalogo di applicazioni di uso comune che supportano SAML 2.0 oppure puoi configurare le tue applicazioni SAML 2.0 o le tue applicazioni OAuth 2.0.

I passaggi di configurazione per configurare l'accesso Single Sign-On alle applicazioni variano in base al tipo di applicazione.

Configurare un'applicazione gestita AWS

AWS le applicazioni gestite come Amazon Managed Grafana e Amazon Monitron si integrano con IAM Identity Center e possono utilizzarlo per servizi di autenticazione e directory. Per configurare un'applicazione AWS gestita in modo che funzioni con IAM Identity Center, è necessario configurare l'applicazione direttamente dalla console per il servizio applicabile oppure è necessario utilizzare le API dell'applicazione.

Configura un'applicazione dal catalogo delle applicazioni

Puoi selezionare un'applicazione SAML 2.0 da un catalogo di applicazioni di uso comune nella console IAM Identity Center. Utilizza questa procedura per configurare una relazione di trust SAML 2.0 tra IAM Identity Center e il fornitore di servizi dell'applicazione.

Per configurare un'applicazione dal catalogo delle applicazioni

1. Apri la console IAM Identity Center.
2. Selezionare Applications (Applicazioni).
3. Scegli la scheda Gestito dal cliente.
4. Scegli Aggiungi applicazione.
5. Nella pagina Seleziona il tipo di applicazione, in Preferenze di configurazione, scegli Desidero selezionare un'applicazione dal catalogo.
6. In Catalogo delle applicazioni, iniziate a digitare il nome dell'applicazione che desiderate aggiungere nella casella di ricerca.
7. Scegliete il nome dell'applicazione dall'elenco quando appare nei risultati della ricerca, quindi scegliete Avanti.
8. Nella pagina Configura applicazione, i campi Nome visualizzato e Descrizione sono precompilati con i dettagli pertinenti per l'applicazione. È possibile modificare queste informazioni.

9. Nei metadati di IAM Identity Center, procedi come segue:

   a. Nel file di metadati SAML di IAM Identity Center, scegli Scarica per scaricare i metadati del provider di identità.

   b. In Certificato IAM Identity Center, scegli Scarica certificato per scaricare il certificato del provider di identità.

   > **Note**
   >
   > Questi file ti serviranno in seguito, quando configurerai l'applicazione dal sito Web del fornitore di servizi. Segui le istruzioni fornite dal provider.

10. (Facoltativo) In Proprietà dell'applicazione, è possibile specificare l'URL di avvio dell'applicazione, lo stato di inoltro e la durata della sessione. Per ulteriori informazioni, consulta Configura le proprietà dell'applicazione nella console IAM Identity Center.
11. In Metadati dell'applicazione, effettuate una delle seguenti operazioni:

    a. Se disponi di un file di metadati, scegli Carica il file di metadati SAML dell'applicazione. Quindi, seleziona Scegli il file per trovare e seleziona il file di metadati.

    b. Se non disponi di un file di metadati, scegli Digita manualmente i valori dei metadati, quindi fornisci i valori dell'URL dell'applicazione ACS e dell'audience SAML dell'applicazione.
12. Scegli Invia. Verrai indirizzato alla pagina dei dettagli dell'applicazione che hai appena aggiunto.

Configura la tua applicazione SAML 2.0

Utilizza questa procedura per configurare la tua relazione di trust SAML 2.0 tra IAM Identity Center e il provider di servizi della tua applicazione SAML 2.0. Prima di iniziare questa procedura, verifica di disporre del certificato e dei file di scambio dei metadati del provider di servizi in modo poter completare la configurazione del livello di attendibilità.

Per configurare la tua applicazione SAML 2.0

1. Apri la console IAM Identity Center.
2. Selezionare Applications (Applicazioni).
3. Scegli la scheda Gestito dal cliente.
4. Scegli Aggiungi applicazione.

5. Nella pagina Seleziona il tipo di applicazione, in Preferenze di configurazione, scegli Ho un'applicazione che voglio configurare.
6. In Tipo di applicazione, scegli SAML 2.0.
7. Seleziona Successivo.
8. Nella pagina Configura applicazione, in Configura applicazione, inserisci un nome visualizzato per l'applicazione, ad esempio**`MyApp`**. Quindi, inserisci una descrizione.
9. Sotto i metadati di IAM Identity Center, procedi come segue:

    a. Nel file di metadati SAML di IAM Identity Center, scegli Scarica per scaricare i metadati del provider di identità.

    b. In Certificato IAM Identity Center, scegli Scarica per scaricare il certificato del provider di identità.

    > **Note**
    >
    > Questi file saranno necessari più tardi durante la configurazione dell'applicazione personalizzata dal sito web del provider di servizi.

10. (Facoltativo) In Proprietà dell'applicazione, puoi anche specificare l'URL di avvio dell'applicazione, lo stato di inoltro e la durata della sessione. Per ulteriori informazioni, consulta Configura le proprietà dell'applicazione nella console IAM Identity Center.
11. In Metadati dell'applicazione, scegli Digita manualmente i valori dei metadati. Quindi, fornisci i valori di pubblico Application ACS URL e Application SAML dell'applicazione.
12. Scegli Invia. Verrai indirizzato alla pagina dei dettagli dell'applicazione che hai appena aggiunto.

Dopo aver configurato le applicazioni, gli utenti possono accedere alle applicazioni dal loro portale di AWS accesso in base alle autorizzazioni assegnate.

Se disponi di applicazioni gestite dai clienti che supportano OAuth 2.0 e gli utenti devono accedere da tali applicazioni ai AWS servizi, puoi utilizzare la propagazione affidabile delle identità. Con la propagazione affidabile delle identità, un utente può accedere a un'applicazione e tale applicazione può trasmettere l'identità degli utenti nelle richieste di accesso ai dati nei servizi. AWS Per ulteriori informazioni, consulta Utilizzo della propagazione affidabile delle identità con applicazioni gestite dal cliente.

Per ulteriori informazioni sui tipi di applicazioni supportati, consulta Gestire l'accesso alle applicazioni.

Visualizza le assegnazioni di utenti e gruppi

Puoi vedere chi ha accesso a cosa in IAM Identity Center dalle pagine Utenti e Gruppi. Utilizza questa procedura per visualizzare il livello di accesso degli utenti agli AWS account, ai set di autorizzazioni, alle applicazioni e ai gruppi.

1. Apri la console IAM Identity Center.
2. Scegli Utenti o Gruppi a seconda che desideri modificare un gruppo di utenti o un utente assegnato individualmente.
3. Scegli un utente o un gruppo dall'elenco.
4. Scegli se visualizzare le assegnazioni degli account, le assegnazioni delle applicazioni o le assegnazioni di gruppo:

   - AWS assegnazioni di account e set di autorizzazioni
     1. Scegliere la scheda Accounts (Account).
     2. Seleziona un account dall'elenco per visualizzare le assegnazioni dei set di autorizzazioni di utenti e gruppi.
     3. Seleziona un set di autorizzazioni da visualizzare per visualizzare i dettagli delle politiche e delle assegnazioni.
   - Assegnazioni delle applicazioni
     1. Scegli la scheda Applicazioni per visualizzare quali applicazioni sono assegnate a un utente o a un gruppo.
     2. Seleziona un'applicazione dall'elenco per visualizzare i dettagli dell'assegnazione.
   - Assegnazioni di gruppo
     1. Dalla pagina Utenti, scegli la scheda Gruppi.
     2. Seleziona un gruppo per visualizzare le assegnazioni di gruppo per un utente.

Gestisci le istanze di organizzazione e account di IAM Identity Center

Un'istanza è una singola implementazione di IAM Identity Center. Sono disponibili due tipi di istanze per IAM Identity Center: istanze organizzative e istanze di account.

Account AWS tipi che possono abilitare IAM Identity Center

Per abilitare IAM Identity Center, accedi a AWS Management Console utilizzando una delle seguenti credenziali, a seconda del tipo di istanza che desideri creare:

- Il tuo account di AWS Organizations gestione (consigliato): necessario per creare un'istanza organizzativa di IAM Identity Center. Utilizza un'istanza organizzativa per le autorizzazioni multi-account e l'assegnazione di applicazioni in tutta l'organizzazione.
- Il tuo account AWS Organizations membro: utilizza per creare un'istanza di account di IAM Identity Center per abilitare le assegnazioni delle applicazioni all'interno di quell'account membro. In un'organizzazione possono esistere uno o più account con un'istanza a livello di membro.
- Un'istanza autonoma Account AWS: da utilizzare per creare un'istanza organizzativa o un'istanza di account di IAM Identity Center. La versione standalone Account AWS non è gestita da. AWS OrganizationsÈ possibile associare una sola istanza di IAM Identity Center a una versione standalone Account AWS ed è possibile utilizzare l'istanza per le assegnazioni di applicazioni all'interno di tale istanza. Account AWS

Funzionalità	Istanza nell'account di AWS Organizations gestione (consigliata)	Istanza in un account membro	Istanza in modalità autonoma Account AWS
Gestisci gli utenti	 S	 S	 Sì
AWS portale di accesso per l'accesso Single Sign-On alle	 S	 S	 Sì

Funzionalità	Istanza nell'account di AWS Organizations gestione (consigliata)	Istanza in un account membro	Istanza in modalità autonoma Account AWS
applicazioni gestite AWS			
applicazioni gestite dai clienti OAuth 2.0 (OIDC)	 S	 S	 Sì
Autorizzazioni per più account	 S	 N	 No
AWS portale di accesso per l'accesso Single Sign-On al Account AWS	 S	 N	 No
applicazioni gestite dai clienti SAML 2.0	 S	 N	 No
L'amministratore delegato può gestire l'istanza	 S	 N	 No

Argomenti

- Istanze organizzative di IAM Identity Center
- Istanze di account di IAM Identity Center
- Abilita le istanze di account nella console IAM Identity Center
- Controlla la creazione di istanze di account con Services Control Policies
- Crea un'istanza di account di IAM Identity Center

Istanze organizzative di IAM Identity Center

Quando abiliti IAM Identity Center insieme a AWS Organizations, crei un'istanza organizzativa di IAM Identity Center. L'istanza dell'organizzazione deve essere abilitata nel tuo account di gestione e puoi gestire centralmente l'accesso di utenti e gruppi con una singola istanza organizzativa. È possibile avere una sola istanza dell'organizzazione per ogni account di gestione in AWS Organizations.

Se hai abilitato IAM Identity Center prima del 15 novembre 2023, disponi di un'istanza organizzativa di IAM Identity Center.

Quando utilizzare un'istanza organizzativa

Un'istanza organizzativa è il metodo principale per abilitare IAM Identity Center e nella maggior parte dei casi è consigliata un'istanza organizzativa. Le istanze organizzative offrono i seguenti vantaggi:

- Support per tutte le funzionalità di IAM Identity Center, inclusa la gestione delle autorizzazioni per più Account AWS utenti dell'organizzazione e l'assegnazione dell'accesso alle applicazioni gestite dai clienti.
- Riduzione del numero di punti di gestione: un'istanza organizzativa ha un unico punto di gestione, l'account di gestione. Si consiglia di abilitare un'istanza organizzativa, anziché un'istanza di account, per ridurre il numero di punti di gestione.
- Controlla la creazione di istanze di account: puoi controllare se le istanze di account possono essere create dagli account dei membri della tua organizzazione, purché non abbia distribuito un'istanza di IAM Identity Center nell'organizzazione in una regione con consenso esplicito (Regione AWS che è disabilitata per impostazione predefinita).

Istanze di account di IAM Identity Center

Con un'istanza di account di IAM Identity Center, puoi distribuire applicazioni AWS gestite supportate e applicazioni gestite dai clienti basate su OIDC. Le istanze di account supportano implementazioni isolate di applicazioni in un'unica soluzione Account AWS, sfruttando le funzionalità del portale di accesso e di identità della forza lavoro di IAM Identity Center.

Le istanze di account sono associate a un'unica istanza Account AWS e vengono utilizzate solo per gestire l'accesso di utenti e gruppi alle applicazioni supportate nello stesso account e. Regione AWS Sei limitato a un'istanza di account per. Account AWS Puoi creare un'istanza di account utilizzando uno dei seguenti metodi:

- Un account membro in AWS Organizations.
- Un sistema autonomo Account AWS che non è gestito da AWS Organizations.

Vincoli di disponibilità per gli account dei membri

È possibile distribuire un'istanza di account in un account membro di un'organizzazione se sono soddisfatte le seguenti condizioni:

- Non avevi un'istanza di IAM Identity Center distribuita nella tua organizzazione prima del 15 novembre 2023.
- Hai già distribuito un'istanza di IAM Identity Center nella tua organizzazione prima del 15 novembre 2023 e l'amministratore ha abilitato gli account dei membri a creare istanze di account IAM Identity Center.
- L'amministratore non ha creato una policy di controllo dei servizi che impedisca agli account dei membri di creare istanze di account.
- A prescindere da ciò, non hai già un'istanza di IAM Identity Center nello stesso account. Regione AWS
- Stai lavorando in un ambiente in Regione AWS cui IAM Identity Center non è disponibile. Per informazioni sulle regioni, consultaAWS IAM Identity Center Disponibilità regionale.

Argomenti

Quando utilizzare le istanze dell'account

Nella maggior parte dei casi, è consigliata un'istanza dell'organizzazione. Le istanze dell'account devono essere utilizzate solo se si applica uno dei seguenti scenari:

- Desideri eseguire una versione di prova temporanea di un'applicazione AWS gestita supportata per determinare se l'applicazione soddisfa le tue esigenze aziendali.
- Non hai intenzione di adottare IAM Identity Center nella tua organizzazione, ma desideri supportare una o più applicazioni AWS gestite.

- Disponi di un'istanza organizzativa di IAM Identity Center, ma desideri distribuire un'applicazione AWS gestita supportata a un set isolato di utenti distinti dagli utenti dell'istanza della tua organizzazione.

> **Important**
>
> Se prevedi di utilizzare IAM Identity Center per supportare applicazioni su più account, crea un'istanza organizzativa e non utilizzare le istanze di account.

Considerazioni sull'istanza dell'account

Un'istanza di account è progettata per casi d'uso specializzati e offre un sottoinsieme di funzionalità disponibili per un'istanza organizzativa. Considerate quanto segue prima di creare un'istanza di account:

- Le istanze di account non supportano i set di autorizzazioni e pertanto non supportano l'accesso a Account AWS.
- Non è possibile convertire un'istanza di account in un'istanza dell'organizzazione.
- Non puoi unire un'istanza di account in un'istanza dell'organizzazione.
- Seleziona solo le istanze dell'account di AWS applicazioni gestite supporto.
- Utilizza istanze di account per utenti isolati che utilizzeranno le applicazioni in un unico account e per tutta la durata delle applicazioni utilizzate.
- Le applicazioni collegate a un'istanza di account devono rimanere collegate all'istanza dell'account fino a quando non si eliminano l'applicazione e le relative risorse.
- Un'istanza di account deve rimanere nella posizione Account AWS in cui è stata creata.

AWS applicazioni gestite che supportano le istanze di account

Scopri quali applicazioni AWS gestite supportano le istanze di account di IAM Identity Center. AWS applicazioni gestite Verifica la disponibilità della creazione di istanze di account con la tua applicazione AWS gestita.

Abilita le istanze di account nella console IAM Identity Center

Se hai abilitato IAM Identity Center prima del 15 novembre 2023, disponi di un'istanza organizzativa di IAM Identity Center e la possibilità per gli account membro di creare istanze di account è disabilitata per impostazione predefinita. Puoi scegliere se i tuoi account membro possono creare istanze di account abilitando la funzionalità di istanza dell'account in. AWS Management Console

> **Note**
>
> Gli account membri possono creare un'istanza di account purché tu non abbia distribuito un'istanza di IAM Identity Center nella tua organizzazione in una regione con attivazione (Regione AWS disabilitata per impostazione predefinita) indipendentemente dalla data di implementazione. Qualsiasi istanza organizzativa di IAM Identity Center implementata in un opt-in Regione AWS impedirà la creazione di istanze di account. Per informazioni sulle regioni, consulta. AWS IAM Identity Center Disponibilità regionale

Per consentire la creazione di istanze di account da parte degli account dei membri dell'organizzazione

1. Apri la console IAM Identity Center.
2. Scegli Impostazioni, quindi scegli la scheda Gestione.
3. Nella sezione Istanze di account di IAM Identity Center, seleziona Abilita le istanze di account di IAM Identity Center.
4. Nella finestra di dialogo Abilita le istanze di account di IAM Identity Center, conferma di voler consentire agli account dei membri della tua organizzazione di creare istanze di account selezionando Abilita.

> **Important**
>
> L'abilitazione delle istanze di account di IAM Identity Center per gli account dei membri è un'operazione una tantum. Ciò significa che questa operazione non può essere annullata. Una volta abilitata, puoi limitare la creazione di istanze di account creando una policy di controllo del servizio (SCP). Per istruzioni, consulta Controllare la creazione di istanze di account con Services Control Policies.

Controlla la creazione di istanze di account con Services Control Policies

Gli utenti possono creare un'istanza di IAM Identity Center associata a un'unica istanza Account AWS, chiamata account, di IAM Identity Center. Puoi controllare la creazione di istanze di account con Service Control Policies (SCP).

1. Apri la console IAM Identity Center.
2. Nella dashboard, nella sezione Gestione centrale, seleziona il pulsante Previeni le istanze dell'account.
3. Nella finestra di dialogo Allega SCP per impedire la creazione di nuove istanze di account, viene fornito un SCP. Copia l'SCP e scegli il pulsante Vai al pannello di controllo di SCP. Verrai indirizzato alla AWS Organizations console per creare l'SCP o allegarlo come dichiarazione a un SCP esistente.

   Le politiche di controllo del servizio sono una funzionalità di. AWS OrganizationsPer istruzioni su come allegare un SCP, vedere Allegare e scollegare le politiche di controllo del servizio nella Guida per l'utente.AWS Organizations

Anziché impedire la creazione di istanze di account, puoi limitare la creazione di istanze di account a uno specifico Account AWS interno all'organizzazione:

Example : SCP per controllare la creazione dell'istanza

```
{
    "Version": "2012-10-17",
    "Statement" : [
        {
            "Sid": "DenyMemberAccountInstances",
            "Effect": "Deny",
            "Action": "sso:CreateInstance",
            "Resource": "*",
            "Condition": {
                 "StringNotEquals": {
                    "aws:PrincipalAccount": ["<ALLOWED-ACCOUNT-ID>"]
                }
            }
        }
    ]
```

```
}
```

Crea un'istanza di account di IAM Identity Center

Un'istanza organizzativa è il metodo principale e consigliato per abilitare IAM Identity Center. Assicurati che il tuo caso d'uso supporti la creazione di un'istanza di account e di conoscere le considerazioni.

Crea un'istanza di account da un account membro dell'organizzazione o autonoma Account AWS

1. Effettua una delle seguenti operazioni per accedere a. AWS Management Console
   - Nuovo utente AWS (utente root): accedi come proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.
   - Già in uso AWS (credenziali IAM): accedi utilizzando le tue credenziali IAM con autorizzazioni amministrative.
2. Apri la console IAM Identity Center.
3. In Abilita IAM Identity Center, scegli Abilita.
4. Seleziona Continua a creare l'istanza dell'account e scegli Continua.

   > **Note**
   >
   > Se esiste un'istanza organizzativa di IAM Identity Center, assicurati che il tuo use case richieda un'istanza di account propria di IAM Identity Center. In caso contrario, scegli Annulla e utilizza l'istanza dell'organizzazione.

5. Facoltativo. Aggiungi i tag che desideri associare a questa istanza di account.

Una notifica nella console indica che è stata creata un'istanza di account riuscita e include l'ID dell'istanza. Puoi assegnare un nome alla tua istanza nel riepilogo delle impostazioni.

> **Note**
>
> L'autenticazione a più fattori (MFA) è abilitata per impostazione predefinita per le istanze di account. Agli utenti viene richiesto di accedere con MFA quando il dispositivo, il browser o la posizione cambiano. Come best practice in materia di sicurezza, consigliamo vivamente

l'MFA per le identità della tua forza lavoro. Ulteriori informazioni su Gestisci i dispositivi MFA in IAM Identity Center.

Le funzionalità di gestione, come la conferma dell'origine dell'identità, la regolazione delle impostazioni di autenticazione a più fattori e l'aggiunta di applicazioni AWS gestite, devono essere completate nella console IAM Identity Center.

Autenticazione

Un utente AWS accede al portale di accesso utilizzando il proprio nome utente. Quando lo fa, IAM Identity Center reindirizza la richiesta al servizio di autenticazione IAM Identity Center in base alla directory associata all'indirizzo e-mail dell'utente. Una volta autenticati, gli utenti hanno accesso Single Sign-On a tutti AWS gli account e le applicazioni di terze software-as-a-service parti (SaaS) presenti nel portale senza richieste di accesso aggiuntive. Ciò significa che gli utenti non devono più tenere traccia delle credenziali di più account per le varie AWS applicazioni assegnate che utilizzano quotidianamente.

Sessioni di autenticazione

Esistono due tipi di sessioni di autenticazione gestite da IAM Identity Center: una per rappresentare l'accesso degli utenti a IAM Identity Center e un'altra per rappresentare l'accesso degli utenti alle applicazioni AWS gestite, come Amazon SageMaker Studio o Amazon Managed Grafana. Ogni volta che un utente accede a IAM Identity Center, viene creata una sessione di accesso per la durata configurata in IAM Identity Center, che può arrivare fino a 90 giorni. Per ulteriori informazioni, consulta Gestisci la durata della sessione del portale di AWS accesso e delle applicazioni integrate IAM Identity Center. Ogni volta che l'utente accede a un'applicazione, la sessione di accesso di IAM Identity Center viene utilizzata per ottenere una sessione dell'applicazione IAM Identity Center per quell'applicazione. Le sessioni applicative IAM Identity Center hanno una durata aggiornabile di 1 ora, ovvero le sessioni applicative IAM Identity Center vengono aggiornate automaticamente ogni ora, purché la sessione di accesso a IAM Identity Center da cui sono state ottenute sia ancora valida. Quando l'utente utilizza IAM Identity Center per accedere a AWS Management Console o CLI, la sessione di accesso di IAM Identity Center viene utilizzata per ottenere una sessione IAM, come specificato nel set di autorizzazioni IAM Identity Center corrispondente (più specificamente, IAM Identity Center assume un ruolo IAM, gestito da IAM Identity Center, nell'account di destinazione).

Quando disabiliti o elimini un utente in IAM Identity Center, a quell'utente verrà immediatamente impedito di accedere per creare nuove sessioni di accesso a IAM Identity Center. Le sessioni di accesso a IAM Identity Center vengono memorizzate nella cache per un'ora, il che significa che quando disabiliti o elimini un utente mentre ha una sessione di accesso IAM Identity Center attiva, la sessione di accesso a IAM Identity Center esistente continuerà per un massimo di un'ora, a seconda dell'ultimo aggiornamento della sessione di accesso. Durante questo periodo, l'utente può avviare nuove sessioni di applicazione IAM Identity Center e ruoli IAM.

Dopo la scadenza della sessione di accesso di IAM Identity Center, l'utente non può più avviare nuove applicazioni IAM Identity Center o sessioni di ruolo IAM. Tuttavia, le sessioni applicative IAM Identity Center possono anche essere memorizzate nella cache per un massimo di un'ora, in modo che l'utente possa mantenere l'accesso a un'applicazione fino a un'ora dopo la scadenza della sessione di accesso a IAM Identity Center. Tutte le sessioni di ruolo IAM esistenti continueranno in base alla durata configurata nel set di autorizzazioni IAM Identity Center (configurabile dall'amministratore, fino a 12 ore).

La tabella seguente riassume questi comportamenti:

Esperienza utente/comportamento del sistema	Tempo dopo la disabilitazione/eliminazione dell'utente
L'utente non può più accedere a IAM Identity Center; l'utente non può ottenere una nuova sessione di accesso a IAM Identity Center	Nessuna (con effetto immediato)
L'utente non può più avviare nuove sessioni di applicazione o ruolo IAM tramite IAM Identity Center	Fino a 1 ora
L'utente non può più accedere a nessuna applicazione (tutte le sessioni dell'applicazione vengono terminate)	Fino a 2 ore (fino a 1 ora per la scadenza della sessione di accesso a IAM Identity Center, più fino a 1 ora per la scadenza della sessione dell'applicazione IAM Identity Center)
L'utente non può più accedervi Account AWS tramite IAM Identity Center	Fino a 13 ore (fino a 1 ora per la scadenza della sessione di accesso a IAM Identity Center, più fino a 12 ore per la scadenza della sessione di ruolo IAM configurata dall'ammi nistratore in base alle impostazioni di durata della sessione di IAM Identity Center per il set di autorizzazioni)

Per ulteriori informazioni sulle sessioni, consulta Imposta la durata della sessione.

Gestisci le identità della forza lavoro

AWS Identity and Access Management(IAM) ti aiuta a gestire in modo sicuro le identità e l'accesso a AWS servizi e risorse. In quanto servizio IAM, AWS IAM Identity Center puoi creare o connettere le identità della tua forza lavoro in AWS una sola volta e gestire l'accesso centralizzato alle tue molteplici applicazioni. Account AWS

Per i clienti di IAM Identity Center, non vi è alcuna modifica al modo in cui gestiscono centralmente l'accesso a più applicazioniAccount AWS. Per i nuovi clienti di IAM Identity Center, puoi configurare in modo flessibile IAM Identity Center in modo che funzioni insieme o sostituisca la gestione ad Account AWS accesso singolo tramite IAM.

Argomenti

Casi d'uso

Di seguito sono riportati alcuni casi d'uso che mostrano come utilizzare IAM Identity Center per soddisfare diverse esigenze aziendali.

Argomenti

Abilita l'accesso Single Sign-On alle tue AWS applicazioni (ruolo di amministratore dell'applicazione)

Questo caso d'uso fornisce indicazioni se sei un amministratore di applicazioni che gestisce applicazioni AWS applicazioni gestite come Amazon SageMaker o AWS IoT SiteWise devi fornire l'accesso Single Sign-On ai tuoi utenti.

Prima di iniziare, considera quanto segue:

- Vuoi creare un ambiente di test o di produzione in un'organizzazione separata inAWS Organizations?
- IAM Identity Center è già abilitato nella tua organizzazione? Disponi delle autorizzazioni per abilitare IAM Identity Center nell'account di gestione diAWS Organizations?

Consulta le seguenti linee guida per determinare i passaggi successivi in base alle tue esigenze aziendali.

Configura la mia AWS applicazione in modalità standalone Account AWS

Se devi fornire l'accesso Single Sign-On a un'AWSapplicazione e sai che il tuo reparto IT non utilizza ancora IAM Identity Center, potresti aver bisogno di crearne uno standalone Account AWS per iniziare. Per impostazione predefinita, quando ne crei una tuaAccount AWS, disporrai delle autorizzazioni necessarie per creare e gestire la tua organizzazione. AWS Per abilitare IAM Identity Center, devi disporre delle Utente root dell'account AWS autorizzazioni.

IAM Identity Center e AWS Organizations può essere abilitato automaticamente durante la configurazione per alcune AWS applicazioni (ad esempio, Amazon Managed Grafana). Se la tua AWS applicazione non offre la possibilità di abilitare questi servizi, devi configurare AWS Organizations IAM Identity Center prima di poter fornire l'accesso Single Sign-On all'applicazione.

IAM Identity Center non è configurato nella mia organizzazione

Nel tuo ruolo di amministratore dell'applicazione, potresti non essere in grado di abilitare IAM Identity Center, a seconda delle tue autorizzazioni. IAM Identity Center richiede autorizzazioni specifiche nell'account di AWS Organizations gestione. In questo caso, contatta l'amministratore appropriato per abilitare IAM Identity Center nell'account di gestione Organizations.

Se disponi di autorizzazioni sufficienti per abilitare IAM Identity Center, esegui prima questa operazione, quindi procedi con la configurazione dell'applicazione. Per ulteriori informazioni, consulta Inizia con le attività più comuni in IAM Identity Center.

IAM Identity Center è attualmente configurato nella mia organizzazione

In questo scenario, puoi continuare a distribuire l'AWSapplicazione senza intraprendere ulteriori azioni.

> **Note**
>
> Se la tua organizzazione ha abilitato IAM Identity Center nell'account di gestione prima del 25 novembre 2019, devi abilitare anche le applicazioni AWS gestite nell'account di gestione e, facoltativamente, negli account dei membri. Se le abiliti solo nell'account di gestione, puoi abilitarle negli account dei membri in un secondo momento. Per abilitare queste applicazioni, scegli Abilita l'accesso nella pagina Impostazioni della console IAM Identity Center nella sezione delle applicazioni AWS gestite. Per ulteriori informazioni, consulta Configurazione di IAM Identity Center per condividere le informazioni sull'identità .

Abilita l'accesso Single Sign-On alle istanze Windows di Amazon EC2

Puoi abilitare l'accesso Single Sign-on alle tue istanze Windows di Amazon EC2 se sei un amministratore di applicazioni che gestisce gli utenti nella directory Identity Center (la fonte di identità predefinita per IAM Identity Center) o un provider di identità esterno supportato (IdP), e devi fornire l'accesso a IAM Identity Center ai tuoi desktop Windows Amazon EC2 dalla console Fleet Manager. AWS

Con questa configurazione, puoi accedere in modo sicuro alle tue istanze Windows di Amazon EC2 con le credenziali aziendali esistenti. Non è necessario condividere le credenziali di amministratore, accedere alle credenziali più volte o configurare il software client di accesso remoto. Puoi concedere e revocare centralmente l'accesso alle tue istanze Windows di Amazon EC2 su larga scala su più istanze. Account AWS Ad esempio, se rimuovi un dipendente dalla tua fonte di identità integrata IAM Identity Center, perderà automaticamente l'accesso a tutte le AWS risorse, incluse le istanze Windows di Amazon EC2.

Per ulteriori informazioni, consulta Come abilitare un single sign-on sicuro e senza interruzioni per le istanze Windows di Amazon EC2 con IAM Identity Center.

Per una dimostrazione di come configurare IAM Identity Center per abilitare questa funzionalità, consulta Enabling Single Sign-on to Amazon EC2 Windows with IAM Identity Center.

Utenti, gruppi e provisioning

Tieni a mente le seguenti considerazioni quando lavori con utenti e gruppi in IAM Identity Center.

Unicità del nome utente e dell'indirizzo e-mail

Gli utenti in IAM Identity Center devono essere identificabili in modo univoco. IAM Identity Center implementa un nome utente che è l'identificatore principale per i tuoi utenti. Sebbene la maggior parte delle persone imposti il nome utente come uguale all'indirizzo e-mail di un utente, IAM Identity Center e lo standard SAML 2.0 non lo richiedono. Tuttavia, molte applicazioni basate su SAML 2.0 utilizzano un indirizzo e-mail come identificatore univoco per gli utenti. Queste applicazioni ottengono queste informazioni dalle asserzioni inviate da un provider di identità SAML 2.0 durante l'autenticazione. Tali applicazioni dipendono dall'unicità degli indirizzi e-mail di ciascun utente. Per questo motivo, IAM Identity Center consente di specificare qualcosa di diverso da un indirizzo e-mail per l'accesso dell'utente. IAM Identity Center richiede che tutti i nomi utente e gli indirizzi e-mail degli utenti siano diversi da NULL e unici.

Gruppi

I gruppi sono una combinazione logica di utenti definita dall'utente. È possibile creare gruppi e aggiungere utenti ai gruppi. IAM Identity Center non supporta l'aggiunta di un gruppo a un gruppo (gruppi annidati). I gruppi sono utili per assegnare l'accesso a Account AWS e applicazioni. Anziché assegnare ogni utente singolarmente, concedi le autorizzazioni a un gruppo. Successivamente, quando aggiungi o rimuovi utenti da un gruppo, l'utente ottiene o perde dinamicamente l'accesso agli account e alle applicazioni che hai assegnato al gruppo.

Assegnazione di ruoli a utenti e gruppi

Il provisioning è il processo che rende disponibili le informazioni su utenti e gruppi per l'uso da parte di IAM Identity Center e delle applicazioni AWS gestite o delle applicazioni gestite dai clienti. Puoi creare utenti e gruppi direttamente in IAM Identity Center o lavorare con utenti e gruppi che hai in Active Directory o con un provider di identità esterno. Prima di poter utilizzare IAM Identity Center per assegnare le autorizzazioni di accesso a utenti e gruppi in un unico Account AWS ambiente, IAM Identity Center deve conoscere gli utenti e i gruppi. Allo stesso modo, le applicazioni AWS gestite e le applicazioni gestite dai clienti possono funzionare con utenti e gruppi di cui IAM Identity Center è a conoscenza.

Il provisioning in IAM Identity Center varia in base alla fonte di identità utilizzata. Per ulteriori informazioni, consulta Gestisci la tua fonte di identità.

Gestisci la tua fonte di identità

La tua fonte di identità in IAM Identity Center definisce dove vengono gestiti gli utenti e i gruppi. Dopo aver configurato la fonte di identità, puoi cercare utenti o gruppi per concedere loro l'accesso Single Sign-On alle Account AWS applicazioni o a entrambi.

Puoi avere una sola fonte di identità per organizzazione in. AWS Organizations Puoi scegliere una delle seguenti come fonte di identità:

- Directory Identity Center: quando abiliti IAM Identity Center per la prima volta, questa viene configurata automaticamente con una directory Identity Center come fonte di identità predefinita. Qui puoi creare utenti e gruppi e assegnare il loro livello di accesso a te Account AWS e alle tue applicazioni.
- Active Directory: scegli questa opzione se desideri continuare a gestire gli utenti nella tua AWS Managed Microsoft AD directory utilizzando AWS Directory Service o utilizzando la directory gestita autonomamente. Active Directory (AD)
- Provider di identità esterno: scegli questa opzione se desideri gestire gli utenti in un provider di identità esterno (IdP) come Okta o. Microsoft Entra ID

> **Note**
>
> IAM Identity Center non supporta Simple AD basato su Samba4 come fonte di identità.

Argomenti

Considerazioni sulla modifica dell'origine dell'identità

Sebbene sia possibile modificare l'origine dell'identità in qualsiasi momento, si consiglia di considerare in che modo questa modifica potrebbe influire sulla distribuzione corrente.

Se gestisci già utenti e gruppi in un'unica fonte di identità, il passaggio a una fonte di identità diversa potrebbe rimuovere tutte le assegnazioni di utenti e gruppi che hai configurato in IAM Identity Center. In tal caso, tutti gli utenti, incluso l'utente amministrativo in IAM Identity Center, perderanno l'accesso Single Sign-On alle proprie Account AWS applicazioni.

Prima di modificare la fonte di identità per IAM Identity Center, esamina le seguenti considerazioni prima di procedere. Se desideri procedere con la modifica della fonte di identità, consulta Cambia la tua fonte di identità per ulteriori informazioni.

Passaggio da IAM Identity Center a Active Directory

Se gestisci già utenti e gruppi in Active Directory, ti consigliamo di prendere in considerazione la possibilità di collegare la tua directory quando abiliti IAM Identity Center e scegli la tua fonte di identità. Esegui questa operazione prima di creare utenti e gruppi nella directory predefinita di Identity Center e di effettuare qualsiasi assegnazione.

Se gestisci già utenti e gruppi nella directory predefinita di Identity Center, considera quanto segue:

- Assegnazioni rimosse e utenti e gruppi eliminati: se si modifica l'origine dell'identità in Active Directory, gli utenti e i gruppi vengono eliminati dalla directory Identity Center. Questa modifica rimuove anche le assegnazioni. In questo caso, dopo il passaggio ad Active Directory, è necessario sincronizzare gli utenti e i gruppi da Active Directory alla directory Identity Center e quindi riapplicare le relative assegnazioni.

  Se si sceglie di non utilizzare Active Directory, è necessario creare gli utenti e i gruppi nella directory Identity Center e quindi effettuare le assegnazioni.
- Le assegnazioni non vengono eliminate quando le identità vengono eliminate: quando le identità vengono eliminate nella directory Identity Center, le assegnazioni corrispondenti vengono eliminate anche in IAM Identity Center. Tuttavia, in Active Directory, quando le identità vengono eliminate (in Active Directory o nelle identità sincronizzate), le assegnazioni corrispondenti non vengono eliminate.
- Nessuna sincronizzazione in uscita per le API: se utilizzi Active Directory come fonte di identità, ti consigliamo di utilizzare le API di creazione, aggiornamento ed eliminazione con cautela. IAM

Identity Center non supporta la sincronizzazione in uscita, quindi la tua fonte di identità non si aggiorna automaticamente con le modifiche che apporti agli utenti o ai gruppi utilizzando queste API.

- L'URL del portale di accesso cambierà: la modifica della fonte di identità tra IAM Identity Center e Active Directory modifica anche l'URL del portale di accesso. AWS

Per informazioni su come IAM Identity Center fornisce utenti e gruppi, consultaConnect a una Microsoft AD directory.

Passaggio da IAM Identity Center a un IdP esterno

Se cambi la tua fonte di identità da IAM Identity Center a un provider di identità esterno (IdP), considera quanto segue:

- Le assegnazioni e le appartenenze funzionano con le asserzioni corrette: le assegnazioni degli utenti, le assegnazioni ai gruppi e le appartenenze ai gruppi continueranno a funzionare finché il nuovo IdP invierà le asserzioni corrette (ad esempio, SAML NameID). Queste asserzioni devono corrispondere ai nomi utente e ai gruppi in IAM Identity Center.
- Nessuna sincronizzazione in uscita: IAM Identity Center non supporta la sincronizzazione in uscita, quindi il tuo IdP esterno non si aggiornerà automaticamente con le modifiche agli utenti e ai gruppi che apporti in IAM Identity Center.
- Provisioning SCIM: se utilizzi il provisioning SCIM, le modifiche agli utenti e ai gruppi nel tuo provider di identità si riflettono in IAM Identity Center solo dopo che il provider di identità ha inviato tali modifiche a IAM Identity Center. Per informazioni, consulta Considerazioni sull'utilizzo del provisioning automatico.
- Rollback: puoi ripristinare la tua origine di identità all'utilizzo di IAM Identity Center in qualsiasi momento. Per informazioni, consulta Passaggio da un IdP esterno a IAM Identity Center.

Per informazioni su come IAM Identity Center effettua il provisioning di utenti e gruppi, consulta. Connect a un provider di identità esterno

Passaggio da un IdP esterno a IAM Identity Center

Se modifichi la fonte di identità da un provider di identità esterno (IdP) a IAM Identity Center, considera quanto segue:

- IAM Identity Center conserva tutte le tue assegnazioni.

- Reimpostazione forzata della password: gli utenti che avevano password in IAM Identity Center possono continuare ad accedere con le vecchie password. Per gli utenti che si trovavano nell'IdP esterno e non erano in IAM Identity Center, un amministratore deve forzare la reimpostazione della password.

Per informazioni su come IAM Identity Center fornisce utenti e gruppi, consulta. Gestisci le identità in IAM Identity Center

Passaggio da un IdP esterno a un altro IdP esterno

Se utilizzi già un IdP esterno come fonte di identità per IAM Identity Center e passi a un altro IdP esterno, considera quanto segue:

- Le assegnazioni e le iscrizioni funzionano con le asserzioni corrette: IAM Identity Center conserva tutte le tue assegnazioni. Le assegnazioni degli utenti, le assegnazioni ai gruppi e le appartenenze ai gruppi continueranno a funzionare finché il nuovo IdP invierà le asserzioni corrette (ad esempio, SAML NameID).

  Queste asserzioni devono corrispondere ai nomi utente in IAM Identity Center quando gli utenti si autenticano tramite il nuovo IdP esterno.
- Provisioning SCIM: se utilizzi SCIM per il provisioning in IAM Identity Center, ti consigliamo di consultare le informazioni specifiche dell'IdP contenute in questa guida e la documentazione fornita dall'IdP per garantire che il nuovo provider abbini correttamente utenti e gruppi quando SCIM è abilitato.

Per informazioni su come IAM Identity Center fornisce utenti e gruppi, consulta. Connect a un provider di identità esterno

Passaggio da Active Directory a un IdP esterno

Se modifichi l'origine dell'identità da un IdP esterno ad Active Directory o da Active Directory a un IdP esterno, considera quanto segue:

- Utenti, gruppi e assegnazioni vengono eliminati: tutti gli utenti, i gruppi e le assegnazioni vengono eliminati da IAM Identity Center. Nessuna informazione sull'utente o sul gruppo è interessata né nell'IdP esterno né in Active Directory.

- Provisioning degli utenti: se passi a un IdP esterno, devi configurare IAM Identity Center per effettuare il provisioning dei tuoi utenti. In alternativa, è necessario effettuare manualmente il provisioning degli utenti e dei gruppi per l'IdP esterno prima di poter configurare le assegnazioni.
- Creare assegnazioni e gruppi: se si passa ad Active Directory, è necessario creare assegnazioni con gli utenti e i gruppi presenti nella directory in Active Directory.

Per informazioni su come IAM Identity Center fornisce utenti e gruppi, consulta. Connect a una Microsoft AD directory

Cambia la tua fonte di identità

La procedura seguente descrive come passare da una directory fornita da IAM Identity Center (la directory predefinita di Identity Center) ad Active Directory o a un provider di identità esterno, o viceversa. Prima di continuare, consulta le informazioni inConsiderazioni sulla modifica dell'origine dell'identità. A seconda della distribuzione corrente, questa modifica potrebbe rimuovere tutte le assegnazioni di utenti e gruppi configurate in IAM Identity Center. In tal caso, tutti gli utenti, incluso l'utente amministrativo in IAM Identity Center, perderanno l'accesso Single Sign-On ai propriAccount AWSe applicazioni.

Per modificare la fonte dell'identità

1. OpenIAM Identity Center.
2. Selezionare Settings (Impostazioni).
3. SulImpostazionipagina, scegli laOrigine di identitàTabulatore. ScegliOperazioni, quindi selezionareModifica della fonte di identità.
4. SottoScegliere la fonte di identità, selezionare la fonte a cui si desidera passare, quindi selezionareSuccessivo.

   Se stai passando ad Active Directory, scegli la directory disponibile dal menu nella pagina successiva.

   > **Important**
   >
   > La modifica dell'origine dell'identità da o verso Active Directory comporta l'eliminazione di utenti e gruppi dalla directory Identity Center. Questa modifica rimuove anche tutte le assegnazioni configurate in IAM Identity Center.

Se si passa a un provider di identità esterno, si consiglia di seguire le fasi riportate inCome connettersi a un provider di identità esterno.

5. Dopo aver letto il disclaimer e essere pronti per continuare, digitareACCETTARE.
6. ScegliModifica della fonte di identità. Se si sta modificando la fonte di identità in Active Directory, procedere alla fase successiva.
7. La modifica dell'origine dell'identità in Active Directory consente di accedere allImpostazionipagina. SulImpostazioniPagina, procedi in una delle modalità seguenti:

   - ScegliAvvia configurazione guidata. Per informazioni su come completare la procedura di configurazione guidata, consultaConfigurazione guidata.
   - NelOrigine di identitàsezione, scegliOperazioni, quindi selezionareGestione della sincronizzazioneper configurareambito di sincronizzazione, l'elenco degli utenti e dei gruppi da sincronizzare.

Gestisci l'accesso e l'uso degli attributi per tutti i tipi di fonti di identità

IAM Identity Center offre il seguente set di funzionalità che consentono agli amministratori di controllare AWS l'uso del portale di accesso, di impostare la durata delle sessioni per gli utenti nel portale di AWS accesso e nelle applicazioni e di utilizzare gli attributi per il controllo degli accessi. Queste funzionalità funzionano con una directory di Identity Center o un provider di identità esterno come fonte di identità.

> **Note**
>
> Se utilizzi Active Directory come fonte di identità per IAM Identity Center, la gestione delle sessioni non è supportata.

Argomenti

- Gestisci la durata della sessione del portale di AWS accesso e delle applicazioni integrate IAM Identity Center
- Configura la durata della sessione del portale di AWS accesso e delle applicazioni integrate in IAM Identity Center
- Eliminare le sessioni per il portale di AWS accesso e le applicazioni AWS integrate

- Attributi utente e di gruppo supportati

Gestisci la durata della sessione del portale di AWS accesso e delle applicazioni integrate IAM Identity Center

L'amministratore di IAM Identity Center può configurare la durata della sessione per entrambe le applicazioni integrate con IAM Identity Center e il Portale di accesso AWS. La configurazione della durata delle sessioni determina la frequenza con cui gli utenti devono effettuare nuovamente l'autenticazione. L'amministratore di IAM Identity Center può terminare una sessione del portale AWS ad accesso attivo e così facendo anche terminare le sessioni delle applicazioni integrate.

Per ulteriori informazioni, consulta Configura la durata della sessione del portale di AWS accesso e delle applicazioni integrate in IAM Identity Center. Per ulteriori informazioni su come gestire le sessioni degli utenti finali, consultaEliminare le sessioni per il portale di AWS accesso e le applicazioni AWS integrate.

> **Note**
>
> La modifica della durata della sessione del portale di AWS accesso e la fine delle sessioni del portale di AWS accesso non hanno alcun effetto sulla durata della sessione della Console di AWS gestione definita nei set di autorizzazioni.

Configura la durata della sessione del portale di AWS accesso e delle applicazioni integrate in IAM Identity Center

La durata della sessione di autenticazione nelle Portale di accesso AWS applicazioni integrate di IAM Identity Center è il periodo di tempo massimo durante il quale un utente può accedere senza eseguire nuovamente l'autenticazione. La durata predefinita della sessione è di 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. Per ulteriori informazioni sulla durata della sessione di autenticazione e sul comportamento degli utenti, consultaAutenticazione.

I seguenti argomenti forniscono informazioni sulla configurazione della durata della sessione del portale di AWS accesso e delle applicazioni integrate IAM Identity Center.

Argomenti

- Prerequisiti e considerazioni

- Come configurare la durata della sessione

Prerequisiti e considerazioni

Di seguito sono riportati i prerequisiti e le considerazioni per la configurazione della durata della sessione per il portale di AWS accesso e le applicazioni integrate IAM Identity Center.

Provider di identità esterni

IAM Identity Center utilizza gli `SessionNotOnOrAfter` attributi delle asserzioni SAML per determinare per quanto tempo la sessione può essere valida.

- Se non `SessionNotOnOrAfter` viene passato in un'asserzione SAML, la durata di una sessione del portale di AWS accesso non è influenzata dalla durata della sessione IdP esterna. Ad esempio, se la durata della sessione IdP è di 24 ore e imposti una durata della sessione di 18 ore in IAM Identity Center, gli utenti devono autenticarsi nuovamente nel portale di accesso dopo 18 ore. AWS
- Se `SessionNotOnOrAfter` viene passato in un'asserzione SAML, il valore della durata della sessione viene impostato sul valore più breve tra la durata della sessione del portale di AWS accesso e la durata della sessione IdP SAML. Se imposti una durata della sessione di 72 ore in IAM Identity Center e il tuo IdP ha una durata della sessione di 18 ore, i tuoi utenti avranno accesso alle AWS risorse per le 18 ore definite nel tuo IdP.
- Se la durata della sessione del tuo IdP è più lunga di quella impostata in IAM Identity Center, i tuoi utenti saranno in grado di avviare una nuova sessione di IAM Identity Center senza reinserire le proprie credenziali, in base alla sessione di accesso ancora valida con il tuo IdP.

> **Note**
>
> Se utilizzi Active Directory come fonte di identità per IAM Identity Center, la gestione delle sessioni non è supportata.

AWS CLI e sessioni SDK

Se utilizzi i AWS Command Line Interface AWS Software Development Kit (SDK) o altri strumenti di AWS sviluppo per accedere ai AWS servizi in modo programmatico, è necessario soddisfare i seguenti prerequisiti per impostare la durata della sessione per il portale di AWS accesso e le applicazioni integrate IAM Identity Center.

- È necessario configurare la durata della sessione del portale di AWS accesso nella console IAM Identity Center.
- È necessario definire un profilo per le impostazioni Single Sign-On nel file di AWS configurazione condiviso. Questo profilo viene utilizzato per connettersi al portale di accesso. AWS Si consiglia di utilizzare la configurazione del provider di token SSO. Con questa configurazione, l' AWS SDK o lo strumento possono recuperare automaticamente i token di autenticazione aggiornati. Per ulteriori informazioni, consulta la configurazione del provider di token SSO nella Guida di riferimento per AWS SDK e strumenti.
- Gli utenti devono eseguire una versione AWS CLI o un SDK che supporti la gestione delle sessioni.

Versioni minime di AWS CLI che supportano la gestione delle sessioni

Di seguito sono riportate le versioni minime di quelle AWS CLI che supportano la gestione delle sessioni.

- AWS CLI V2 2.9 o versione successiva
- AWS CLI V1 1.27.10 o versione successiva

Per informazioni su come installare o aggiornare la AWS CLI versione più recente, vedere Installazione o aggiornamento della versione più recente di. AWS CLI

Se gli utenti utilizzano il AWS CLI, se aggiorni il set di autorizzazioni appena prima della scadenza della sessione di IAM Identity Center e la durata della sessione è impostata su 20 ore mentre la durata del set di autorizzazioni è impostata su 12 ore, la AWS CLI sessione dura un massimo di 20 ore più 12 ore per un totale di 32 ore. Per ulteriori informazioni sulla CLI di IAM Identity Center, consulta AWS CLI Command Reference.

Versioni minime degli SDK che supportano la gestione delle sessioni di IAM Identity Center

Di seguito sono riportate le versioni minime degli SDK che supportano la gestione delle sessioni di IAM Identity Center.

SDK	Versione minima
Python	1.26.10
PHP	3,245,0

SDK	Versione minima
Ruby	aws-sdk-core 3,167,0
Java V2	AWS SDK per Java v2 (2.18.13)
Vai a V2	SDK completo: release-2022-11-11 e moduli Go specifici: credentials/v1.13.0, config/v1.18.0
È V2	2,1253,0
È V3	v3.210.0
C++	1,9,372
.NET	v3.7.400.0

Come configurare la durata della sessione

Utilizza la seguente procedura per configurare la durata della sessione del portale di AWS accesso e delle applicazioni integrate IAM Identity Center.

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Autenticazione.
4. In Autenticazione, accanto a Impostazioni sessione, scegli Configura. Viene visualizzata una finestra di dialogo Configura le impostazioni della sessione.
5. Nella finestra di dialogo Configura le impostazioni della sessione, scegli la durata massima della sessione in minuti, ore e giorni per gli utenti selezionando la freccia a discesa. Scegli la durata della sessione, quindi scegli Salva. Ritorni alla pagina Impostazioni.

Eliminare le sessioni per il portale di AWS accesso e le applicazioni AWS integrate

Utilizza la seguente procedura per visualizzare ed eliminare le sessioni attive per un utente IAM Identity Center.

Per eliminare una sessione attiva del portale di AWS accesso e delle applicazioni integrate IAM Identity Center

1. Apri la console IAM Identity Center.
2. Scegliere Users (Utenti).
3. Nella pagina Utenti, scegli il nome utente dell'utente di cui desideri gestire le sessioni. Verrai indirizzato a una pagina con le informazioni dell'utente.
4. Nella pagina dell'utente, scegli la scheda Sessioni attive. Il numero tra parentesi accanto a Sessioni attive indica il numero di sessioni attive correnti per questo utente.
5. Seleziona le caselle di controllo accanto alle sessioni che desideri eliminare, quindi scegli Elimina sessione. Viene visualizzata una finestra di dialogo che conferma che stai eliminando le sessioni attive per questo utente. Leggi le informazioni nella finestra di dialogo e, se vuoi continuare, scegli Elimina sessione.
6. Verrai reindirizzato alla pagina dell'utente. Viene visualizzata una barra flash verde per indicare che le sessioni selezionate sono state eliminate con successo.

Per ulteriori informazioni sul comportamento delle sessioni di autenticazione revocate, vedereSessioni di autenticazione.

Attributi utente e di gruppo supportati

Gli attributi sono informazioni che consentono di definire e identificare singoli oggetti di utenti o gruppi, ad esempio `name`e`email`, o`members`. IAM Identity Center supporta gli attributi più comunemente utilizzati indipendentemente dal fatto che vengano inseriti manualmente durante la creazione dell'utente o che vengano forniti automaticamente utilizzando un motore di sincronizzazione come definito nella specifica System for Cross-Domain Identity Management (SCIM). Per ulteriori informazioni su questa specifica, consulta https://tools.ietf.org/html/rfc7642. Per ulteriori informazioni sul provisioning manuale e automatico, vedereProvisioning quando gli utenti provengono da un IdP esterno.

Poiché IAM Identity Center supporta SCIM per i casi d'uso di provisioning automatico, la directory Identity Center supporta tutti gli stessi attributi di utente e gruppo elencati nella specifica SCIM, con alcune eccezioni. Le seguenti sezioni descrivono quali attributi non sono supportati da IAM Identity Center.

Oggetti utente

Tutti gli attributi dello schema utente SCIM (https://tools.ietf.org/html/rfc7643#section-8.3) sono supportati nell'archivio di identità di IAM Identity Center, ad eccezione dei seguenti:

- `password`
- `ims`
- `photos`
- `entitlements`
- `x509Certificates`

Sono supportati tutti gli attributi secondari per gli utenti, ad eccezione dei seguenti:

- `'display'`attributo secondario di qualsiasi attributo multivalore (ad esempio, o) `emails` `phoneNumbers`
- `'version'`attributo secondario dell'attributo `'meta'`

Raggruppa oggetti

Sono supportati tutti gli attributi dello schema di gruppo SCIM (https://tools.ietf.org/html/rfc7643#section-8.4).

Sono supportati tutti gli attributi secondari dei gruppi, ad eccezione dei seguenti:

- `'display'`attributo secondario di qualsiasi attributo multivalore (ad esempio, members).

Gestisci le identità in IAM Identity Center

IAM Identity Center offre le seguenti funzionalità per utenti e gruppi:

- Creazione di utenti e gruppi.
- Aggiungi gli utenti come membri dei gruppi.
- Assegna ai gruppi il livello di accesso desiderato alle tue applicazioni Account AWS e alle tue.

Per gestire utenti e gruppi nello store IAM Identity Center, AWS supporta le operazioni API elencate in Identity Center Actions.

Eseguire il provisioning quando gli utenti si trovano in IAM Identity Center

Quando crei utenti e gruppi direttamente in IAM Identity Center, il provisioning è automatico. Queste identità sono immediatamente disponibili per l'uso nell'esecuzione di assegnazioni e per l'uso da parte delle applicazioni. Per ulteriori informazioni, consulta Assegnazione di ruoli a utenti e gruppi.

Modifica della fonte dell'identità

Se preferisci gestire gli utenti in AWS Managed Microsoft AD, puoi smettere di usare la tua directory Identity Center in qualsiasi momento e connettere invece IAM Identity Center alla tua directory in Microsoft AD utilizzando AWS Directory Service. Per ulteriori informazioni, consulta Considerazioni perPassaggio da IAM Identity Center a Active Directory.

Se preferisci gestire gli utenti in un provider di identità (IdP) esterno, puoi connettere IAM Identity Center al tuo IdP e abilitare il provisioning automatico. Per ulteriori informazioni, consulta Considerazioni per. Passaggio da IAM Identity Center a un IdP esterno

Argomenti

- Aggiungere gli utenti
- Aggiungi gruppi
- Aggiungi utenti ai gruppi
- Elimina i gruppi in IAM Identity Center
- Elimina gli utenti in IAM Identity Center
- Disabilita l'accesso degli utenti in IAM Identity Center
- Modifica le proprietà dell'utente
- Reimposta la password utente di IAM Identity Center per un utente finale
- Invia e-mail OTP per gli utenti creati dall'API
- Requisiti relativi alle password per la gestione delle identità in IAM Identity Center

Aggiungere gli utenti

Gli utenti e i gruppi che crei nella directory di Identity Center sono disponibili solo in IAM Identity Center. Utilizza la seguente procedura per aggiungere utenti alla directory di Identity Center utilizzando la console IAM Identity Center. In alternativa, puoi chiamare l'operazione AWS API CreateUserper aggiungere utenti.

Aggiunta di un utente

1. Apri la console IAM Identity Center.
2. Scegliere Users (Utenti).
3. Scegli Aggiungi utente e fornisci le seguenti informazioni richieste:

   a. Nome utente: questo nome utente è necessario per accedere al portale di AWS accesso e non può essere modificato in seguito. Deve contenere da 1 a 100 caratteri.

   b. Password: puoi inviare un'e-mail con le istruzioni per l'impostazione della password (questa è l'opzione predefinita) o generare una password monouso. Se stai creando un utente amministrativo e scegli di inviare un'e-mail, assicurati di specificare un indirizzo e-mail a cui puoi accedere.

      i. Invia un'e-mail a questo utente con le istruzioni per l'impostazione della password. — Questa opzione invia automaticamente all'utente un'e-mail indirizzata da Amazon Web Services, con l'oggetto Invito a partecipare AWS IAM Identity Center (successore di AWS Single Sign-On). L'e-mail invita l'utente per conto della tua azienda ad accedere al portale di accesso IAM Identity Center AWS .

      > **Note**
      >
      > In alcune regioni, IAM Identity Center invia e-mail agli utenti che utilizzano Amazon Simple Email Service da un'altra Regione AWS. Per informazioni su come vengono inviate le e-mail, consultaChiamate tra regioni.
      > Tutte le e-mail inviate dal servizio IAM Identity Center proverranno dall'indirizzo `no-reply@signin.aws.com` 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.

      ii. Genera una password monouso da condividere con questo utente. — Questa opzione fornisce l'URL del portale di AWS accesso e i dettagli della password che è possibile inviare manualmente all'utente dal proprio indirizzo e-mail.

   c. Indirizzo e-mail: l'indirizzo e-mail deve essere univoco.

   d. Conferma l'indirizzo e-mail

   e. Nome: è necessario inserire un nome qui affinché il provisioning automatico funzioni. Per ulteriori informazioni, consulta Provisioning automatico.

f. Cognome: è necessario inserire un nome in questo campo affinché il provisioning automatico funzioni.

g. Display name (Nome visualizzato)

> **Note**
>
> (Facoltativo) Se applicabile, puoi specificare valori per attributi aggiuntivi come l'ID immutabile Microsoft 365 dell'utente per fornire all'utente l'accesso Single Sign-On a determinate applicazioni aziendali.

4. Seleziona Successivo.
5. Se applicabile, seleziona uno o più gruppi a cui desideri aggiungere l'utente e scegli Avanti.
6. Rivedi le informazioni che hai specificato per il Passaggio 1: Specificare i dettagli dell'utente e il Passaggio 2: Aggiungi utente ai gruppi (facoltativo). Scegli Modifica in entrambi i passaggi per apportare modifiche. Dopo aver confermato che sono state specificate le informazioni corrette per entrambi i passaggi, scegli Aggiungi utente.

Aggiungi gruppi

Utilizza la seguente procedura per aggiungere gruppi alla directory di Identity Center utilizzando la console IAM Identity Center. In alternativa, puoi chiamare l'operazione AWS API CreateGroupper aggiungere gruppi.

Per aggiungere un gruppo

1. Apri la console IAM Identity Center.
2. Scegliere Groups (Gruppi).
3. Seleziona Crea gruppo.
4. Inserisci un nome e una descrizione del gruppo (facoltativo). La descrizione dovrebbe fornire dettagli su quali autorizzazioni sono state o saranno assegnate al gruppo. In Aggiungi utenti al gruppo: facoltativo, individua gli utenti che desideri aggiungere come membri. Selezionare quindi la casella di controllo di ciascuno di essi.
5. Seleziona Crea gruppo.

Dopo aver aggiunto questo gruppo alla directory dell'Identity Center, puoi assegnare l'accesso Single Sign-On a questo gruppo. Per ulteriori informazioni, consulta Assegna l'accesso utente a Account AWS.

Aggiungi utenti ai gruppi

Utilizza la seguente procedura per aggiungere utenti come membri di un gruppo creato in precedenza nella directory di Identity Center utilizzando la console IAM Identity Center. In alternativa, puoi chiamare l'operazione AWS API CreateGroupMembershipper aggiungere un utente come membro di un gruppo.

Per aggiungere un utente come membro di un gruppo

1. Apri la console IAM Identity Center.
2. Scegliere Groups (Gruppi).
3. Scegli il nome del gruppo che desideri aggiornare.
4. Nella pagina dei dettagli del gruppo, in Utenti di questo gruppo, scegli Aggiungi utenti al gruppo.
5. Nella pagina Aggiungi utenti al gruppo, in Altri utenti, individua gli utenti che desideri aggiungere come membri. Quindi, seleziona la casella di controllo accanto a ciascuno di essi.
6. Scegli Aggiungi utenti.

Elimina i gruppi in IAM Identity Center

Quando elimini un gruppo nella tua directory IAM Identity Center, rimuove l'accesso Account AWS e le applicazioni per tutti gli utenti che sono membri di questo gruppo. Una volta eliminato, un gruppo non può essere annullato. Utilizza la seguente procedura per eliminare un gruppo nella directory di Identity Center utilizzando la console IAM Identity Center.

Per eliminare un gruppo in IAM Identity Center

> **Important**
>
> Le istruzioni in questa pagina si applicano a AWS IAM Identity Center. Non si applicano a AWS Identity and Access Management(IAM). Gli utenti, i gruppi e le credenziali utente di IAM Identity Center sono diversi dagli utenti, dai gruppi e dalle credenziali utente IAM. Se stai cercando istruzioni sull'eliminazione di gruppi in IAM, consulta Eliminazione di un gruppo di utenti IAM nella Guida per l'utente.AWS Identity and Access Management

1. Apri la console IAM Identity Center.
2. Scegliere Groups (Gruppi).
3. Esistono due modi per eliminare un gruppo:
   - Nella pagina Gruppi, puoi selezionare più gruppi da eliminare. Seleziona il nome del gruppo che desideri eliminare e scegli Elimina gruppo.
   - Scegli il nome del gruppo che desideri eliminare. Nella pagina dei dettagli del gruppo, scegli Elimina gruppo.
4. È possibile che ti venga chiesto di confermare l'intenzione di eliminare il gruppo.
   - Se elimini più gruppi contemporaneamente, conferma l'intenzione digitando **`Delete`** nella finestra di dialogo Elimina gruppo.
   - Se eliminate un singolo gruppo che contiene utenti, confermate l'intenzione digitando il nome del gruppo da eliminare nella finestra di dialogo Elimina gruppo.
5. Scegliere Delete group (Elimina gruppo). Se avete selezionato più gruppi da eliminare, scegliete Elimina # gruppi.

Elimina gli utenti in IAM Identity Center

Quando elimini un utente nella tua directory IAM Identity Center, rimuove il suo accesso Account AWS e le sue applicazioni. Una volta eliminato, un utente non può essere annullato. Utilizza la seguente procedura per eliminare un utente nella directory di Identity Center utilizzando la console IAM Identity Center.

> **Note**
>
> Quando disabiliti l'accesso utente o elimini un utente in IAM Identity Center, a quell'utente verrà immediatamente impedito di AWS accedere al portale di accesso e non sarà in grado di creare nuove sessioni di accesso. Per ulteriori informazioni, consulta Sessioni di autenticazione.

Per eliminare un utente in IAM Identity Center

> **Important**
>
> Le istruzioni in questa pagina si applicano a AWS IAM Identity Center. Non si applicano a AWS Identity and Access Management(IAM). Gli utenti, i gruppi e le credenziali utente di IAM Identity Center sono diversi dagli utenti, dai gruppi e dalle credenziali utente IAM. Se stai cercando istruzioni sull'eliminazione degli utenti in IAM, consulta Eliminazione di un utente IAM nella Guida per l'utente.AWS Identity and Access Management

1. Apri la console IAM Identity Center.
2. Scegliere Users (Utenti).
3. Esistono due modi per eliminare un utente:
   - Nella pagina Utenti, puoi selezionare più utenti da eliminare. Seleziona il nome utente che desideri eliminare e scegli Elimina utenti.
   - Scegli il nome utente che desideri eliminare. Nella pagina dei dettagli dell'utente, scegli Elimina utente.
4. Se elimini più utenti contemporaneamente, conferma l'intenzione digitando **`Delete`** nella finestra di dialogo Elimina utente.
5. Scegli Elimina utente. Se hai selezionato più utenti per l'eliminazione, scegli Elimina # utenti.

Disabilita l'accesso degli utenti in IAM Identity Center

Quando disabiliti l'accesso degli utenti nella tua directory IAM Identity Center, non puoi modificare i dettagli utente, reimpostare la password, aggiungere l'utente a un gruppo o visualizzarne l'appartenenza al gruppo. Utilizza la seguente procedura per disabilitare l'accesso degli utenti nella directory di Identity Center utilizzando la console IAM Identity Center.

> **Note**
>
> Quando disabiliti l'accesso utente o elimini un utente in IAM Identity Center, a quell'utente verrà immediatamente impedito di AWS accedere al portale di accesso e non sarà in grado di creare nuove sessioni di accesso. Per ulteriori informazioni, consulta Sessioni di autenticazione.

Per disabilitare l'accesso degli utenti in IAM Identity Center

1. Apri la console IAM Identity Center.

   > **Important**
   >
   > Le istruzioni riportate in questa pagina si applicano a AWS IAM Identity Center. Non si applicano a AWS Identity and Access Management(IAM). Gli utenti, i gruppi e le credenziali utente di IAM Identity Center sono diversi dagli utenti, dai gruppi e dalle credenziali utente IAM. Se stai cercando istruzioni sulla disattivazione degli utenti in IAM, consulta Managing IAM users nella User Guide.AWS Identity and Access Management

2. Scegliere Users (Utenti).
3. Seleziona il nome utente dell'utente di cui desideri disabilitare l'accesso.
4. Sotto il nome utente dell'utente di cui desideri disabilitare l'accesso, nella sezione Informazioni generali, scegli Disabilita l'accesso utente.
5. Nella finestra di dialogo Disabilita l'accesso utente, scegli Disabilita l'accesso utente.

Modifica le proprietà dell'utente

Utilizza la seguente procedura per modificare le proprietà di un utente nella directory di Identity Center utilizzando la console IAM Identity Center. In alternativa, puoi chiamare l'operazione AWS API UpdateUserper aggiornare le proprietà dell'utente.

Per modificare le proprietà degli utenti in IAM Identity Center

1. Apri la console IAM Identity Center.
2. Scegliere Users (Utenti).
3. Scegli l'utente che desideri modificare.
4. Nella pagina del profilo utente, accanto a Dettagli del profilo, scegli Modifica.
5. Nella pagina Modifica dettagli del profilo, aggiorna le proprietà in base alle esigenze. Quindi, scegli Save changes (Salva modifiche).

> **Note**
>
> (Facoltativo) Puoi modificare attributi aggiuntivi come il numero del dipendente e l'ID immutabile di Office 365 per aiutare a mappare l'identità dell'utente in IAM Identity Center con determinate applicazioni aziendali che gli utenti devono utilizzare.

> **Note**
>
> L'attributo Email address è un campo modificabile e il valore fornito deve essere univoco.

Reimposta la password utente di IAM Identity Center per un utente finale

Questa procedura è destinata agli amministratori che devono reimpostare la password di un utente nella directory di IAM Identity Center. Utilizzerai la console IAM Identity Center per reimpostare le password.

Considerazioni per i provider di identità e i tipi di utenti

- MicrosoftActive Directory o provider esterno: se stai connettendo IAM Identity Center ad Microsoft Active Directory o a un provider esterno, la reimpostazione della password utente deve essere eseguita dall'interno di Active Directory o dal provider esterno. Ciò significa che le password di tali utenti non possono essere reimpostate dalla console IAM Identity Center.
- Utenti nella directory IAM Identity Center: se sei un utente IAM Identity Center, puoi reimpostare la tua password di IAM Identity Center, vediReimpostazione della password utente di IAM Identity Center.

Per reimpostare una password per un utente finale di IAM Identity Center

> **Important**
>
> Le istruzioni in questa pagina si applicano a AWS IAM Identity Center. Non si applicano a AWS Identity and Access Management(IAM). Gli utenti, i gruppi e le credenziali utente di IAM Identity Center sono diversi dagli utenti, dai gruppi e dalle credenziali utente IAM. Se stai

cercando istruzioni su come modificare le password per gli utenti IAM, consulta Gestire le password per gli utenti IAM nella Guida per l'utente.AWS Identity and Access Management

1. Apri la console IAM Identity Center.
2. Scegliere Users (Utenti).
3. Seleziona il nome utente dell'utente di cui desideri reimpostare la password.
4. Nella pagina dei dettagli dell'utente, scegli Reimposta password.
5. Nella finestra di dialogo Reimposta password, seleziona una delle seguenti opzioni, quindi scegli Reimposta password:

   a. Invia un'e-mail all'utente con le istruzioni per reimpostare la password: questa opzione invia automaticamente all'utente un'e-mail indirizzata da Amazon Web Services che lo guida su come reimpostare la password.

      > **Warning**
      >
      > Come best practice di sicurezza, verifica che l'indirizzo e-mail di questo utente sia corretto prima di selezionare questa opzione. Se questa e-mail di reimpostazione della password dovesse essere inviata a un indirizzo e-mail errato o configurato in modo errato, un destinatario malintenzionato potrebbe utilizzarla per ottenere l'accesso non autorizzato al tuo AWS ambiente.

   b. Genera una password monouso e condividi la password con l'utente: questa opzione fornisce i dettagli della password che puoi inviare manualmente all'utente dal tuo indirizzo e-mail.

Invia e-mail OTP per gli utenti creati dall'API

Quando crei utenti con l'operazione CreateUserAPI, questi non dispongono di password. Puoi modificare questa impostazione scegliendo di inviare agli utenti una password monouso (OTP) via e-mail quando vengono creati con l'API. Gli utenti ricevono l'e-mail OTP al primo tentativo di accesso. Dopo aver ricevuto l'e-mail OTP, quando un utente accede, deve impostare una nuova password. Se non abiliti questa impostazione, devi generare e condividere OTP con gli utenti che crei utilizzando l'CreateUserAPI.

Per inviare e-mail OTP agli utenti creati con l'API CreateUser

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Autenticazione.
4. Nella sezione Autenticazione standard, scegli Configura.
5. Viene visualizzata una finestra di dialogo. Seleziona la casella accanto a Invia email OTP. Quindi, scegliere Save (Salva). Lo stato viene aggiornato da Disabilitato a Attivato.

Requisiti relativi alle password per la gestione delle identità in IAM Identity Center

> **Note**
>
> Questi requisiti si applicano solo agli utenti creati nella directory Identity Center. Se hai configurato una fonte di identità diversa da IAM Identity Center per l'autenticazione, ad Active Directoryesempio un provider di identità esterno, le politiche relative alle password per gli utenti vengono definite e applicate in tali sistemi, non in IAM Identity Center. Se la tua fonte di identità è AWS Managed Microsoft AD, consulta Gestire le politiche delle password AWS Managed Microsoft AD per ulteriori informazioni.

Quando utilizzi IAM Identity Center come fonte di identità, gli utenti devono rispettare i seguenti requisiti in materia di password per impostare o modificare la propria 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 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- 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.

Connect a una Microsoft AD directory

Con AWS IAM Identity Center, è possibile connettere una directory autogestita in Active Directory (AD) o una directory in AWS Managed Microsoft AD utilizzando. AWS Directory ServiceQuesta directory Microsoft AD definisce il pool di identità da cui gli amministratori possono attingere quando utilizzano la console IAM Identity Center per assegnare l'accesso Single Sign-On. Dopo aver collegato la directory aziendale a IAM Identity Center, puoi quindi concedere agli utenti o ai gruppi di AD l'accesso alle applicazioni o a entrambe Account AWS.

AWS Directory Service ti aiuta a configurare ed eseguire una AWS Managed Microsoft AD directory autonoma ospitata nel AWS cloud. Puoi anche usarla AWS Directory Service per connettere AWS le tue risorse a un AD esistente autogestito. AWS Directory Service Per configurarlo in modo da funzionare con il tuo AD autogestito, devi prima impostare relazioni di fiducia per estendere l'autenticazione al cloud.

IAM Identity Center utilizza la connessione fornita da AWS Directory Service per eseguire l'autenticazione pass-through all'istanza AD di origine. Se lo utilizzi AWS Managed Microsoft AD come fonte di identità, IAM Identity Center può funzionare con utenti provenienti da AWS Managed Microsoft AD o provenienti da qualsiasi dominio connesso tramite un trust AD. Se desideri localizzare gli utenti in quattro o più domini, gli utenti devono utilizzare la `DOMAIN\user` sintassi come nome utente quando effettuano gli accessi a IAM Identity Center.

> **Note**
>
> - Come passaggio preliminare, assicurati che l'AD Connector o la directory in AWS Managed Microsoft AD in si trovino all'interno del AWS Directory Service tuo account di AWS Organizations gestione. Per ulteriori informazioni, consulta Conferma le tue fonti di identità in IAM Identity Center.
> - IAM Identity Center non supporta Simple AD basato su SAMBA 4 come directory connessa.

Considerazioni sull'utilizzo di Active Directory

Se si desidera utilizzare Active Directory come origine dell'identità, la configurazione deve soddisfare i seguenti prerequisiti:

- Se lo utilizzi AWS Managed Microsoft AD, devi abilitare IAM Identity Center nello stesso Regione AWS luogo in cui è configurata la tua AWS Managed Microsoft AD directory. IAM Identity Center archivia i dati di assegnazione nella stessa regione della directory. Per amministrare IAM Identity Center, potrebbe essere necessario passare alla regione in cui è configurato IAM Identity Center. Inoltre, tieni presente che il portale di AWS accesso utilizza lo stesso URL di accesso della tua directory.
- Usa un Active Directory che risiede nell'account di gestione:

  Devi avere un AD Connector o una AWS Managed Microsoft AD directory esistente configurata in AWS Directory Servicee deve risiedere nel tuo account di AWS Organizations gestione. È possibile connettere solo una directory AD Connector o una directory AWS Managed Microsoft AD alla volta. Se devi supportare più domini o foreste, usa AWS Managed Microsoft AD. Per ulteriori informazioni, consultare:

  - Connect una directory AWS Managed Microsoft AD a IAM Identity Center
  - Connect una directory autogestita in Active Directory a IAM Identity Center
- Utilizza un Active Directory che risiede nell'account amministratore delegato:

  Se prevedi di abilitare l'amministratore delegato di IAM Identity Center e utilizzare Active Directory come fonte di identità IAM Identity Center, puoi utilizzare un AD Connector o una AWS Managed Microsoft AD directory esistente configurata in AWS Directory che risiede nell'account amministratore delegato.

  Se decidi di cambiare l'origine dell'identità di IAM Identity Center da qualsiasi altra fonte ad Active Directory o di cambiarla da Active Directory a qualsiasi altra fonte, la directory deve risiedere nell'account membro amministratore delegato di IAM Identity Center, se esistente; in caso contrario, deve essere nell'account di gestione.

Connect Active Directory e specifica un utente

Se utilizzi già Active Directory, i seguenti argomenti ti aiuteranno a prepararti a connettere la tua directory a IAM Identity Center.

Puoi connettere una AWS Managed Microsoft AD directory o una directory autogestita in Active Directory con IAM Identity Center. Se prevedi di connettere una AWS Managed Microsoft AD directory o una directory autogestita in Active Directory, assicurati che la configurazione di Active Directory soddisfi i prerequisiti di. Conferma le tue fonti di identità in IAM Identity Center

> **Note**
>
> Come best practice di sicurezza, consigliamo vivamente di abilitare l'autenticazione a più fattori. Se prevedi di connettere una AWS Managed Microsoft AD directory o una directory autogestita in Active Directory e non utilizzi RADIUS MFA AWS Directory Servicecon, abilita l'MFA in IAM Identity Center.

AWS Managed Microsoft AD

1. Consulta la guida in. Connect a una Microsoft AD directory
2. Seguire la procedura riportata in Connect una directory AWS Managed Microsoft AD a IAM Identity Center.
3. Configura Active Directory per sincronizzare l'utente a cui desideri concedere le autorizzazioni amministrative in IAM Identity Center. Per ulteriori informazioni, consulta Sincronizza un utente amministrativo in IAM Identity Center.

Directory gestita automaticamente in Active Directory

1. Consulta le linee guida contenute inConnect a una Microsoft AD directory.
2. Seguire la procedura riportata in Connect una directory autogestita in Active Directory a IAM Identity Center.
3. Configura Active Directory per sincronizzare l'utente a cui desideri concedere le autorizzazioni amministrative in IAM Identity Center. Per ulteriori informazioni, consulta Sincronizza un utente amministrativo in IAM Identity Center.

IdP esterno

1. Consulta la guida inConnect a un provider di identità esterno.
2. Seguire la procedura riportata in Come connettersi a un provider di identità esterno.
3. Configura il tuo IdP per fornire agli utenti IAM Identity Center.

> **Note**
>
> Prima di configurare il provisioning automatico e basato su gruppi di tutte le identità della tua forza lavoro dal tuo IdP a IAM Identity Center, ti consigliamo di sincronizzare l'unico utente a cui desideri concedere le autorizzazioni amministrative in IAM Identity Center.

Sincronizza un utente amministrativo in IAM Identity Center

Dopo aver collegato la directory a IAM Identity Center, puoi specificare un utente a cui concedere le autorizzazioni amministrative e quindi sincronizzare quell'utente dalla tua directory a IAM Identity Center.

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, scegli Azioni, quindi scegli Gestisci sincronizzazione.
4. Nella pagina Gestisci sincronizzazione, scegli la scheda Utenti, quindi scegli Aggiungi utenti e gruppi.
5. Nella scheda Utenti, in Utente, inserisci il nome utente esatto e scegli Aggiungi.
6. In Utenti e gruppi aggiunti, procedi come segue:
   a. Conferma che l'utente a cui desideri concedere le autorizzazioni amministrative sia specificato.
   b. Seleziona la casella di controllo a sinistra del nome utente.
   c. Seleziona Invia.
7. Nella pagina Gestisci sincronizzazione, l'utente specificato viene visualizzato nell'elenco degli ambiti Utenti sincronizzati.
8. Nel pannello di navigazione, seleziona Utenti.
9. Nella pagina Utenti, potrebbe essere necessario del tempo prima che l'utente specificato compaia nell'elenco. Scegli l'icona di aggiornamento per aggiornare l'elenco degli utenti.

A questo punto, l'utente non ha accesso all'account di gestione. Configurerai l'accesso amministrativo a questo account creando un set di autorizzazioni amministrative e assegnando l'utente a tale set di autorizzazioni. Per ulteriori informazioni, consulta Crea un set di autorizzazioni..

Eseguire il provisioning quando gli utenti provengono da Active Directory

IAM Identity Center utilizza la connessione fornita da AWS Directory Service per sincronizzare le informazioni su utenti, gruppi e appartenenze dalla directory di origine in Active Directory all'archivio di identità di IAM Identity Center. Nessuna informazione sulla password viene sincronizzata con IAM Identity Center, poiché l'autenticazione dell'utente avviene direttamente dalla directory di origine in Active Directory. Questi dati di identità vengono utilizzati dalle applicazioni per facilitare gli scenari di ricerca, autorizzazione e collaborazione in-app senza trasferire l'attività LDAP alla directory di origine in Active Directory.

Per ulteriori informazioni sul provisioning, vedere. Assegnazione di ruoli a utenti e gruppi

Argomenti

- Connect una directory AWS Managed Microsoft AD a IAM Identity Center
- Connect una directory autogestita in Active Directory a IAM Identity Center
- AWS Managed Microsoft AD Mappature degli attributi per le directory
- Effettua il provisioning di utenti e gruppi da Active Directory

Connect una directory AWS Managed Microsoft AD a IAM Identity Center

Utilizza la seguente procedura per connettere una directory AWS Managed Microsoft AD gestita da AWS Directory Service a IAM Identity Center.

Per connettersi AWS Managed Microsoft AD a IAM Identity Center

1. Apri la console IAM Identity Center.

   > **Note**
   >
   > Assicurati che la console IAM Identity Center utilizzi una delle regioni in cui si trova la tua AWS Managed Microsoft AD directory prima di passare alla fase successiva.

2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, quindi scegli Azioni > Modifica l'origine dell'identità.
4. In Scegli l'origine dell'identità, seleziona Active Directory, quindi scegli Avanti.

5. In Connect active directory, scegli una directory AWS Managed Microsoft AD dall'elenco, quindi scegli Avanti.
6. In Conferma modifica, rivedi le informazioni e, quando sei pronto, digita ACCETTA, quindi scegli Cambia origine identità.

> **Important**
>
> Per specificare un utente in Active Directory come utente amministrativo in IAM Identity Center, devi prima sincronizzare l'utente a cui desideri concedere le autorizzazioni amministrative da Active Directory in IAM Identity Center. A tale scopo, segui la procedura in Sincronizza un utente amministrativo in IAM Identity Center.

Connect una directory autogestita in Active Directory a IAM Identity Center

Gli utenti della directory autogestita in Active Directory (AD) possono inoltre disporre dell'accesso Single Sign-On alle applicazioni Account AWS e al portale di accesso. AWS Per configurare l'accesso Single Sign-on per questi utenti, puoi effettuare una delle seguenti operazioni:

- Crea una relazione di trust bidirezionale: quando vengono create relazioni di trust bidirezionale tra AWS Managed Microsoft AD e una directory autogestita in AD, gli utenti della directory autogestita in AD possono accedere con le proprie credenziali aziendali a vari servizi e applicazioni aziendali. AWS I trust unidirezionali non funzionano con IAM Identity Center.

  AWS IAM Identity Center richiede un trust bidirezionale in modo da disporre delle autorizzazioni per leggere le informazioni su utenti e gruppi dal dominio per sincronizzare i metadati di utenti e gruppi. IAM Identity Center utilizza questi metadati per assegnare l'accesso a set di autorizzazioni o applicazioni. I metadati di utenti e gruppi vengono utilizzati anche dalle applicazioni per la collaborazione, ad esempio quando condividi una dashboard con un altro utente o gruppo. L'attribuzione di fiducia AWS Directory Service per Microsoft Active Directory al tuo dominio consente a IAM Identity Center di affidare il tuo dominio per l'autenticazione. La fiducia nella direzione opposta concede le AWS autorizzazioni per leggere i metadati di utenti e gruppi.

  Per ulteriori informazioni sulla configurazione di un trust bidirezionale, vedere Quando creare una relazione di trust nella Guida all'amministrazione.AWS Directory Service
- Crea un connettore AD: AD Connector è un gateway di directory in grado di reindirizzare le richieste di directory al tuo AD autogestito senza memorizzare nella cache alcuna informazione

nel cloud. Per ulteriori informazioni, vedere Connect to a Directory nella AWS Directory Service Administration Guide.

> **Note**
>
> Se stai connettendo IAM Identity Center a una directory AD Connector, eventuali future reimpostazioni delle password utente devono essere eseguite dall'interno di AD. Ciò significa che gli utenti non saranno in grado di reimpostare le proprie password dal portale di AWS accesso.
> Se utilizzi AD Connector per connettere il tuo servizio di dominio Active Directory a IAM Identity Center, IAM Identity Center ha accesso solo agli utenti e ai gruppi del singolo dominio a cui si collega AD Connector. Se devi supportare più domini o foreste, usalo AWS Directory Service per Microsoft Active Directory.

> **Note**
>
> IAM Identity Center non funziona con le directory Simple AD basate su Samba4.

AWS Managed Microsoft AD Mappature degli attributi per le directory

Le mappature degli attributi vengono utilizzate per mappare i tipi di attributi esistenti in IAM Identity Center con attributi simili in una directory. AWS Managed Microsoft AD IAM Identity Center recupera gli attributi utente dalla directory Microsoft AD e li mappa agli attributi utente di IAM Identity Center. Queste mappature degli attributi utente di IAM Identity Center vengono utilizzate anche per generare asserzioni SAML 2.0 per le tue applicazioni. Ogni applicazione determina l'elenco degli attributi SAML 2.0 necessari per il single sign-on di successo.

IAM Identity Center precompila automaticamente un set di attributi nella scheda Mappature degli attributi che si trova nella pagina di configurazione dell'applicazione. IAM Identity Center utilizza questi attributi utente per compilare le asserzioni SAML (come attributi SAML) che vengono inviate all'applicazione. Questi attributi utente vengono quindi recuperati dalla directory Microsoft AD. Per ulteriori informazioni, consulta Mappa gli attributi dell'applicazione agli attributi di IAM Identity Center.

IAM Identity Center gestisce anche una serie di attributi nella sezione Mappature degli attributi della pagina di configurazione delle directory. Per ulteriori informazioni, consulta Mappa gli attributi in IAM Identity Center agli attributi nella tua directory AWS Managed Microsoft AD.

Attributi di directory supportati

La tabella seguente elenca tutti gli attributi di AWS Managed Microsoft AD directory supportati e che possono essere mappati agli attributi utente in IAM Identity Center.

Attributi supportati nella directory Microsoft AD
`${dir:email}`
`${dir:displayname}`
`${dir:distinguishedName}`
`${dir:firstname}`
`${dir:guid}`
`${dir:initials}`
`${dir:lastname}`
`${dir:proxyAddresses}`
`${dir:proxyAddresses:smtp}`
`${dir:proxyAddresses:SMTP}`
`${dir:windowsUpn}`

Puoi specificare qualsiasi combinazione di attributi di directory Microsoft AD supportati da mappare a un singolo attributo mutabile in IAM Identity Center. Ad esempio, puoi scegliere l'`subject`attributo sotto l'attributo User nella colonna IAM Identity Center. Quindi mappalo a uno `${dir:displayname}` `${dir:lastname}${dir:firstname }` o a qualsiasi attributo supportato singolo o a qualsiasi combinazione arbitraria di attributi supportati. Per un elenco delle mappature predefinite per gli attributi utente in IAM Identity Center, consulta. Mappature predefinite

> **Warning**
>
> Alcuni attributi di IAM Identity Center non possono essere modificati perché sono immutabili e mappati per impostazione predefinita su specifici attributi di directory Microsoft AD.

Ad esempio, «username» è un attributo obbligatorio in IAM Identity Center. Se mappi «username» a un attributo di directory AD con un valore vuoto, IAM Identity Center considererà il `windowsUpn` valore come valore predefinito per «username». Se desideri modificare la mappatura degli attributi per «username» rispetto alla mappatura attuale, conferma che i flussi di IAM Identity Center con dipendenza da «username» continueranno a funzionare come previsto, prima di apportare la modifica.

Se si utilizzano le azioni ListUserso ListGroupsAPI o i comandi list-userse list-groups AWS CLI per assegnare l'accesso a utenti e gruppi alle Account AWS applicazioni, è necessario specificare il valore per `AttributeValue` come nome di dominio completo. Questo valore deve essere nel seguente formato: user@example.com. Nell'esempio seguente, `AttributeValue` è impostato `sujanedoe@example.com`.

```
aws identitystore list-users --identity-store-id d-12345a678b --filters
 AttributePath=UserName,AttributeValue=janedoe@example.com
```

Attributi IAM Identity Center supportati

La tabella seguente elenca tutti gli attributi di IAM Identity Center supportati e che possono essere mappati agli attributi utente nella AWS Managed Microsoft AD directory. Dopo aver impostato le mappature degli attributi dell'applicazione, puoi utilizzare gli stessi attributi di IAM Identity Center per mappare gli attributi effettivi utilizzati da quell'applicazione.

Attributi supportati in IAM Identity Center
`${user:AD_GUID}`
`${user:email}`
`${user:familyName}`
`${user:givenName}`
`${user:middleName}`
`${user:name}`
`${user:preferredUsername}`

Attributi supportati in IAM Identity Center
`${user:subject}`

Attributi del provider di identità esterno supportati

La tabella seguente elenca tutti gli attributi del provider di identità esterno (IdP) che sono supportati e che possono essere mappati agli attributi che è possibile utilizzare durante la configurazione Attributi per il controllo degli accessi in IAM Identity Center. Quando usi le asserzioni SAML, puoi utilizzare qualsiasi attributo supportato dal tuo IdP.

Attributi supportati nel tuo IdP
`${path:userName}`
`${path:name.familyName}`
`${path:name.givenName}`
`${path:displayName}`
`${path:nickName}`
`${path:emails[primary eq true].value}`
`${path:addresses[type eq "work"].streetAddress}`
`${path:addresses[type eq "work"].locality}`
`${path:addresses[type eq "work"].region}`
`${path:addresses[type eq "work"].postalCode}`
`${path:addresses[type eq "work"].country}`
`${path:addresses[type eq "work"].formatted}`
`${path:phoneNumbers[type eq "work"].value}`
`${path:userType}`

Attributi supportati nel tuo IdP
`${path:title}`
`${path:locale}`
`${path:timezone}`
`${path:enterprise.employeeNumber}`
`${path:enterprise.costCenter}`
`${path:enterprise.organization}`
`${path:enterprise.division}`
`${path:enterprise.department}`
`${path:enterprise.manager.value}`

Mappature predefinite

La tabella seguente elenca le mappature predefinite degli attributi utente in IAM Identity Center con gli attributi utente nella directory. AWS Managed Microsoft AD IAM Identity Center supporta solo l'elenco degli attributi nell'attributo User nella colonna IAM Identity Center.

> **Note**
>
> Se non hai alcuna assegnazione per i tuoi utenti e gruppi in IAM Identity Center quando abiliti la sincronizzazione AD configurabile, vengono utilizzate le mappature predefinite nella tabella seguente. Per informazioni su come personalizzare queste mappature, consulta. Configura le mappature degli attributi per la sincronizzazione

Attributo utente in IAM Identity Center	Esegue la mappatura a questo attributo nella directory Microsoft AD
`AD_GUID`	`${dir:guid}`

Attributo utente in IAM Identity Center	Esegue la mappatura a questo attributo nella directory Microsoft AD
`email` *	`${dir:windowsUpn}`
`familyName`	`${dir:lastname}`
`givenName`	`${dir:firstname}`
`middleName`	`${dir:initials}`
`name`	`${dir:displayname}`
`preferredUsername`	`${dir:displayname}`
`subject`	`${dir:windowsUpn}`

* L'attributo email in IAM Identity Center deve essere univoco all'interno della directory. In caso contrario, il processo di accesso JIT potrebbe fallire.

Puoi modificare le mappature predefinite o aggiungere altri attributi all'asserzione SAML 2.0 in base ai tuoi requisiti. Ad esempio, supponiamo che l'applicazione richieda l'e-mail dell'utente nell'attributo SAML 2.0. `User.Email` Inoltre, si supponga che gli indirizzi e-mail siano memorizzati nell'`windowsUpn`attributo nella directory Microsoft AD. Per ottenere questa mappatura, è necessario apportare modifiche nelle seguenti due posizioni della console IAM Identity Center:

1. Nella pagina Directory, nella sezione Attribute mappings (Mappature attributi), devi mappare l'attributo utente **`email`** all'attributo **`${dir:windowsUpn}`** nella colonna Maps to this attribute in your directory (Esegue la mappatura a questo attributo nella directory)
2. Nella pagina Applicazioni, scegli l'applicazione dalla tabella. Scegli la scheda Mappature degli attributi. Quindi mappa l'`User.Email`attributo all'**`${user:email}`**attributo (nella colonna Maps to this string value o user attribute in IAM Identity Center).

Nota che devi fornire ogni attributo di directory nel formato $ {dir:**`AttributeName`**}. Ad esempio, l'attributo `firstname` nella directory Microsoft AD diventa `${dir:firstname}`. È importante che a ogni attributo di directory venga assegnato un valore effettivo. La mancanza negli attributi di un valore dopo `${dir:` causerà problemi di accesso all'utente.

Mappa gli attributi in IAM Identity Center agli attributi nella tua directory AWS Managed Microsoft AD

È possibile utilizzare la seguente procedura per specificare in che modo gli attributi utente in IAM Identity Center devono mappare agli attributi corrispondenti nella directory Microsoft AD.

Per mappare gli attributi in IAM Identity Center agli attributi nella tua directory

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Attributi per il controllo degli accessi, quindi scegli Gestisci attributi.
4. Nella pagina Gestisci l'attributo per il controllo degli accessi, trova l'attributo in IAM Identity Center che desideri mappare, quindi digita un valore nella casella di testo. Ad esempio, potresti voler mappare l'attributo utente di IAM Identity Center **`email`**all'attributo di directory Microsoft AD **`${dir:windowsUpn}`**.
5. Seleziona Salvataggio delle modifiche.

Effettua il provisioning di utenti e gruppi da Active Directory

IAM Identity Center offre i seguenti due modi per effettuare il provisioning di utenti e gruppi da Active Directory.

- Sincronizzazione configurabile con Active Directory (AD) con IAM Identity Center (consigliata): con questo metodo di sincronizzazione, puoi effettuare le seguenti operazioni:
  - Controlla i limiti dei dati definendo in modo esplicito gli utenti e i gruppi in Microsoft Active Directory che vengono sincronizzati automaticamente in IAM Identity Center. Puoi aggiungere utenti e gruppi o rimuovere utenti e gruppi per modificare l'ambito della sincronizzazione in qualsiasi momento.
  - Assegna a utenti e gruppi sincronizzati l'accesso Single Sign-On alle applicazioni Account AWSo l'accesso alle applicazioni. Le applicazioni possono essere applicazioni gestite o applicazioni AWS gestite dal cliente.
  - Controlla il processo di sincronizzazione mettendo in pausa e riprendendo la sincronizzazione secondo necessità. Questo ti aiuta a regolare il carico sui sistemi di produzione.
- Sincronizzazione con IAM Identity Center AD: con questo metodo di sincronizzazione, utilizzi IAM Identity Center per assegnare a utenti e gruppi in Active Directory l'accesso agli AWS account e

alle applicazioni. Tutte le identità con assegnazioni vengono sincronizzate automaticamente in IAM Identity Center.

Sincronizzazione AD configurabile con IAM Identity Center

La sincronizzazione con Active Directory (AD) configurabile con IAM Identity Center consente di configurare in modo esplicito le identità in Microsoft Active Directory che vengono sincronizzate automaticamente in IAM Identity Center e di controllare il processo di sincronizzazione.

I seguenti argomenti forniscono informazioni per consentire all'utente di configurare e amministrare la sincronizzazione AD configurabile.

Argomenti

Prerequisiti e considerazioni

Prima di utilizzare la sincronizzazione AD configurabile, tieni presente i seguenti prerequisiti e considerazioni:

- Specificare utenti e gruppi in Active Directory da sincronizzare

  Prima di poter utilizzare IAM Identity Center per assegnare a nuovi utenti e gruppi l'accesso alle Account AWS applicazioni gestite o alle applicazioni AWS gestite dai clienti, è necessario specificare gli utenti e i gruppi in Active Directory da sincronizzare e quindi sincronizzarli in IAM Identity Center.

  - Sincronizzazione AD: quando si effettuano assegnazioni per nuovi utenti e gruppi utilizzando la console IAM Identity Center o le relative azioni API di assegnazione, IAM Identity Center cerca direttamente nel controller di dominio gli utenti o i gruppi specificati, completa l'assegnazione e quindi sincronizza periodicamente i metadati dell'utente o del gruppo in IAM Identity Center.
  - Sincronizzazione AD configurabile: IAM Identity Center non cerca direttamente utenti e gruppi nel controller di dominio. Invece, devi prima specificare l'elenco di utenti e gruppi da sincronizzare. Puoi configurare questo elenco, noto anche come ambito di sincronizzazione, in uno dei seguenti modi, a seconda che tu abbia utenti e gruppi già sincronizzati in IAM Identity Center o che tu

abbia nuovi utenti e gruppi che sincronizzi per la prima volta utilizzando la sincronizzazione AD configurabile.

- Utenti e gruppi esistenti: se hai utenti e gruppi già sincronizzati in IAM Identity Center, l'ambito di sincronizzazione nella sincronizzazione AD configurabile è precompilato con un elenco di tali utenti e gruppi. Per assegnare nuovi utenti o gruppi, devi aggiungerli specificamente all'ambito di sincronizzazione. Per ulteriori informazioni, consulta Aggiungi utenti e gruppi all'ambito di sincronizzazione.
- Nuovi utenti e gruppi: se desideri assegnare a nuovi utenti e gruppi l'accesso alle Account AWS e alle applicazioni, devi specificare quali utenti e gruppi aggiungere all'ambito di sincronizzazione nella sincronizzazione configurabile di AD prima di poter utilizzare IAM Identity Center per effettuare l'assegnazione. Per ulteriori informazioni, consulta Aggiungi utenti e gruppi all'ambito di sincronizzazione.

- Assegnazione di assegnazioni a gruppi annidati in Active Directory

  I gruppi che sono membri di altri gruppi sono chiamati gruppi nidificati (o gruppi secondari). Quando si eseguono assegnazioni a un gruppo in Active Directory che contiene gruppi nidificati, il modo in cui vengono applicate le assegnazioni dipende dal fatto che si utilizzi la sincronizzazione AD o la sincronizzazione AD configurabile.

  - Sincronizzazione AD: quando si effettuano assegnazioni a un gruppo in Active Directory che contiene gruppi nidificati, solo i membri diretti del gruppo possono accedere all'account. Ad esempio, se si assegna l'accesso al gruppo A e il gruppo B è membro del gruppo A, solo i membri diretti del gruppo A possono accedere all'account. Nessun membro del Gruppo B eredita l'accesso.
  - Sincronizzazione AD configurabile: l'utilizzo della sincronizzazione AD configurabile per assegnare assegnazioni a un gruppo in Active Directory che contiene gruppi annidati può aumentare il numero di utenti che hanno accesso alle o alle applicazioni. Account AWS In questo caso, l'assegnazione si applica a tutti gli utenti, inclusi quelli dei gruppi nidificati. Ad esempio, se si assegna l'accesso al Gruppo A e il Gruppo B è membro del Gruppo A, anche i membri del Gruppo B ereditano questo accesso.
- Aggiornamento dei flussi di lavoro automatizzati

  Se disponi di flussi di lavoro automatizzati che utilizzano le azioni API IAM Identity Store e le azioni API di assegnazione di IAM Identity Center per assegnare a nuovi utenti e gruppi l'accesso agli account e alle applicazioni e per sincronizzarli con IAM Identity Center, devi modificare tali flussi

di lavoro entro il 15 aprile 2022 in modo che funzionino come previsto con la sincronizzazione AD configurabile. La sincronizzazione AD configurabile modifica l'ordine in cui avvengono l'assegnazione e il provisioning di utenti e gruppi e il modo in cui vengono eseguite le query.

- Sincronizzazione AD: il processo di assegnazione viene eseguito per primo. Assegnate a utenti e gruppi l'accesso alle Account AWS e alle applicazioni. Una volta assegnato l'accesso agli utenti e ai gruppi, questi vengono assegnati automaticamente (sincronizzati con IAM Identity Center). Se disponi di un flusso di lavoro automatizzato, ciò significa che quando aggiungi un nuovo utente ad Active Directory, il flusso di lavoro automatizzato può interrogare Active Directory per l'utente utilizzando l'azione dell'`ListUser`API Identity Store e quindi assegnare l'accesso all'utente utilizzando le azioni dell'API di assegnazione di IAM Identity Center. Poiché l'utente ha un'assegnazione, tale utente viene automaticamente inserito in IAM Identity Center.
- Sincronizzazione AD configurabile: il provisioning avviene per primo e non viene eseguito automaticamente. È invece necessario innanzitutto aggiungere in modo esplicito utenti e gruppi all'archivio di identità aggiungendoli all'ambito di sincronizzazione. Per informazioni sui passaggi consigliati per automatizzare la configurazione di sincronizzazione per la sincronizzazione AD configurabile, consulta. Automatizza la configurazione di sincronizzazione per una sincronizzazione AD configurabile

Come funziona la sincronizzazione AD configurabile

IAM Identity Center aggiorna i dati di identità basati su AD nell'archivio delle identità utilizzando il seguente processo.

Creazione

Dopo aver collegato la directory autogestita in Active Directory o la AWS Managed Microsoft AD directory gestita da AWS Directory Service IAM Identity Center, puoi configurare in modo esplicito gli utenti e i gruppi di Active Directory che desideri sincronizzare nell'archivio di identità di IAM Identity Center. Le identità scelte verranno sincronizzate ogni tre ore circa nell'archivio di identità di IAM Identity Center. A seconda delle dimensioni della directory, il processo di sincronizzazione potrebbe richiedere più tempo.

Anche i gruppi che sono membri di altri gruppi (denominati gruppi annidati o gruppi secondari) vengono scritti nell'archivio di identità. Quando si eseguono assegnazioni a un gruppo in Active Directory che contiene gruppi nidificati, il modo in cui vengono applicate le assegnazioni dipende dal fatto che si utilizzi la sincronizzazione AD o la sincronizzazione AD configurabile. Per ulteriori informazioni, consulta Making assignments to nested groups in Active Directory.

Puoi assegnare l'accesso a nuovi utenti o gruppi solo dopo che sono stati sincronizzati nell'archivio di identità di IAM Identity Center.

Aggiornamento

I dati di identità nell'archivio di identità di IAM Identity Center rimangono aggiornati leggendo periodicamente i dati dalla directory di origine in Active Directory. Per impostazione predefinita, IAM Identity Center sincronizza i dati da Active Directory ogni ora in un ciclo di sincronizzazione. La sincronizzazione dei dati con IAM Identity Center può richiedere da 30 minuti a 2 ore, in base alle dimensioni di Active Directory.

Gli oggetti utente e di gruppo inclusi nell'ambito di sincronizzazione e le relative appartenenze vengono creati o aggiornati in IAM Identity Center per essere mappati agli oggetti corrispondenti nella directory di origine in Active Directory. Per gli attributi utente, solo il sottoinsieme di attributi elencati nella sezione Attributi per il controllo degli accessi della console IAM Identity Center viene aggiornato in IAM Identity Center. Potrebbe essere necessario un ciclo di sincronizzazione affinché tutti gli aggiornamenti degli attributi apportati in Active Directory si riflettano in IAM Identity Center.

Puoi anche aggiornare il sottoinsieme di utenti e gruppi che sincronizzi nell'archivio di identità di IAM Identity Center. Puoi scegliere di aggiungere nuovi utenti o gruppi a questo sottoinsieme o rimuoverli. Tutte le identità aggiunte vengono sincronizzate alla successiva sincronizzazione pianificata. Le identità rimosse dal sottoinsieme smetteranno di essere aggiornate nell'archivio di identità di IAM Identity Center. Qualsiasi utente che non è sincronizzato per più di 28 giorni verrà disabilitato nell'archivio di identità di IAM Identity Center. Gli oggetti utente corrispondenti verranno automaticamente disabilitati nell'archivio di identità di IAM Identity Center durante il ciclo di sincronizzazione successivo, a meno che non facciano parte di un altro gruppo che fa ancora parte dell'ambito di sincronizzazione.

Eliminazione

Gli utenti e i gruppi vengono eliminati dall'archivio di identità di IAM Identity Center quando gli oggetti utente o gruppo corrispondenti vengono eliminati dalla directory di origine in Active Directory. In alternativa, puoi eliminare in modo esplicito gli oggetti utente dall'archivio di identità IAM Identity Center utilizzando la console IAM Identity Center. Se utilizzi la console IAM Identity Center, devi anche rimuovere gli utenti dall'ambito di sincronizzazione per garantire che non vengano risincronizzati con IAM Identity Center durante il ciclo di sincronizzazione successivo.

Puoi anche mettere in pausa e riavviare la sincronizzazione in qualsiasi momento. Se sospendi la sincronizzazione per più di 28 giorni, tutti gli utenti verranno disabilitati.

Configura e gestisci l'ambito di sincronizzazione

Puoi configurare l'ambito di sincronizzazione in uno dei seguenti modi:

- Configurazione guidata: se sincronizzi utenti e gruppi da Active Directory a IAM Identity Center per la prima volta, segui i passaggi indicati Configurazione guidata per configurare l'ambito di sincronizzazione. Dopo aver completato la configurazione guidata, puoi modificare l'ambito di sincronizzazione in qualsiasi momento seguendo le altre procedure in questa sezione.
- Se hai già utenti e gruppi sincronizzati in IAM Identity Center o non desideri seguire la configurazione guidata, scegli Gestisci la sincronizzazione. Ignora la procedura di configurazione guidata e segui le altre procedure in questa sezione, se necessario per configurare e gestire l'ambito di sincronizzazione.

Procedure

- Configurazione guidata
- Aggiungi utenti e gruppi all'ambito di sincronizzazione
- Rimuovi utenti e gruppi dall'ambito di sincronizzazione
- Metti in pausa e riprendi la sincronizzazione
- Configura le mappature degli attributi per la sincronizzazione
- Automatizza la configurazione di sincronizzazione per una sincronizzazione AD configurabile

Configurazione guidata

1. Apri la console IAM Identity Center.

   > **Note**
   >
   > Assicurati che la console IAM Identity Center utilizzi una delle directory Regioni AWS in cui si trova la tua AWS Managed Microsoft AD directory prima di passare alla fase successiva.

2. Seleziona Impostazioni.
3. Nella parte superiore della pagina, nel messaggio di notifica, scegli Avvia configurazione guidata.
4. Nel passaggio 1, facoltativo: configura le mappature degli attributi, esamina le mappature degli attributi di utenti e gruppi predefinite. Se non sono necessarie modifiche, scegli Avanti. Se sono necessarie modifiche, apporta le modifiche e quindi scegli Salva modifiche.

5. Nel passaggio 2, facoltativo: configura l'ambito di sincronizzazione, scegli la scheda Utenti. Quindi, inserisci il nome utente esatto dell'utente che desideri aggiungere all'ambito di sincronizzazione e scegli Aggiungi. Quindi, scegli la scheda Gruppi. Inserisci il nome esatto del gruppo che desideri aggiungere all'ambito di sincronizzazione e scegli Aggiungi. Quindi, seleziona Next (Successivo). Se desideri aggiungere utenti e gruppi all'ambito di sincronizzazione in un secondo momento, non apportare modifiche e scegli Avanti.
6. Nel Passaggio 3: Rivedi e salva la configurazione, conferma le mappature degli attributi nel Passaggio 1: Mappature degli attributi e gli Utenti e i gruppi nel Passaggio 2: Sincronizzazione dell'ambito. Seleziona Save configuration (Salva configurazione). Verrà visualizzata la pagina Gestisci sincronizzazione.

Aggiungi utenti e gruppi all'ambito di sincronizzazione

Come aggiungere utenti

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, scegli Azioni, quindi scegli Gestisci sincronizzazione.
4. Nella pagina Gestisci sincronizzazione, scegli la scheda Utenti, quindi scegli Aggiungi utenti e gruppi.
5. Nella scheda Utenti, in Utente, inserisci il nome utente esatto e scegli Aggiungi.
6. In Utenti e gruppi aggiunti, controlla l'utente che desideri aggiungere.
7. Seleziona Invia.
8. Nel pannello di navigazione, seleziona Utenti.
9. Nella pagina Utenti, potrebbe essere necessario del tempo prima che l'utente specificato compaia nell'elenco. Scegli l'icona di aggiornamento per aggiornare l'elenco degli utenti.

Per aggiungere gruppi

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, scegli Azioni, quindi scegli Gestisci sincronizzazione.

4. Nella pagina Gestisci sincronizzazione, scegli la scheda Gruppi, quindi scegli Aggiungi utenti e gruppi.
5. Scegliere la scheda Groups (Gruppi). In Gruppo, inserisci il nome esatto del gruppo e scegli Aggiungi.
6. In Utenti e gruppi aggiunti, controlla il gruppo che desideri aggiungere.
7. Seleziona Invia.
8. Nel riquadro di navigazione, selezionare Groups (Gruppi).
9. Nella pagina Gruppi, potrebbe essere necessario del tempo prima che il gruppo specificato compaia nell'elenco. Scegli l'icona di aggiornamento per aggiornare l'elenco dei gruppi.

Rimuovi utenti e gruppi dall'ambito di sincronizzazione

Per ulteriori informazioni su cosa succede quando rimuovi utenti e gruppi dall'ambito di sincronizzazione, consultaCome funziona la sincronizzazione AD configurabile.

Per rimuovere utenti

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, scegli Azioni, quindi scegli Gestisci sincronizzazione.
4. Scegli la scheda Users (Utenti);
5. In Utenti nell'ambito di sincronizzazione, seleziona la casella di controllo accanto all'utente che desideri eliminare. Per eliminare tutti gli utenti, seleziona la casella di controllo accanto a Nome utente.
6. Scegli Rimuovi.

Per rimuovere gruppi

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, scegli Azioni, quindi scegli Gestisci sincronizzazione.
4. Scegliere la scheda Groups (Gruppi).

5. In Gruppi nell'ambito di sincronizzazione, seleziona la casella di controllo accanto all'utente che desideri eliminare. Per eliminare tutti i gruppi, seleziona la casella di controllo accanto al nome del gruppo.
6. Scegli Rimuovi.

Metti in pausa e riprendi la sincronizzazione

La sospensione della sincronizzazione sospende tutti i cicli di sincronizzazione futuri e impedisce che le modifiche apportate a utenti e gruppi in Active Directory si riflettano in IAM Identity Center. Dopo aver ripreso la sincronizzazione, il ciclo di sincronizzazione riprende queste modifiche dalla successiva sincronizzazione pianificata.

Per mettere in pausa la sincronizzazione

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, scegli Azioni, quindi scegli Gestisci sincronizzazione.
4. In Gestisci sincronizzazione, scegli Metti in pausa la sincronizzazione.

Per riprendere la sincronizzazione

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, scegli Azioni, quindi scegli Gestisci sincronizzazione.
4. In Gestisci sincronizzazione, scegli Riprendi sincronizzazione.

> **Note**
>
> Se vedi Sospendi la sincronizzazione anziché Riprendi la sincronizzazione, la sincronizzazione da Active Directory a IAM Identity Center è già stata ripresa.

Configura le mappature degli attributi per la sincronizzazione

Per ulteriori informazioni sugli attributi disponibili, vedere. AWS Managed Microsoft AD Mappature degli attributi per le directory

Per configurare le mappature degli attributi in IAM Identity Center nella tua directory

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, scegli Azioni, quindi scegli Gestisci sincronizzazione.
4. In Gestisci sincronizzazione, scegli Visualizza mappatura degli attributi.
5. In Attributi utente di Active Directory, configura gli attributi dell'archivio di identità di IAM Identity Center e gli attributi utente di Active Directory. Ad esempio, potresti voler mappare l'attributo Identity Store di identità di IAM Identity Center `email` all'attributo della directory utente di Active Directory`${objectguid}`.

   > **Note**
   >
   > In Attributi di gruppo, gli attributi dell'archivio di identità di IAM Identity Center e gli attributi del gruppo Active Directory non possono essere modificati.

6. Seleziona Salvataggio delle modifiche. Questo ti riporta alla pagina Manage Sync.

Automatizza la configurazione di sincronizzazione per una sincronizzazione AD configurabile

Per garantire che il flusso di lavoro automatizzato funzioni come previsto con la sincronizzazione AD configurabile, ti consigliamo di eseguire i seguenti passaggi per automatizzare la configurazione di sincronizzazione.

Per automatizzare la configurazione di sincronizzazione per la sincronizzazione AD configurabile

1. In Active Directory, crea un gruppo di sincronizzazione principale che contenga tutti gli utenti e i gruppi che desideri sincronizzare con IAM Identity Center. Ad esempio, puoi denominare il gruppo IAM IdentityCenterAllUsersAndGroups.
2. In IAM Identity Center, aggiungi il gruppo di sincronizzazione principale all'elenco di sincronizzazione configurabile. IAM Identity Center sincronizzerà tutti gli utenti, i gruppi, i sottogruppi e i membri di tutti i gruppi contenuti nel gruppo di sincronizzazione principale.

3. Utilizza le azioni dell'API di gestione di utenti e gruppi di Active Directory fornite da Microsoft per aggiungere o rimuovere utenti e gruppi dal gruppo di sincronizzazione principale.

Sincronizzazione con IAM Identity Center AD

Con la sincronizzazione di IAM Identity Center AD, utilizzi IAM Identity Center per assegnare a utenti e gruppi in Active Directory l'accesso alle Account AWS e alle applicazioni AWS gestite o alle applicazioni gestite dai clienti. Tutte le identità con assegnazioni vengono sincronizzate automaticamente in IAM Identity Center.

Come funziona la sincronizzazione con IAM Identity Center AD

IAM Identity Center aggiorna i dati di identità basati su AD nell'archivio delle identità utilizzando il seguente processo.

Creazione

Quando assegni utenti o gruppi a o applicazioni utilizzando la AWS console Account AWS o le chiamate API di assegnazione, le informazioni sugli utenti, i gruppi e l'appartenenza vengono periodicamente sincronizzate nell'archivio di identità di IAM Identity Center. Gli utenti o i gruppi che vengono aggiunti alle assegnazioni di IAM Identity Center di solito compaiono nell'archivio di AWS identità entro due ore. A seconda della quantità di dati da sincronizzare, questo processo potrebbe richiedere più tempo. Vengono sincronizzati solo gli utenti e i gruppi a cui è assegnato l'accesso diretto o che sono membri di un gruppo a cui è assegnato l'accesso.

I gruppi che sono membri di altri gruppi (denominati gruppi annidati) vengono scritti anche nell'archivio di identità. Quando si eseguono assegnazioni a un gruppo in Active Directory che contiene gruppi nidificati, il modo in cui vengono applicate le assegnazioni dipende dal fatto che si utilizzi la sincronizzazione AD o la sincronizzazione AD configurabile.

- Sincronizzazione AD: quando si effettuano assegnazioni a un gruppo in Active Directory che contiene gruppi nidificati, solo i membri diretti del gruppo possono accedere all'account. Ad esempio, se si assegna l'accesso al gruppo A e il gruppo B è membro del gruppo A, solo i membri diretti del gruppo A possono accedere all'account. Nessun membro del Gruppo B eredita l'accesso.
- Sincronizzazione AD configurabile: l'utilizzo della sincronizzazione AD configurabile per assegnare assegnazioni a un gruppo in Active Directory che contiene gruppi annidati può aumentare il numero di utenti che hanno accesso alle o alle applicazioni. Account AWS In questo caso, l'assegnazione si applica a tutti gli utenti, inclusi quelli dei gruppi nidificati. Ad esempio, se si assegna l'accesso al

Gruppo A e il Gruppo B è membro del Gruppo A, anche i membri del Gruppo B ereditano questo accesso.

Se un utente accede a IAM Identity Center prima che il suo oggetto utente sia stato sincronizzato per la prima volta, l'oggetto dell'archivio di identità dell'utente viene creato su richiesta utilizzando il provisioning just-in-time (JIT). Gli utenti creati dal provisioning JIT non vengono sincronizzati a meno che non abbiano diritti IAM Identity Center assegnati direttamente o basati sul gruppo. Le appartenenze ai gruppi per gli utenti con provisioning JIT non sono disponibili fino a dopo la sincronizzazione.

Per istruzioni su come assegnare agli utenti l'accesso a, vedere. Account AWSAccesso Single Sign-On a Account AWS

Aggiornamento

I dati di identità nell'archivio di identità di IAM Identity Center rimangono aggiornati leggendo periodicamente i dati dalla directory di origine in Active Directory. I dati di identità modificati in Active Directory di solito vengono visualizzati nell'archivio delle AWS identità entro quattro ore. A seconda della quantità di dati da sincronizzare, questo processo potrebbe richiedere più tempo.

Gli oggetti utente e di gruppo e le relative appartenenze vengono creati o aggiornati in IAM Identity Center per essere mappati agli oggetti corrispondenti nella directory di origine in Active Directory. Per gli attributi utente, solo il sottoinsieme di attributi elencati nella sezione Gestisci gli attributi per il controllo degli accessi della console IAM Identity Center viene aggiornato in IAM Identity Center. Inoltre, gli attributi utente vengono aggiornati con ogni evento di autenticazione utente.

Eliminazione

Gli utenti e i gruppi vengono eliminati dall'archivio di identità di IAM Identity Center quando gli oggetti utente o gruppo corrispondenti vengono eliminati dalla directory di origine in Active Directory.

Connect a un provider di identità esterno

Se utilizzi una directory autogestita in Active Directory o una AWS Managed Microsoft AD, consulta. Connect a una Microsoft AD directory Per altri provider di identità esterni (IdPs), puoi utilizzare AWS IAM Identity Center per autenticare le identità IdPs tramite lo standard Security Assertion Markup Language (SAML) 2.0. Ciò consente agli utenti di accedere al portale di AWS accesso con le proprie credenziali aziendali. Possono quindi accedere agli account, ai ruoli e alle applicazioni assegnati ospitati in ambienti esterni IdPs.

Ad esempio, puoi connettere un IdP esterno come Okta oMicrosoft Entra ID, a IAM Identity Center. Gli utenti possono quindi accedere al portale di AWS accesso con le proprie Microsoft Entra ID credenziali Okta o esistenti. Per controllare cosa possono fare gli utenti una volta effettuato l'accesso, è possibile assegnare loro le autorizzazioni di accesso centralmente a tutti gli account e le applicazioni dell'organizzazione. AWS Inoltre, gli sviluppatori possono semplicemente accedere a AWS Command Line Interface (AWS CLI) utilizzando le credenziali esistenti e trarre vantaggio dalla generazione e dalla rotazione automatiche delle credenziali a breve termine.

Il protocollo SAML non fornisce un modo per interrogare l'IdP per ottenere informazioni su utenti e gruppi. Pertanto, è necessario rendere IAM Identity Center consapevole di tali utenti e gruppi inserendoli in IAM Identity Center.

Provisioning quando gli utenti provengono da un IdP esterno

Quando si utilizza un IdP esterno, è necessario effettuare il provisioning di tutti gli utenti e i gruppi applicabili in IAM Identity Center prima di poter effettuare qualsiasi assegnazione o applicazione. Account AWS A tale scopo, puoi configurare o utilizzare Provisioning automatico i tuoi utenti e gruppi. Fornitura manuale Indipendentemente dalla modalità di provisioning degli utenti, IAM Identity Center reindirizza l' AWS Management Console interfaccia a riga di comando e l'autenticazione delle applicazioni al tuo IdP esterno. IAM Identity Center concede quindi l'accesso a tali risorse in base alle policy create in IAM Identity Center. Per ulteriori informazioni sul provisioning, consulta. Assegnazione di ruoli a utenti e gruppi

Come connettersi a un provider di identità esterno

Sono disponibili step-by-step tutorial per le persone supportate: IdPs

- CyberArk
- Google Workspace
- JumpCloud
- Microsoft Entra ID
- Okta
- OneLogin
- Ping Identity

Esistono diversi prerequisiti, considerazioni e procedure di approvvigionamento per i diversi dispositivi esterni supportati. IdPs La procedura seguente fornisce una panoramica generale della procedura utilizzata con tutti i provider di identità esterni.

Per connettersi a un provider di identità esterno

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, quindi scegli Azioni > Modifica l'origine dell'identità.
4. In Scegli l'origine dell'identità, seleziona Provider di identità esterno, quindi scegli Avanti.
5. In Configura provider di identità esterno, procedi come segue:

    a. In Metadati del fornitore di servizi, scegli Scarica il file di metadati per scaricare il file di metadati e salvarlo sul tuo sistema. Il file di metadati SAML di IAM Identity Center è richiesto dal tuo provider di identità esterno.

    b. In Metadati del provider di identità, scegli Scegli file e individua il file di metadati che hai scaricato dal tuo provider di identità esterno. Quindi carica il file. Questo file di metadati contiene il certificato x509 pubblico necessario utilizzato per considerare attendibili i messaggi inviati dall'IdP.

    c. Seleziona Successivo.

    > **Important**
    >
    > La modifica dell'origine da o verso Active Directory rimuove tutte le assegnazioni di utenti e gruppi esistenti. È necessario riapplicare manualmente le assegnazioni dopo aver modificato correttamente l'origine.

6. Dopo aver letto il disclaimer e aver iniziato a procedere, inserisci ACCETTA.
7. Scegli Cambia fonte di identità. Un messaggio di stato ti informa che hai cambiato correttamente l'origine dell'identità.

Argomenti

- Utilizzo della federazione delle identità SAML e SCIM con provider di identità esterni
- Profilo SCIM e implementazione SAML 2.0

Utilizzo della federazione delle identità SAML e SCIM con provider di identità esterni

IAM Identity Center implementa i seguenti protocolli basati su standard per la federazione delle identità:

- SAML 2.0 per l'autenticazione degli utenti
- SCIM per il provisioning

Qualsiasi provider di identità (IdP) che implementa questi protocolli standard dovrebbe interagire con successo con IAM Identity Center, con le seguenti considerazioni speciali:

- SAML
  - IAM Identity Center richiede un indirizzo e-mail in formato SAML NameID (ovvero,). `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
  - Il valore del campo NameID nelle asserzioni deve essere una stringa («») conforme a RFC 2822 (https://tools.ietf.org/html/rfc2822) addr-spec (https://tools.ietf.org/html/rfc2822#section-3.4.1). `name@domain.com`
  - Il file di metadati non può contenere più di 75000 caratteri.
  - I metadati devono contenere un EntityID, un certificato X509 e SingleSignOnService come parte dell'URL di accesso.
  - Una chiave di crittografia non è supportata.

- SCIM
  - L'implementazione di IAM Identity Center SCIM si basa sulle RFC SCIM 7642 (https://tools.ietf.org/html/rfc7642), 7643 (https://tools.ietf.org/html/rfc7643) e 7644 (https://tools.ietf.org/html/rfc7644) e sui requisiti di interoperabilità stabiliti nella bozza di marzo 2020 del Basic SCIM Profile 1.0 (https://openid.net/specs/fastfed-scim-1_0-02.html#rfc.section.4). FastFed Qualsiasi differenza tra questi documenti e l'attuale implementazione in IAM Identity Center è descritta nella sezione Operazioni API supportate della IAM Identity Center SCIM Implementation Developer Guide.

IdPs i prodotti che non sono conformi agli standard e alle considerazioni sopra menzionati non sono supportati. Contatta il tuo IdP per domande o chiarimenti sulla conformità dei suoi prodotti a questi standard e considerazioni.

In caso di problemi nel connettere il tuo IdP a IAM Identity Center, ti consigliamo di controllare:

- AWS CloudTrail registra filtrando il nome dell'evento P ExternalId DirectoryLogin
- Registri e/o registri di debug specifici per IDP
- Risoluzione dei problemi relativi a IAM Identity Center

> **Note**
>
> Alcuni IdPs, come quelli inclusi inTutorial introduttivi, offrono un'esperienza di configurazione semplificata per IAM Identity Center sotto forma di «applicazione» o «connettore» creato appositamente per IAM Identity Center. Se il tuo IdP offre questa opzione, ti consigliamo di utilizzarla, facendo attenzione a scegliere l'elemento creato specificamente per IAM Identity Center. Altri elementi denominati «AWS», «AWS federazione» o nomi «AWS" generici simili possono utilizzare altri approcci e/o endpoint di federazione e potrebbero non funzionare come previsto con IAM Identity Center.

Profilo SCIM e implementazione SAML 2.0

Sia SCIM che SAML sono considerazioni importanti per la configurazione di IAM Identity Center.

Implementazione SAML 2.0

IAM Identity Center supporta la federazione delle identità con SAML (Security Assertion Markup Language) 2.0. Ciò consente a IAM Identity Center di autenticare le identità di provider di identità esterni (). IdPs SAML 2.0 è uno standard aperto utilizzato per lo scambio sicuro di asserzioni SAML. SAML 2.0 trasmette informazioni su un utente tra un'autorità SAML (chiamata provider di identità o IdP) e un consumatore SAML (chiamato service provider o SP). Il servizio IAM Identity Center utilizza queste informazioni per fornire un single sign-on federato. Il Single Sign-On consente agli utenti di accedere Account AWS e configurare le applicazioni in base alle credenziali esistenti del provider di identità.

IAM Identity Center aggiunge funzionalità SAML IdP al tuo archivio AWS Managed Microsoft AD IAM Identity Center o a un provider di identità esterno. Gli utenti possono quindi accedere tramite Single Sign-On ai servizi che supportano SAML, incluse le applicazioni AWS Management Console e quelle di terze parti come, e. Microsoft 365 Concur Salesforce

Il protocollo SAML, tuttavia, non fornisce un modo per interrogare l'IdP per conoscere utenti e gruppi. Pertanto, è necessario rendere IAM Identity Center consapevole di tali utenti e gruppi inserendoli in IAM Identity Center.

Profilo SCIM

IAM Identity Center fornisce supporto per lo standard System for Cross-domain Identity Management (SCIM) v2.0. SCIM mantiene le identità del tuo IAM Identity Center sincronizzate con le identità del tuo IdP. Ciò include qualsiasi fornitura, aggiornamento e deprovisioning degli utenti tra il tuo IdP e IAM Identity Center.

Per ulteriori informazioni su come implementare SCIM, consulta. Provisioning automatico Per ulteriori dettagli sull'implementazione SCIM di IAM Identity Center, consulta la IAM Identity Center SCIM Implementation Developer Guide.

Argomenti

- Provisioning automatico
- Fornitura manuale
- Gestisci i certificati SAML 2.0

Provisioning automatico

IAM Identity Center supporta il provisioning automatico (sincronizzazione) di informazioni su utenti e gruppi dal tuo provider di identità (IdP) a IAM Identity Center utilizzando il protocollo System for Cross-domain Identity Management (SCIM) v2.0. Quando configuri la sincronizzazione SCIM, crei una mappatura degli attributi utente del tuo provider di identità (IdP) agli attributi denominati in IAM Identity Center. Ciò fa sì che gli attributi previsti corrispondano tra IAM Identity Center e il tuo IdP. Puoi configurare questa connessione nel tuo IdP utilizzando l'endpoint SCIM per IAM Identity Center e un token bearer che crei in IAM Identity Center.

Argomenti

- Considerazioni sull'utilizzo del provisioning automatico
- Come monitorare la scadenza dei token di accesso
- Come abilitare il provisioning automatico
- Come disattivare il provisioning automatico
- Come generare un nuovo token di accesso

- Come eliminare un token di accesso
- Come ruotare un token di accesso

Considerazioni sull'utilizzo del provisioning automatico

Prima di iniziare a implementare SCIM, ti consigliamo di esaminare innanzitutto le seguenti importanti considerazioni su come funziona con IAM Identity Center. Per ulteriori considerazioni sul provisioning, consulta la sezione Tutorial introduttivi applicabile al tuo IdP.

- Se stai fornendo un indirizzo email principale, questo valore di attributo deve essere unico per ogni utente. In alcuni casi IdPs, l'indirizzo e-mail principale potrebbe non essere un indirizzo e-mail reale. Ad esempio, potrebbe essere un Universal Principal Name (UPN) che assomiglia solo a un'e-mail. Questi IdPs possono avere un indirizzo e-mail secondario o «altro» che contiene l'indirizzo e-mail reale dell'utente. Devi configurare SCIM nel tuo IdP per mappare l'indirizzo email univoco non NULL all'attributo dell'indirizzo email primario di IAM Identity Center. Inoltre, devi mappare l'identificatore di accesso univoco non NULL degli utenti all'attributo del nome utente di IAM Identity Center. Verifica se il tuo IdP ha un unico valore che è sia l'identificatore di accesso che il nome e-mail dell'utente. In tal caso, puoi mappare il campo IdP sia all'e-mail principale di IAM Identity Center che al nome utente IAM Identity Center.
- Affinché la sincronizzazione SCIM funzioni, ogni utente deve avere un valore specificato per nome, cognome, nome utente e nome visualizzato. Se uno di questi valori non è presente in un utente, a quell'utente non verrà assegnato alcun ruolo.
- Se devi utilizzare applicazioni di terze parti, dovrai prima mappare l'attributo del soggetto SAML in uscita all'attributo del nome utente. Se l'applicazione di terze parti richiede un indirizzo e-mail instradabile, devi fornire l'attributo email al tuo IdP.
- Gli intervalli di provisioning e aggiornamento di SCIM sono controllati dal tuo provider di identità. Le modifiche agli utenti e ai gruppi nel tuo provider di identità si riflettono in IAM Identity Center solo dopo che il provider di identità ha inviato tali modifiche a IAM Identity Center. Rivolgiti al tuo provider di identità per i dettagli sulla frequenza degli aggiornamenti di utenti e gruppi.
- Attualmente, SCIM non fornisce attributi multivalore (come email o numeri di telefono multipli per un determinato utente). I tentativi di sincronizzare gli attributi multivalore in IAM Identity Center con SCIM falliranno. Per evitare errori, assicurati che venga passato un solo valore per ogni attributo. Se hai utenti con attributi multivalore, rimuovi o modifica le mappature degli attributi duplicati in SCIM presso il tuo IdP per la connessione a IAM Identity Center.
- Verifica che la mappatura `externalId` SCIM del tuo IdP corrisponda a un valore unico, sempre presente e con meno probabilità di modifica per i tuoi utenti. Ad esempio, il tuo IdP potrebbe fornire

un identificatore garantito `objectId` o di altro tipo che non è influenzato dalle modifiche agli attributi utente come nome ed email. In tal caso, puoi mappare quel valore nel campo `externalId` SCIM. Ciò garantisce che gli utenti non perdano AWS diritti, assegnazioni o autorizzazioni se è necessario modificare il loro nome o indirizzo e-mail.

- Utenti che non sono ancora stati assegnati a un'applicazione o che non Account AWS possono essere inseriti in IAM Identity Center. Per sincronizzare utenti e gruppi, assicurati che siano assegnati all'applicazione o a un'altra configurazione che rappresenti la connessione del tuo IdP a IAM Identity Center.
- Il comportamento di deprovisioning degli utenti è gestito dal provider di identità e può variare in base all'implementazione. Rivolgiti al tuo provider di identità per i dettagli sul deprovisioning degli utenti.

Per ulteriori informazioni sull'implementazione SCIM di IAM Identity Center, consulta la IAM Identity Center SCIM Implementation Developer Guide.

Come monitorare la scadenza dei token di accesso

I token di accesso SCIM vengono generati con una validità di un anno. Quando il token di accesso SCIM è impostato per scadere tra 90 giorni o meno, ti AWS invia promemoria nella console IAM Identity Center e tramite la AWS Health Dashboard per aiutarti a ruotare il token. Ruotando il token di accesso SCIM prima della scadenza, garantisci continuamente la fornitura automatica delle informazioni su utenti e gruppi. Se il token di accesso SCIM scade, la sincronizzazione delle informazioni su utenti e gruppi dal provider di identità in IAM Identity Center si interrompe, quindi il provisioning automatico non può più effettuare aggiornamenti o creare ed eliminare informazioni. L'interruzione del provisioning automatico può comportare maggiori rischi per la sicurezza e influire sull'accesso ai servizi.

I promemoria della console di Identity Center persistono finché non si ruota il token di accesso SCIM e si eliminano i token di accesso non utilizzati o scaduti. Gli eventi del AWS Health Dashboard vengono rinnovati settimanalmente da 90 a 60 giorni, due volte a settimana da 60 a 30 giorni, tre volte alla settimana da 30 a 15 giorni e ogni giorno da 15 giorni fino alla scadenza dei token di accesso SCIM.

Come abilitare il provisioning automatico

Utilizza la seguente procedura per abilitare il provisioning automatico di utenti e gruppi dal tuo IdP a IAM Identity Center utilizzando il protocollo SCIM.

> **Note**
>
> Prima di iniziare questa procedura, ti consigliamo di esaminare innanzitutto le considerazioni sul provisioning applicabili al tuo IdP. Per ulteriori informazioni, consulta la pagina Tutorial introduttivi dedicata al tuo IdP.

Per abilitare il provisioning automatico in IAM Identity Center

1. Dopo aver completato i prerequisiti, apri la console IAM Identity Center.
2. Scegli Impostazioni nel riquadro di navigazione a sinistra.
3. Nella pagina Impostazioni, individua la casella Informazioni sulla fornitura automatica, quindi scegli Abilita. Ciò abilita immediatamente il provisioning automatico in IAM Identity Center e visualizza le informazioni necessarie sull'endpoint SCIM e sul token di accesso.
4. Nella finestra di dialogo di provisioning automatico in entrata, copia ciascuno dei valori per le seguenti opzioni. Dovrai incollarli in un secondo momento quando configuri il provisioning nel tuo IdP.
   a. Endpoint SCIM
   b. Token di accesso
5. Scegli Chiudi.

Dopo aver completato questa procedura, è necessario configurare il provisioning automatico nel proprio IdP. Per ulteriori informazioni, consulta la pagina Tutorial introduttivi dedicata al tuo IdP.

Come disattivare il provisioning automatico

Utilizza la seguente procedura per disabilitare il provisioning automatico nella console IAM Identity Center.

> **Important**
>
> È necessario eliminare il token di accesso prima di iniziare questa procedura. Per ulteriori informazioni, consulta Come eliminare un token di accesso.

Per disabilitare il provisioning automatico nella console IAM Identity Center

1. Nella console IAM Identity Center, scegli Impostazioni nel riquadro di navigazione a sinistra.
2. Nella pagina Impostazioni, scegli la scheda Identity source, quindi scegli Azioni > Gestisci il provisioning.
3. Nella pagina Provisioning automatico, scegli Disabilita.
4. Nella finestra di dialogo Disabilita il provisioning automatico, esaminate le informazioni, digitate DISABLE, quindi scegliete Disabilita il provisioning automatico.

Come generare un nuovo token di accesso

Utilizza la seguente procedura per generare un nuovo token di accesso nella console IAM Identity Center.

> **Note**
>
> Questa procedura richiede che il provisioning automatico sia stato precedentemente abilitato. Per ulteriori informazioni, consulta Come abilitare il provisioning automatico.

Per generare un nuovo token di accesso

1. Nella console IAM Identity Center, scegli Impostazioni nel riquadro di navigazione a sinistra.
2. Nella pagina Impostazioni, scegli la scheda Identity source, quindi scegli Azioni > Gestisci il provisioning.
3. Nella pagina Provisioning automatico, in Token di accesso, scegli Genera token.
4. Nella finestra di dialogo Genera nuovo token di accesso, copia il nuovo token di accesso e salvalo in un posto sicuro.
5. Scegli Chiudi.

Come eliminare un token di accesso

Utilizza la seguente procedura per eliminare un token di accesso esistente nella console IAM Identity Center.

Per eliminare un token di accesso esistente

1. Nella console IAM Identity Center, scegli Impostazioni nel riquadro di navigazione a sinistra.
2. Nella pagina Impostazioni, scegli la scheda Identity source, quindi scegli Azioni > Gestisci il provisioning.
3. Nella pagina Provisioning automatico, in Token di accesso, seleziona il token di accesso che desideri eliminare, quindi scegli Elimina.
4. Nella finestra di dialogo Elimina token di accesso, esaminate le informazioni, digitate DELETE, quindi scegliete Elimina token di accesso.

Come ruotare un token di accesso

Una directory IAM Identity Center supporta fino a due token di accesso alla volta. Per generare un token di accesso aggiuntivo prima di qualsiasi rotazione, elimina tutti i token di accesso scaduti o non utilizzati.

Se il token di accesso SCIM sta per scadere, puoi utilizzare la seguente procedura per ruotare un token di accesso esistente nella console IAM Identity Center.

Per ruotare un token di accesso

1. Nella console IAM Identity Center, scegli Impostazioni nel riquadro di navigazione a sinistra.
2. Nella pagina Impostazioni, scegli la scheda Identity source, quindi scegli Azioni > Gestisci il provisioning.
3. Nella pagina Provisioning automatico, in Token di accesso, prendi nota dell'ID del token che desideri ruotare.
4. Segui i passaggi indicati Come generare un nuovo token di accesso per creare un nuovo token. Se hai già creato il numero massimo di token di accesso SCIM, dovrai prima eliminare uno dei token esistenti.
5. Vai al sito web del tuo provider di identità e configura il nuovo token di accesso per il provisioning SCIM, quindi verifica la connettività a IAM Identity Center utilizzando il nuovo token di accesso SCIM. Dopo aver confermato che il provisioning funziona correttamente utilizzando il nuovo token, continua con il passaggio successivo di questa procedura.
6. Segui i passaggi indicati Come eliminare un token di accesso per eliminare il vecchio token di accesso annotato in precedenza. Puoi anche utilizzare la data di creazione del token come suggerimento su quale token rimuovere.

Fornitura manuale

Alcuni IdPs non dispongono del supporto System for Cross-domain Identity Management (SCIM) o hanno un'implementazione SCIM incompatibile. In questi casi, puoi effettuare manualmente il provisioning degli utenti tramite la console IAM Identity Center. Quando aggiungi utenti a IAM Identity Center, assicurati di impostare il nome utente in modo che sia identico al nome utente che hai nel tuo IdP. Come minimo, devi avere un indirizzo email e un nome utente univoci. Per ulteriori informazioni, consulta Unicità del nome utente e dell'indirizzo e-mail.

È inoltre necessario gestire tutti i gruppi manualmente in IAM Identity Center. Per fare ciò, crei i gruppi e li aggiungi utilizzando la console IAM Identity Center. Non è necessario che questi gruppi corrispondano a quelli esistenti nel tuo IdP. Per ulteriori informazioni, consulta Gruppi.

Gestisci i certificati SAML 2.0

IAM Identity Center utilizza i certificati per configurare una relazione di fiducia SAML tra IAM Identity Center e il tuo provider di identità esterno (IdP). Quando aggiungi un IdP esterno in IAM Identity Center, devi anche ottenere almeno un certificato SAML 2.0 X.509 pubblico dall'IdP esterno. Tale certificato viene in genere installato automaticamente durante lo scambio di metadati IdP SAML durante la creazione di trust.

In qualità di amministratore di IAM Identity Center, a volte dovrai sostituire i vecchi certificati IdP con quelli più recenti. Ad esempio, potrebbe essere necessario sostituire un certificato IdP quando si avvicina la data di scadenza del certificato. Il processo di sostituzione di un certificato precedente con uno più recente viene definito rotazione dei certificati.

Argomenti

- Ruota un certificato SAML 2.0
- Indicatori dello stato di scadenza del certificato

Ruota un certificato SAML 2.0

Potrebbe essere necessario importare i certificati periodicamente per modificare i certificati non validi o scaduti emessi dal tuo provider di identità. Questo aiuta a prevenire interruzioni o tempi di inattività dell'autenticazione. Tutti i certificati importati sono automaticamente attivi. I certificati devono essere eliminati solo dopo aver verificato che non siano più utilizzati dal provider di identità associato.

È inoltre necessario considerare che alcuni IdPs potrebbero non supportare più certificati. In questo caso, la rotazione dei certificati con questi dati IdPs potrebbe comportare un'interruzione temporanea

del servizio per gli utenti. Il servizio viene ripristinato quando la fiducia con quell'IdP è stata ristabilita con successo. Pianifica attentamente questa operazione durante le ore non di punta, se possibile.

> **Note**
>
> Come best practice di sicurezza, in caso di segni di compromissione o cattiva gestione di un certificato SAML esistente, dovresti immediatamente rimuovere e ruotare il certificato.

La rotazione di un certificato IAM Identity Center è un processo in più fasi che prevede quanto segue:

- Ottenere un nuovo certificato dall'IdP
- Importazione del nuovo certificato in IAM Identity Center
- Attivazione del nuovo certificato nell'IdP
- Eliminazione del certificato precedente

Utilizza tutte le seguenti procedure per completare il processo di rotazione dei certificati evitando interruzioni dell'autenticazione.

Passaggio 1: ottenere un nuovo certificato dall'IdP

Vai al sito Web IdP e scarica il certificato SAML 2.0. Assicurati che il file del certificato sia scaricato in formato codificato PEM. La maggior parte dei provider consente di creare più certificati SAML 2.0 nell'IdP. È probabile che questi vengano contrassegnati come disabilitati o inattivi.

Fase 2: Importa il nuovo certificato in IAM Identity Center

Utilizza la seguente procedura per importare il nuovo certificato utilizzando la console IAM Identity Center.

1. Nella console IAM Identity Center, scegli Impostazioni.
2. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, quindi scegli Azioni > Gestisci l'autenticazione.
3. Nella pagina Gestisci certificati SAML 2.0, scegli Importa certificato.
4. Nella finestra di dialogo Importa certificato SAML 2.0, scegli Scegli file, vai al file del certificato e selezionalo, quindi scegli Importa certificato.

A questo punto, IAM Identity Center considererà attendibili tutti i messaggi SAML in entrata firmati da entrambi i certificati che hai importato.

Fase 3: Attiva il nuovo certificato nell'IdP

Torna al sito Web IdP e contrassegna il nuovo certificato creato in precedenza come principale o attivo. A questo punto tutti i messaggi SAML firmati dall'IdP dovrebbero utilizzare il nuovo certificato.

Fase 4: Eliminare il vecchio certificato

Utilizza la procedura seguente per completare il processo di rotazione dei certificati per il tuo IdP. Nell'elenco deve sempre essere presente almeno un certificato valido che non può essere rimosso.

> **Note**
>
> Assicurati che il tuo provider di identità non firmi più le risposte SAML con questo certificato prima di eliminarlo.

1. Nella pagina Gestisci i certificati SAML 2.0, scegli il certificato che desideri eliminare. Scegli Elimina.
2. Nella finestra di dialogo Elimina certificato SAML 2.0, digita **`DELETE`** per confermare, quindi scegli Elimina.
3. Torna al sito Web dell'IdP ed esegui i passaggi necessari per rimuovere il vecchio certificato inattivo.

Indicatori dello stato di scadenza del certificato

Nella pagina Gestisci i certificati SAML 2.0, potresti notare delle icone colorate degli indicatori di stato. Queste icone vengono visualizzate nella colonna Scade il accanto a ciascun certificato nell'elenco. Di seguito vengono descritti i criteri utilizzati da IAM Identity Center per determinare quale icona viene visualizzata per ogni certificato.

- Rosso: indica che un certificato è attualmente scaduto.
- Giallo: indica che un certificato scadrà tra 90 giorni o meno.
- Verde: indica che un certificato è attualmente valido e rimarrà valido per almeno altri 90 giorni.

Per verificare lo stato attuale di un certificato

1. Nella console IAM Identity Center, scegli Impostazioni.
2. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, quindi scegli Azioni > Gestisci l'autenticazione.
3. Nella pagina Gestisci l'autenticazione SAML 2.0, in Gestisci i certificati SAML 2.0, esamina lo stato dei certificati nell'elenco, come indicato nella colonna Scade il.

Utilizzo del portale di AWS accesso

Il portale di AWS accesso fornisce a voi (utenti finali) l'accesso Single Sign-On a tutte le vostre applicazioni cloud Account AWS e a quelle più comunemente utilizzate come Office 365, Concur, Salesforce e molte altre. È possibile avviare rapidamente più applicazioni semplicemente scegliendo l'icona Account AWS o dell'applicazione nel portale. La presenza di icone delle applicazioni nel portale di AWS accesso significa che un amministratore della società ha concesso l'accesso a quelle Account AWS o alle applicazioni. Significa anche che è possibile accedere a tutti questi account o applicazioni dal portale di AWS accesso senza ulteriori richieste di accesso.

Contatta l'amministratore per richiedere un accesso aggiuntivo nelle seguenti situazioni:

- Non vedi un'applicazione Account AWS o a cui devi accedere.
- L'accesso che hai a un determinato account o applicazione non è quello che ti aspettavi.

Argomenti

Accettazione dell'invito a entrare a far parte di IAM Identity Center

Se è la prima volta che AWS accedi al portale di accesso, controlla la tua e-mail per istruzioni su come attivare le credenziali utente.

Per attivare le credenziali utente

1. A seconda dell'e-mail che hai ricevuto dalla tua azienda, scegli uno dei seguenti metodi per attivare le credenziali utente in modo da poter iniziare a utilizzare il portale di AWS accesso.

   a. Se hai ricevuto un'e-mail con l'oggetto Invito a iscriverti a AWS IAM Identity Center (successore di AWS Single Sign-On), aprila e scegli Accetta invito. Nella pagina di registrazione di un nuovo utente, inserisci e conferma una password, quindi scegli Imposta nuova password. Utilizzerai quella password ogni volta che accederai al portale.

   b. Se ti è stata inviata un'e-mail dal supporto IT o dall'amministratore IT della tua azienda, segui le istruzioni fornite per attivare le credenziali utente.

2. Dopo aver attivato le credenziali utente fornendo una nuova password, il portale di AWS accesso effettua l'accesso automaticamente. Se ciò non si verifica, puoi accedere manualmente al portale di AWS accesso utilizzando le istruzioni fornite nella sezione successiva.

Accedere al portale di AWS accesso

A questo punto, un amministratore dovrebbe aver ricevuto un URL di AWS accesso specifico al portale di accesso. Una volta ottenuto questo URL, puoi procedere con l'accesso al portale. Per ulteriori informazioni, consulta Accedere al portale di AWS accesso.

> **Note**
>
> Dopo l'accesso, la durata predefinita della sessione del portale di AWS accesso è di 8 ore. Tieni presente che un amministratore può modificare la durata di questa sessione.

Dispositivi attendibili

Quando scegli l'opzione Questo è un dispositivo affidabile dalla pagina di accesso, IAM Identity Center considera autorizzati tutti gli accessi futuri da quel dispositivo. Ciò significa che IAM Identity Center non presenterà un'opzione per inserire un codice MFA fintanto che utilizzi quel dispositivo affidabile. Tuttavia, ci sono alcune eccezioni, tra cui l'accesso da un nuovo browser o quando al dispositivo è stato assegnato un indirizzo IP sconosciuto.

Suggerimenti per l' AWS accesso al portale di accesso

Ecco alcuni suggerimenti per aiutarti a gestire la tua esperienza con il portale di AWS accesso.

- A volte, potrebbe essere necessario disconnettersi e accedere nuovamente al portale di AWS accesso. Questa operazione potrebbe essere necessaria per accedere a nuove applicazioni recentemente assegnate dall'amministratore, ma non è obbligatoria in quanto tutte le nuove applicazioni vengono aggiornate ogni ora.
- Quando accedi al portale di AWS accesso, puoi aprire una qualsiasi delle applicazioni elencate nel portale scegliendo l'icona dell'applicazione. Dopo aver finito di utilizzare l'applicazione, è possibile chiuderla o uscire dal portale di AWS accesso. La chiusura dell'applicazione determina esclusivamente l'uscita da tale applicazione. Tutte le altre applicazioni aperte dal portale di AWS accesso rimangono aperte e in esecuzione.
- Prima di poter accedere come utente diverso, è necessario disconnettersi dal portale di AWS accesso. L'uscita dal portale determina la rimozione completa delle credenziali dalla sessione del browser.
- Dopo aver effettuato l' AWS accesso al portale di accesso, puoi passare a un ruolo. Il cambio di ruolo annulla temporaneamente le autorizzazioni utente originali e ti dà invece le autorizzazioni assegnate al ruolo. Per ulteriori informazioni, consulta Cambio di un ruolo (console).

Uscire dal portale di accesso AWS

Quando esci dal portale, le tue credenziali vengono rimosse completamente dalla sessione del browser. Per ulteriori informazioni, consulta Uscire dal portale di AWS accesso nella Accedi ad AWSguida.

Per uscire dal portale di AWS accesso

- Nel portale di AWS accesso, scegli Esci dalla barra di navigazione.

> **Note**
>
> Se desideri accedere come utente diverso, devi prima disconnetterti dal portale di AWS accesso.

Reimpostazione della password utente di IAM Identity Center

Il portale di AWS accesso fornisce agli utenti di IAM Identity Center l'accesso Single Sign-On a tutti gli AWS account assegnati e alle applicazioni cloud tramite un portale web. Il portale di AWS accesso è

diverso dal AWS Management Console, che è una raccolta di console di servizio per la gestione delle risorse. AWS

Utilizza questa procedura per reimpostare la password utente di IAM Identity Center per il portale di AWS accesso. Scopri di più sui tipi di utente nella Guida Accedi ad AWS per l'utente.

Considerazioni

La funzionalità di reimpostazione della password per il portale di AWS accesso è disponibile solo per gli utenti delle istanze di Identity Center che utilizzano la directory di Identity Center o AWS Managed Microsoft ADcome fonte di identità. Se l'utente è connesso a un provider di identità esterno o AD Connector, la reimpostazione della password utente deve essere eseguita dal provider di identità esterno o connessoActive Directory.

- Se la fonte dell'identità è una directory di IAM Identity Center, consultaRequisiti relativi alle password per la gestione delle identità in IAM Identity Center.
- Se la fonte dell'identità è una AWS Managed Microsoft AD, consulta Requisiti della password per la reimpostazione di una password. AWS Managed Microsoft AD

Per reimpostare la password del AWS portale di accesso

1. Apri un browser web e vai alla pagina di accesso del tuo portale di AWS accesso.

   Se non disponi dell'URL del portale di AWS accesso, controlla la posta elettronica. Dovresti aver ricevuto via email un invito a iscriverti a AWS IAM Identity Center che include un URL di accesso specifico al portale di AWS accesso. In alternativa, l'amministratore potrebbe averti fornito direttamente una password monouso e l'URL del portale di AWS accesso. Se non riesci a trovare queste informazioni, chiedi all'amministratore di inviartele.

   Per ulteriori informazioni sull'accesso al portale di AWS accesso, consulta Accedere al portale di AWS accesso nella Guida per l'Accedi ad AWS utente.
2. Inserisci il tuo nome utente, quindi scegli Avanti.
3. In Password, scegli Password dimenticata.

   Verifica il tuo nome utente e inserisci i caratteri dell'immagine fornita per confermare che non sei un robot. Quindi scegli Successivo. Potrebbe essere necessario disattivare il software di blocco degli annunci se non riesci a inserire caratteri.

4. Viene visualizzato un messaggio per confermare l'invio di un'e-mail di reimpostazione della password. Scegli Continua.
5. Riceverai un'email `no-reply@signin.aws` con l'oggetto Richiesta di reimpostazione della password. Nella tua email, scegli Reimposta la password.
6. Nella pagina Reimposta la password, verifica il tuo nome utente, specifica una nuova password per il portale di AWS accesso, quindi scegli Imposta nuova password.
7. Riceverai un'email da `no-reply@signin.aws` con l'oggetto Password aggiornata.

> **Note**
>
> Un amministratore può reimpostare la password inviandoti un'e-mail con le istruzioni per reimpostare la password o generando una password monouso e condividendola con te. Se sei un amministratore, consulta. Reimposta la password utente di IAM Identity Center per un utente finale

Ottenere le credenziali utente di IAM Identity Center per gli SDK AWS CLI or AWS

Puoi accedere ai AWS servizi in modo programmatico utilizzando i AWS Command Line Interface o i AWS Software Development Kit (SDK) con le credenziali utente di IAM Identity Center. Questo argomento descrive come ottenere credenziali temporanee per un utente in IAM Identity Center.

Il portale di AWS accesso fornisce agli utenti di IAM Identity Center l'accesso Single Sign-On alle proprie applicazioni Account AWS e a quelle sul cloud. Dopo aver effettuato l' AWS accesso al portale di accesso come utente IAM Identity Center, puoi ottenere credenziali temporanee. Puoi quindi utilizzare le credenziali, note anche come credenziali utente IAM Identity Center, negli AWS SDK AWS CLI o per accedere alle risorse in un. Account AWS

Se utilizzi il AWS CLI per accedere ai AWS servizi a livello di codice, puoi utilizzare le procedure in questo argomento per avviare l'accesso a. AWS CLIPer informazioni su AWS CLI, consulta la Guida per l'AWS Command Line Interface utente.

Se utilizzi gli AWS SDK per accedere ai AWS servizi in modo programmatico, seguendo le procedure riportate in questo argomento viene inoltre stabilita direttamente l'autenticazione per gli SDK. AWS Per informazioni sugli SDK, consulta la AWS Guida di riferimento agli SDK e agli strumenti AWS .

> **Note**
>
> Gli utenti di IAM Identity Center sono diversi dagli utenti IAM. Agli utenti IAM vengono concesse credenziali a lungo termine per AWS le risorse. Agli utenti di IAM Identity Center vengono concesse credenziali temporanee. Ti consigliamo di utilizzare credenziali temporanee come best practice di sicurezza per accedere alle tue, Account AWS poiché queste credenziali vengono generate ogni volta che accedi.

Prerequisiti

Per ottenere le credenziali temporanee per il tuo utente IAM Identity Center, avrai bisogno di quanto segue:

- Un utente IAM Identity Center: accederai al portale di AWS accesso come questo utente. Tu o il tuo amministratore potreste creare questo utente. Per informazioni su come abilitare IAM Identity Center e creare un utente IAM Identity Center, consultaInizia con le attività più comuni in IAM Identity Center.
- Accesso utente a un Account AWS: per concedere a un utente IAM Identity Center l'autorizzazione a recuperare le proprie credenziali temporanee, tu o un amministratore dovete assegnare all'utente IAM Identity Center un set di autorizzazioni. I set di autorizzazioni sono archiviati in IAM Identity Center e definiscono il livello di accesso che un utente IAM Identity Center ha a un. Account AWS Se il tuo amministratore ha creato l'utente IAM Identity Center per te, chiedigli di aggiungere questo accesso per te. Per ulteriori informazioni, consulta Assegna l'accesso utente a Account AWS.
- AWS CLI installato: per utilizzare le credenziali temporanee, devi installare il AWS CLI. Per le istruzioni, consulta Installazione o aggiornamento dell'ultima versione della AWS CLI nella Guida per l'utente di AWS CLI .

Considerazioni

Prima di completare i passaggi per ottenere le credenziali temporanee per il tuo utente IAM Identity Center, tieni a mente le seguenti considerazioni:

- IAM Identity Center crea ruoli IAM: quando assegni un utente in IAM Identity Center a un set di autorizzazioni, IAM Identity Center crea un ruolo IAM corrispondente dal set di autorizzazioni. I ruoli IAM creati dai set di autorizzazioni differiscono dai ruoli IAM creati AWS Identity and Access Management nei seguenti modi:

- IAM Identity Center possiede e protegge i ruoli creati dai set di autorizzazioni. Solo IAM Identity Center può modificare questi ruoli.
- Solo gli utenti di IAM Identity Center possono assumere i ruoli che corrispondono ai set di autorizzazioni loro assegnati. Non è possibile assegnare l'accesso ai set di autorizzazioni agli utenti IAM, agli utenti federati IAM o agli account di servizio.
- Non è possibile modificare una policy di fiducia dei ruoli su questi ruoli per consentire l'accesso ai principali al di fuori di IAM Identity Center.

Per informazioni su come ottenere credenziali temporanee per un ruolo creato in IAM, consulta Using temporary security credenziali with the AWS CLI nella Guida per l'utente.AWS Identity and Access Management

- Puoi impostare la durata della sessione per i set di autorizzazioni: dopo aver effettuato l'accesso al portale di AWS accesso, il set di autorizzazioni a cui è assegnato l'utente dell'IAM Identity Center viene visualizzato come ruolo disponibile. IAM Identity Center crea una sessione separata per questo ruolo. Questa sessione può durare da una a 12 ore, a seconda della durata della sessione configurata per il set di autorizzazioni. La durata predefinita della sessione è di un'ora. Per ulteriori informazioni, consulta Imposta la durata della sessione.

Acquisizione e aggiornamento delle credenziali temporanee

Puoi ottenere e aggiornare le credenziali temporanee per il tuo utente IAM Identity Center automaticamente o manualmente.

Argomenti

- Aggiornamento automatico delle credenziali (consigliato)
- Aggiornamento manuale delle credenziali

Aggiornamento automatico delle credenziali (consigliato)

L'aggiornamento automatico delle credenziali utilizza lo standard Open ID Connect (OIDC) Device Code Authorization. Con questo metodo, si avvia l'accesso direttamente utilizzando il comando in. `aws configure sso` AWS CLI Puoi utilizzare questo comando per accedere automaticamente a qualsiasi ruolo associato a qualsiasi set di autorizzazioni a cui sei assegnato per qualsiasi Account AWS ruolo.

Per accedere al ruolo creato per il tuo utente IAM Identity Center, esegui il `aws configure sso` comando, quindi autorizzalo AWS CLI da una finestra del browser. Finché è attiva una sessione del portale di AWS accesso, recupera AWS CLI automaticamente le credenziali temporanee e aggiorna automaticamente le credenziali.

Per ulteriori informazioni, consulta Configurare il profilo *`aws configure sso wizard`* nella Guida per l'utente.AWS Command Line Interface

Per ottenere credenziali temporanee che si aggiornano automaticamente

1. Accedi al portale di AWS accesso utilizzando l'URL di accesso specifico fornito dall'amministratore. Se hai creato l'utente IAM Identity Center, hai AWS inviato un invito via e-mail che include l'URL di accesso. Per ulteriori informazioni, consulta Accedere al portale di AWS accesso nella Guida per l'utente di AWS accesso.
2. Nella scheda Account, individua la cartella Account AWS da cui desideri recuperare le credenziali. Quando scegli l'account, vengono visualizzati il nome dell'account, l'ID dell'account e l'indirizzo e-mail associati all'account.

   > **Note**
   >
   > Se non ne vedi nessuno Account AWSnell'elenco, è probabile che non ti sia ancora stato assegnato un set di autorizzazioni per quell'account. In questo caso, contatta l'amministratore e chiedigli di aggiungere questo accesso per te. Per ulteriori informazioni, consulta Assegna l'accesso utente a Account AWS.

3. Sotto il nome dell'account, il set di autorizzazioni a cui è assegnato l'utente IAM Identity Center appare come ruolo disponibile. Ad esempio, se l'utente IAM Identity Center è assegnato al set di PowerUserAccessautorizzazioni per l'account, il ruolo viene visualizzato nel portale di AWS accesso come PowerUserAccess.
4. A seconda dell'opzione accanto al nome del ruolo, scegli Chiavi di accesso o scegli Accesso da riga di comando o accesso programmatico.
5. Nella finestra di dialogo Ottieni credenziali, scegli macOS e Linux, Windows PowerShelloppure, a seconda del sistema operativo su cui hai installato il. AWS CLI
6. Sotto le credenziali di AWS IAM Identity Center (consigliato), vengono visualizzati i tuoi `SSO Start URL` e`SSO Region`. Questi valori sono necessari per configurare sia un profilo abilitato per IAM Identity Center che `sso-session` per il tuo AWS CLI. Per completare questa

configurazione, segui le istruzioni in Configura il tuo profilo con la `aws configure sso wizard` Guida per l'AWS Command Line Interface utente.

Continua a utilizzare AWS CLI le credenziali necessarie Account AWS fino alla scadenza delle credenziali.

Aggiornamento manuale delle credenziali

È possibile utilizzare il metodo di aggiornamento manuale delle credenziali per ottenere credenziali temporanee per un ruolo associato a un set di autorizzazioni specifico in uno specifico. Account AWS A tale scopo, copiate e incollate i comandi richiesti per le credenziali temporanee. Con questo metodo, è necessario aggiornare manualmente le credenziali temporanee.

È possibile eseguire AWS CLI i comandi fino alla scadenza delle credenziali temporanee.

Per ottenere credenziali da aggiornare manualmente

1. Accedi al portale di AWS accesso utilizzando l'URL di accesso specifico fornito dall'amministratore. Se hai creato l'utente IAM Identity Center, hai AWS inviato un invito via e-mail che include l'URL di accesso. Per ulteriori informazioni, consulta Accedere al portale di AWS accesso nella Guida per l'utente di AWS accesso.
2. Nella scheda Account, individua la cartella Account AWS da cui desideri recuperare le credenziali di accesso ed espandila per mostrare il nome del ruolo IAM (ad esempio Amministratore). A seconda dell'opzione che hai accanto al nome del ruolo IAM, scegli Chiavi di accesso o scegli Accesso da riga di comando o accesso programmatico.

   > **Note**
   >
   > Se non ne vedi nessuno Account AWSnell'elenco, è probabile che non ti sia ancora stato assegnato un set di autorizzazioni per quell'account. In questo caso, contatta l'amministratore e chiedigli di aggiungere questo accesso per te. Per ulteriori informazioni, consulta Assegna l'accesso utente a Account AWS.

3. Nella finestra di dialogo Ottieni credenziali, scegli macOS e Linux, Windows PowerShello, a seconda del sistema operativo su cui hai installato il. AWS CLI
4. Selezionare una delle seguenti opzioni:

   - Opzione 1: imposta AWS le variabili di ambiente

Scegliete questa opzione per sovrascrivere tutte le impostazioni delle credenziali, incluse le impostazioni nei `credentials` file e `config` nei file. Per ulteriori informazioni, consulta Variabili di ambiente da configurare AWS CLI nella Guida per l'AWS CLI utente.

Per utilizzare questa opzione, copiate i comandi negli appunti, incollateli nella finestra del AWS CLI terminale e premete Invio per impostare le variabili di ambiente richieste.

- Opzione 2: aggiungi un profilo al file delle credenziali AWS

  Scegli questa opzione per eseguire comandi con diversi set di credenziali.

  Per utilizzare questa opzione, copia i comandi negli appunti, quindi incollali nel AWS `credentials` file condiviso per configurare un nuovo profilo denominato. Per ulteriori informazioni, consulta File di configurazione e credenziali condivisi nella Guida di riferimento agli AWS SDK e agli strumenti. Per utilizzare questa credenziale, specifica l'`--profile`opzione nel comando. AWS CLI Ciò influisce su tutti gli ambienti che utilizzano lo stesso file di credenziali.

- Opzione 3: utilizza valori individuali nel client AWS di servizio

  Scegliete questa opzione per accedere alle AWS risorse da un client AWS di servizio. Per ulteriori informazioni, consulta Strumenti su cui basarsi AWS.

  Per utilizzare questa opzione, copia i valori negli appunti, incolla i valori nel codice e assegnali alle variabili appropriate per il tuo SDK. Per ulteriori informazioni, consulta la documentazione per la tua API SDK specifica.

Creazione di collegamenti rapidi alle destinazioni AWS Management Console

I collegamenti di scelta rapida creati nel portale di AWS accesso indirizzano gli utenti di IAM Identity Center verso una destinazione specifica nel AWS Management Console, con un set di autorizzazioni specifico e in uno specifico. Account AWS

I link di scelta rapida fanno risparmiare tempo a te e ai tuoi collaboratori. Invece di navigare verso l'URL di destinazione desiderato AWS Management Console (ad esempio, una pagina di istanza del bucket Amazon S3) tra più pagine, AWS incluso il portale di accesso, puoi utilizzare un collegamento di scelta rapida per raggiungere automaticamente la stessa destinazione.

Opzioni di destinazione del collegamento di scelta rapida

I link di scelta rapida hanno tre opzioni di destinazione, elencate qui per priorità:

- (Facoltativo) Qualsiasi URL di destinazione incluso AWS Management Console nel collegamento di scelta rapida. Ad esempio, la pagina dell'istanza del bucket Amazon S3.
- (Facoltativo) URL dello stato di inoltro configurato dall'amministratore per il set di autorizzazioni in questione. Per ulteriori informazioni sull'impostazione dello stato del relè, vedere. Imposta lo stato del relè
- AWS Management Console casa. La destinazione predefinita se non ne specifichi una.

> **Note**
>
> La navigazione automatica verso una destinazione ha esito positivo solo se sei autenticato con IAM Identity Center e hai assegnato il set di autorizzazioni necessario per l' AWS account e l'URL di destinazione.

Il portale di AWS accesso include un pulsante Crea scorciatoia che ti aiuta a creare un collegamento di scelta rapida condivisibile. Se intendi specificare un URL di destinazione (la prima opzione nell'elenco precedente), puoi copiare l'URL negli appunti per condividerlo.

Crea un collegamento di scelta rapida nel portale di accesso AWS

1. Una volta effettuato l' AWS accesso al portale di accesso, scegli la scheda Account, quindi scegli il pulsante Crea collegamento.
2. Nella finestra di dialogo:
   a. Scegli un account Account AWS utilizzando l'ID o il nome dell'account. Durante la digitazione, un menu a discesa mostra gli ID e i nomi degli account corrispondenti a cui puoi accedere. Puoi scegliere solo un account a cui hai accesso.
   b. Facoltativamente, scegli un ruolo IAM dall'elenco a discesa. Questi sono i set di autorizzazioni che ti sono stati assegnati per l'account selezionato. Se si omette di scegliere il ruolo, agli utenti viene richiesto di selezionarne uno assegnato per l'account scelto quando utilizzano il collegamento di scelta rapida.

> **Note**
>
> Non puoi concedere un nuovo accesso con i link di scelta rapida. I link di scelta rapida funzionano solo con i set di autorizzazioni già assegnati all'utente. Se all'utente non sono assegnati i set di autorizzazioni necessari per l'account e l'URL di destinazione, gli viene negato l'accesso.

c. Facoltativamente, inserisci l'URL di destinazione del portale di AWS accesso. Se si omette di inserire un URL, la destinazione viene determinata automaticamente quando si utilizza il collegamento di scelta rapida, in base alle opzioni di destinazione del collegamento di scelta rapida menzionate in precedenza.

d. Il link di scelta rapida viene generato nella parte inferiore della finestra di dialogo, in base all'input. Scegliete il pulsante Copia URL. Ora puoi creare un segnalibro con il link di scelta rapida copiato o condividerlo con i tuoi collaboratori che hanno accesso allo stesso account con lo stesso set di autorizzazioni o un altro set di autorizzazioni sufficiente.

Creazione di collegamenti rapidi sicuri AWS Management Console con codifica URL

Tutti i valori dei parametri dell'URL, inclusi l'ID dell'account, il nome del set di autorizzazioni e l'URL di destinazione, devono essere codificati come URL.

I link di scelta rapida estendono l'URL del portale di AWS accesso con il seguente percorso:

```
/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

L'URL completo nella AWS partizione classica segue questo schema:

```
https://[your_subdomain].awsapps.com/start/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

Ecco un esempio di collegamento rapido che collega un utente all'account `123456789012` con il set di `S3FullAccess` autorizzazioni e lo reindirizza alla home page della console S3:

- `https://example.awsapps.com/start/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`

- (AWS GovCloud (US) Region) `https://start.us-gov-west-1.us-gov-home.awsapps.com/directory/example/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`

Registrazione di un dispositivo per l'MFA

Utilizza la seguente procedura all'interno del portale di AWS accesso per registrare il tuo nuovo dispositivo per l'autenticazione a più fattori (MFA).

> **Note**
>
> Ti consigliamo di scaricare l'app Authenticator appropriata sul tuo dispositivo prima di iniziare i passaggi di questa procedura. Per un elenco di app che puoi utilizzare per i dispositivi MFA, consulta. App di autenticazione virtuale

Per registrare il dispositivo per l'utilizzo con MFA

1. Accedi al tuo portale di AWS accesso. Per ulteriori informazioni, consulta Accedere al portale di AWS accesso.
2. In alto a destra della pagina, scegli Dispositivi MFA.
3. Nella pagina Dispositivi di autenticazione a più fattori (MFA), scegli Registra dispositivo.

   > **Note**
   >
   > Se l'opzione Registra dispositivo MFA è disattivata, contatta l'amministratore per ricevere assistenza sulla registrazione del dispositivo.

4. Nella pagina Registra dispositivo MFA, seleziona uno dei seguenti tipi di dispositivi MFA e segui le istruzioni:

   - App Authenticator
     1. Nella pagina Configura l'app di autenticazione, potresti notare le informazioni di configurazione per il nuovo dispositivo MFA, inclusa una grafica con codice QR. L'immagine è una rappresentazione della chiave segreta disponibile per l'immissione manuale sui dispositivi che non supportano i codici QR.

2. Utilizzando il dispositivo MFA fisico, procedi come segue:

   a. Apri un'app di autenticazione MFA compatibile. Per un elenco delle app testate che puoi utilizzare con i dispositivi MFA, consulta. App di autenticazione virtuale Se l'app MFA supporta più account (più dispositivi MFA), scegli l'opzione per creare un nuovo account (un nuovo dispositivo MFA).

   b. Determina se l'app MFA supporta i codici QR, quindi esegui una delle seguenti operazioni nella pagina Configura l'app di autenticazione:

      i. 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.

      ii. Scegli Mostra chiave segreta, quindi inserisci quella chiave segreta nella tua app MFA.

      > **Important**
      >
      > Quando configuri un dispositivo MFA per IAM Identity Center, ti consigliamo di salvare una copia del codice QR o della chiave segreta in un luogo sicuro. Questo può essere utile se perdi il telefono o devi reinstallare l'app MFA Authenticator. Se si verifica una di queste situazioni, puoi riconfigurare rapidamente l'app per utilizzare la stessa configurazione MFA.

3. Nella pagina Configura l'app di autenticazione, in Codice di autenticazione, inserisci la password monouso attualmente visualizzata sul dispositivo MFA fisico.

   > **Important**
   >
   > Invia la richiesta immediatamente dopo la generazione del codice. Se si genera il codice e poi si attende troppo a lungo per inviare la richiesta, il dispositivo MFA viene associato correttamente all'utente, ma il dispositivo MFA non è sincronizzato. Ciò accade perché le password monouso temporanee (TOTP) scadono dopo un breve periodo di tempo. In tal caso, puoi sincronizzare nuovamente il dispositivo.

4. Scegliere Assign MFA (Assegna MFA). Il dispositivo MFA può ora iniziare a generare password monouso ed è ora pronto per l'uso con. AWS

- Chiave di sicurezza o autenticatore integrato

1. Nella pagina Registra la chiave di sicurezza dell'utente, segui le istruzioni fornite dal tuo browser o dalla tua piattaforma.

> **Note**
>
> L'esperienza varia in base al browser o alla piattaforma. Dopo aver registrato correttamente il dispositivo, puoi associare un nome visualizzato descrittivo al dispositivo appena registrato. Per modificare il nome, scegli Rinomina, inserisci il nuovo nome, quindi scegli Salva.

Personalizzazione dell'URL del portale di AWS accesso

Per impostazione predefinita, puoi accedere al portale di AWS accesso utilizzando un URL che segue questo formato:`d-xxxxxxxxxx.awsapps.com/start`. Puoi personalizzare l'URL come segue:`your_subdomain.awsapps.com/start`.

> **Important**
>
> Se modifichi l'URL del portale di AWS accesso, non puoi modificarlo in un secondo momento.

Per personalizzare il tuo URL

1. Apri la AWS IAM Identity Center console all'indirizzo https://console.aws.amazon.com/singlesignon/.
2. Nella console IAM Identity Center, scegli Dashboard nel riquadro di navigazione e individua la sezione di riepilogo delle impostazioni.
3. Scegli il pulsante Personalizza sotto l'URL del portale di AWS accesso.

> **Note**
>
> Se il pulsante Personalizza non viene visualizzato, significa che il portale di AWS accesso è già stato personalizzato. La personalizzazione dell'URL del portale di AWS accesso è un'operazione unica che non può essere annullata.

4. Inserisci il nome del sottodominio desiderato e scegli Salva.

Ora puoi accedere alla AWS Console tramite il tuo portale di AWS accesso con il tuo URL personalizzato.

Autenticazione a più fattori per gli utenti di Identity Center

L'autenticazione a più fattori (MFA) offre un modo semplice e sicuro per aggiungere un ulteriore livello di protezione oltre al meccanismo di autenticazione predefinito di nome utente e password.

Quando gli amministratori abilitano la MFA, gli utenti devono accedere AWS al portale di accesso con due fattori:

- Nome utente e password. Questo è il primo fattore ed è qualcosa che gli utenti sanno.
- Un codice, una chiave di sicurezza o dati biometrici. Questo è il secondo fattore ed è qualcosa che gli utenti possiedono (possesso) o possiedono (dati biometrici). Il secondo fattore potrebbe essere un codice di autenticazione generato dal dispositivo mobile, una chiave di sicurezza collegata al computer o la scansione biometrica dell'utente.

Insieme, questi molteplici fattori garantiscono una maggiore sicurezza impedendo l'accesso non autorizzato alle AWS risorse a meno che una sfida MFA valida non sia stata completata con successo.

Ogni utente può registrare fino a due app di autenticazione virtuale, ossia applicazioni di autenticazione delle password monouso installate sul dispositivo mobile o tablet, e sei autenticatori FIDO, che includono autenticatori e chiavi di sicurezza integrati, per un totale di otto dispositivi MFA. Ulteriori informazioni su Tipi di MFA disponibili per IAM Identity Center.

> **Important**
>
> Come best practice di sicurezza, consigliamo vivamente di abilitare l'MFA.

Argomenti

Tipi di MFA disponibili per IAM Identity Center

L'autenticazione a più fattori (MFA) è un meccanismo semplice ed efficace per migliorare la sicurezza degli utenti. Il primo fattore di un utente, la password, è un segreto che memorizza, 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 ulteriore livello di sicurezza al tuo account.

IAM Identity Center MFA supporta i seguenti tipi di dispositivi. Tutti i tipi di MFA sono supportati sia per l'accesso alla console basato su browser che per l'utilizzo della versione AWS CLI v2 con IAM Identity Center.

- Autenticatori FIDO2, inclusi autenticatori e chiavi di sicurezza integrati
- App di autenticazione virtuale
- La tua RAGGIO MFA implementazione connessa tramite AWS Managed Microsoft AD

Un utente può avere fino a otto dispositivi MFA, che includono fino a due app di autenticazione virtuale e sei autenticatori FIDO, registrati su un account. Puoi anche configurare le impostazioni di abilitazione della MFA in modo che richieda l'MFA ogni volta che gli utenti accedono o per abilitare dispositivi affidabili che non richiedono l'MFA a ogni accesso. Per ulteriori informazioni su come configurare i tipi di MFA per gli utenti, consulta Scegli i tipi di MFA e. Configurazione dell'applicazione dei dispositivi MFA

Autenticatori FIDO2

FIDO2 è uno standard che include CTAP2 e WebAuthnsi 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

AWSsupporta 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
- Chiavi di sicurezza
- Gestori di password, fornitori di chiavi di accesso e altri autenticatori FIDO

Autenticatori integrati

Molti computer e telefoni cellulari moderni dispongono di autenticatori integrati, come TouchID su Macbook o una fotocamera compatibile con Windows Hello. Se il dispositivo dispone di un autenticatore integrato compatibile con FIDO, puoi utilizzare l'impronta digitale, il viso o il pin del dispositivo come secondo fattore.

Chiavi di sicurezza

Le chiavi di sicurezza sono autenticatori hardware esterni compatibili con FIDO che puoi acquistare e connettere al tuo dispositivo tramite USB, BLE o NFC. Quando viene richiesta l'autenticazione a più fattori, è sufficiente eseguire un gesto con il sensore della chiave. Alcuni esempi di chiavi di sicurezza includono le chiavi Feitian YubiKeys e le chiavi di sicurezza più comuni creano credenziali FIDO legate al dispositivo. Per un elenco di tutte le chiavi di sicurezza certificate FIDO, 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).

App di autenticazione virtuale

Le app di autenticazione sono essenzialmente autenticatori di terze parti basati su password monouso (OTP). 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 la MFA, gli utenti devono inserire un codice valido dall'app di autenticazione nella casella di immissione visualizzata. Ogni dispositivo MFA assegnato a un utente deve essere univoco. È possibile registrare due app di autenticazione per ogni utente.

App di autenticazione testate

Qualsiasi applicazione conforme a TOTP funzionerà con IAM Identity Center MFA. La tabella seguente elenca le app di autenticazione di terze parti più note tra cui scegliere.

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

RAGGIO MFA

Il Remote Authentication Dial-In User Service (RADIUS) è un protocollo client-server standard del settore che fornisce l'autenticazione, l'autorizzazione e la gestione contabile in modo che gli utenti possano connettersi ai servizi di rete. AWS Directory Serviceinclude un client RADIUS che si connette al server RADIUS su cui è stata implementata la soluzione MFA. Per ulteriori informazioni, consulta Enable Multi-Factor Authentication for. AWS Managed Microsoft AD

Puoi utilizzare RADIUS MFA o MFA in IAM Identity Center per gli accessi degli utenti al portale utenti, ma non entrambi. L'MFA in IAM Identity Center è un'alternativa a RADIUS MFA nei casi in cui si desideri l'autenticazione AWS nativa a due fattori per l'accesso al portale.

Quando abiliti l'MFA in IAM Identity Center, i tuoi utenti hanno bisogno di un dispositivo MFA per accedere al portale di accesso. AWS Se in precedenza avevi utilizzato RADIUS MFA, l'attivazione dell'MFA in IAM Identity Center sostituisce di fatto RADIUS MFA per gli utenti che accedono al portale di accesso. AWS Tuttavia, RADIUS MFA continua a rappresentare una sfida per gli utenti quando accedono a tutte le altre applicazioni che funzionano conAWS Directory Service, come Amazon. WorkDocs

Se la tua MFA è disabilitata sulla console IAM Identity Center e hai configurato RADIUS MFA con, AWS Directory Service RADIUS MFA regola l'accesso al portale di accesso. AWS Ciò significa che IAM Identity Center torna alla configurazione RADIUS MFA se l'MFA è disabilitata.

Configurazione MFA

I seguenti argomenti forniscono istruzioni per la configurazione dei dispositivi MFA in IAM Identity Center.

Argomenti

Considerazioni prima di abilitare la MFA in IAM Identity Center

Prima di abilitare l'MFA, considera quanto segue:

- Gli utenti sono invitati a registrare più autenticatori di backup per tutti i tipi di MFA abilitati. Questa pratica può prevenire la perdita di accesso in caso di guasto o smarrimento di un dispositivo MFA.
- Non scegliere l'opzione Richiedi loro di fornire una password monouso inviata tramite e-mail se gli utenti devono accedere al portale di accesso per AWS accedere alla propria posta elettronica. Ad esempio, gli utenti potrebbero utilizzare il portale Microsoft 365 di AWS accesso per leggere le proprie e-mail. In questo caso, gli utenti non saranno in grado di recuperare il codice di verifica e non potranno AWS accedere al portale di accesso. Per ulteriori informazioni, consulta Configurazione dell'applicazione dei dispositivi MFA.
- Se utilizzi già RADIUS MFA con cui hai configuratoAWS Directory Service, non è necessario abilitare l'MFA all'interno di IAM Identity Center. MFA in IAM Identity Center è un'alternativa a RADIUS MFA per Microsoft Active Directory gli utenti di IAM Identity Center. Per ulteriori informazioni, consulta RAGGIO MFA.
- Puoi utilizzare le funzionalità MFA in IAM Identity Center quando la tua origine di identità è configurata con l'identity store di IAM Identity Center o AD AWS Managed Microsoft AD Connector. L'MFA in IAM Identity Center non è attualmente supportata per i provider di identità esterni.

Abilita l'MFA in IAM Identity Center

Puoi abilitare l'accesso sicuro al portale di AWS accesso, alle app integrate di IAM Identity Center e AWS CLI abilitando l'autenticazione a più fattori (MFA).

Argomenti

Richiedi agli utenti l'MFA

Utilizza i seguenti passaggi per abilitare l'MFA nella console IAM Identity Center. Prima di iniziare, ti consigliamo di comprendere ilTipi di MFA disponibili per IAM Identity Center.

> **Note**
>
> Se utilizzi un IdP esterno, la sezione Autenticazione a più fattori non sarà disponibile. Il tuo IdP esterno gestisce le impostazioni MFA, anziché IAM Identity Center a gestirle.

Per abilitare l'MFA

1. Apri la console IAM Identity Center.
2. Nel riquadro di navigazione a sinistra scegliere Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Autenticazione.
4. Nella sezione Autenticazione a più fattori, scegli Configura.
5. Nella pagina Configura l'autenticazione a più fattori, in Richiedi l'autenticazione a più fattori agli utenti, scegli una delle seguenti modalità di autenticazione in base al livello di sicurezza richiesto dalla tua azienda:

   - Solo quando il loro contesto di accesso cambia (sensibile al contesto)

     In questa modalità (impostazione predefinita), IAM Identity Center offre agli utenti la possibilità di fidarsi del proprio dispositivo durante l'accesso. Dopo che un utente ha indicato di volersi fidare di un dispositivo, IAM Identity Center richiede all'utente l'MFA una volta e analizza il contesto di accesso (ad esempio dispositivo, browser e posizione) per gli accessi successivi dell'utente. Per gli accessi successivi, IAM Identity Center determina se l'utente accede

con un contesto precedentemente attendibile. Se il contesto di accesso dell'utente cambia, IAM Identity Center richiede all'utente l'MFA oltre all'indirizzo e-mail e alle credenziali della password.

Questa modalità offre facilità d'uso per gli utenti che accedono spesso dal proprio posto di lavoro, quindi non devono completare la MFA a ogni accesso. Viene loro richiesta l'autenticazione a più fattori solo se il contesto di accesso cambia.

- Ogni volta che accedono (sempre attivi)

  In questa modalità, IAM Identity Center richiede che gli utenti con un dispositivo MFA registrato vengano avvisati ogni volta che effettuano l'accesso. È consigliabile utilizzare questa modalità se si utilizzano politiche organizzative o di conformità che richiedono agli utenti di completare la MFA ogni volta che accedono al portale di AWS accesso. Ad esempio, PCI DSS consiglia vivamente l'MFA durante ogni accesso per accedere alle applicazioni che supportano transazioni di pagamento ad alto rischio.

- Mai (disabilitato)

  In questa modalità, tutti gli utenti accederanno solo con il nome utente e la password standard. La scelta di questa opzione disattiva IAM Identity Center MFA.

  > **Note**
  >
  > Se utilizzi già RADIUS MFA con AWS Directory Service e desideri continuare a utilizzarlo come tipo di MFA predefinito, puoi lasciare la modalità di autenticazione disabilitata per bypassare le funzionalità MFA in IAM Identity Center. Il passaggio dalla modalità Disabilitata alla modalità con riconoscimento del contesto o Always-on sostituirà le impostazioni MFA RADIUS esistenti. Per ulteriori informazioni, consulta RAGGIO MFA.

6. Seleziona Save changes (Salva modifiche).

Argomenti correlati

- Scegli i tipi di MFA
- Configurazione dell'applicazione dei dispositivi MFA
- Consenti agli utenti di registrare i propri dispositivi MFA

Disattiva l'MFA per la tua directory IAM Identity Center

Quando disabiliti l'autenticazione a più fattori (MFA) per la tua directory IAM Identity Center, consente agli utenti di accedere solo con il nome utente e la password standard. Sebbene l'autenticazione a più fattori sia disattivata per la directory degli utenti di Identity Center, non è possibile gestire i dispositivi MFA nei relativi dettagli utente e gli utenti della directory Identity Center non possono gestire i dispositivi MFA dal portale di accesso. AWS

Per disabilitare l'MFA per la tua directory IAM Identity Center

> **Important**
>
> Le istruzioni in questa sezione si applicano a. AWS IAM Identity Center Non si applicano a AWS Identity and Access Management(IAM). Gli utenti, i gruppi e le credenziali utente di IAM Identity Center sono diversi dagli utenti, dai gruppi e dalle credenziali utente IAM. Se stai cercando istruzioni sulla disattivazione della MFA per gli utenti IAM, consulta Disattivazione dei dispositivi MFA nella Guida per l'utente. AWS Identity and Access Management

1. Apri la console IAM Identity Center.
2. Nel riquadro di navigazione a sinistra scegliere Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Autenticazione.
4. Nella sezione Autenticazione a più fattori, scegli Configura.
5. Nella pagina Configura l'autenticazione a più fattori, nella sezione Richiedi agli utenti la MFA, scegli il pulsante di opzione Mai (disabilitato).
6. Seleziona Salvataggio delle modifiche.

Scegli i tipi di MFA

Utilizza la procedura seguente per scegliere i tipi di dispositivi con cui gli utenti possono autenticarsi quando viene richiesta l'autenticazione MFA nel portale di accesso. AWS

Per configurare i tipi di MFA per i tuoi utenti

1. Apri la console IAM Identity Center.
2. Nel riquadro di navigazione a sinistra scegliere Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Autenticazione.

4. Nella sezione Autenticazione a più fattori, scegli Configura.
5. Nella pagina Configura l'autenticazione a più fattori, in Gli utenti possono autenticarsi con questi tipi di MFA, scegli uno dei seguenti tipi di MFA in base alle tue esigenze aziendali. Per ulteriori informazioni, consulta Tipi di MFA disponibili per IAM Identity Center.

   - Autenticatori FIDO2, inclusi autenticatori e chiavi di sicurezza integrati
   - App di autenticazione virtuale
6. Seleziona Salvataggio delle modifiche.

Configurazione dell'applicazione dei dispositivi MFA

Utilizzare la procedura seguente per determinare se gli utenti devono disporre di un dispositivo MFA registrato per AWS accedere al portale di accesso.

Per configurare l'applicazione dei dispositivi MFA per i tuoi utenti

1. Apri la console IAM Identity Center.
2. Nel riquadro di navigazione a sinistra scegliere Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Autenticazione.
4. Nella sezione Autenticazione a più fattori, scegli Configura.
5. Nella pagina Configura l'autenticazione a più fattori, in Se un utente non dispone ancora di un dispositivo MFA registrato, scegli una delle seguenti scelte in base alle tue esigenze aziendali:

   - Richiedi loro di registrare un dispositivo MFA al momento dell'accesso

     Questa è l'impostazione predefinita quando configuri MFA per la prima volta per IAM Identity Center. Utilizza questa opzione quando desideri richiedere agli utenti che non dispongono ancora di un dispositivo MFA registrato di registrare automaticamente un dispositivo durante l'accesso dopo un'autenticazione con password riuscita. Ciò consente di proteggere AWS gli ambienti dell'organizzazione con l'MFA senza dover registrare e distribuire singolarmente i dispositivi di autenticazione agli utenti. Durante l'iscrizione automatica, i tuoi utenti possono registrare qualsiasi dispositivo tra quelli disponibili Tipi di MFA disponibili per IAM Identity Center che hai abilitato in precedenza. Dopo aver completato la registrazione, gli utenti hanno la possibilità di assegnare un nome descrittivo al dispositivo MFA appena registrato, dopodiché IAM Identity Center reindirizza l'utente alla destinazione originale. Se il dispositivo dell'utente viene smarrito o rubato, puoi semplicemente rimuoverlo dal suo account e IAM Identity Center richiederà all'utente di registrare automaticamente un nuovo dispositivo al successivo accesso.

- Richiedi loro di fornire una password monouso inviata via e-mail per accedere

  Utilizza questa opzione quando desideri che i codici di verifica vengano inviati agli utenti tramite e-mail. Poiché l'e-mail non è associata a un dispositivo specifico, questa opzione non soddisfa i requisiti dell'autenticazione a più fattori standard del settore. Ma migliora la sicurezza rispetto alla sola password. La verifica via e-mail verrà richiesta solo se un utente non ha registrato un dispositivo MFA. Se il metodo di autenticazione sensibile al contesto è stato abilitato, l'utente avrà la possibilità di contrassegnare come attendibile il dispositivo su cui riceve l'e-mail. Successivamente non sarà loro richiesto di verificare un codice e-mail per i futuri accessi da quella combinazione di dispositivo, browser e indirizzo IP.

  > **Note**
  >
  > Se utilizzi Active Directory come fonte di identità abilitata per IAM Identity Center, l'indirizzo e-mail sarà sempre basato sull'attributo Active Directory`email`. Le mappature personalizzate degli attributi di Active Directory non sostituiranno questo comportamento.

- Blocca il loro accesso

  Usa l'opzione Blocca il loro accesso per imporre l'uso della MFA a tutti gli utenti prima che possano accedere. AWS

  > **Important**
  >
  > Se il metodo di autenticazione è impostato su Context-aware, un utente potrebbe selezionare la casella di controllo Questo è un dispositivo affidabile nella pagina di accesso. In tal caso, all'utente non verrà richiesta l'autenticazione a più fattori anche se hai abilitato l'impostazione Blocca il loro accesso. Se desideri che questi utenti vengano avvisati, modifica il metodo di autenticazione su Always On.

- Consenti loro di accedere

  Utilizzate questa opzione per indicare che i dispositivi MFA non sono necessari per consentire agli utenti di accedere al portale di AWS accesso. Agli utenti che hanno scelto di registrare i dispositivi MFA verrà comunque richiesta l'MFA.

6. Seleziona Salvataggio delle modifiche.

Consenti agli utenti di registrare i propri dispositivi MFA

Utilizza la procedura seguente per consentire agli utenti di registrare automaticamente i propri dispositivi MFA.

Per consentire agli utenti di registrare i propri dispositivi MFA

1. Apri la console IAM Identity Center.
2. Nel riquadro di navigazione a sinistra scegliere Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Autenticazione.
4. Nella sezione Autenticazione a più fattori, scegli Configura.
5. Nella pagina Configura l'autenticazione a più fattori, in Chi può gestire i dispositivi MFA, scegli Gli utenti possono aggiungere e gestire i propri dispositivi MFA.
6. Seleziona Salvataggio delle modifiche.

> **Note**
>
> Dopo aver configurato l'autoregistrazione per i tuoi utenti, potresti voler inviare loro un link alla procedura. Registrazione di un dispositivo per l'MFA Questo argomento fornisce istruzioni su come configurare i propri dispositivi MFA.

Gestisci i dispositivi MFA in IAM Identity Center

I seguenti argomenti forniscono istruzioni per la gestione dei dispositivi MFA in IAM Identity Center.

Argomenti

- Registrazione di un dispositivo MFA
- Gestire il dispositivo MFA di un utente

Registrazione di un dispositivo MFA

Utilizza la seguente procedura per configurare un nuovo dispositivo MFA per l'accesso da parte di un utente specifico nella console IAM Identity Center. È necessario disporre dell'accesso fisico al dispositivo MFA dell'utente per registrarlo. Ad esempio, se configuri l'autenticazione a più fattori per un utente che utilizzerà un dispositivo MFA in esecuzione su uno smartphone, dovrai

accedere fisicamente allo smartphone per completare il processo di registrazione. In alternativa, puoi consentire agli utenti di configurare e gestire i propri dispositivi MFA. Per ulteriori informazioni, consulta Consenti agli utenti di registrare i propri dispositivi MFA.

Per registrare un dispositivo MFA

1. Apri la console IAM Identity Center.
2. Nel riquadro di navigazione a sinistra, seleziona Users (Utenti). Scegli un utente dall'elenco. Non selezionare la casella di controllo accanto all'utente per questo passaggio.
3. Nella pagina dei dettagli utente, scegli la scheda Dispositivi MFA, quindi scegli Registra dispositivo MFA.
4. Nella pagina Registra dispositivo MFA, seleziona uno dei seguenti tipi di dispositivi MFA e segui le istruzioni:

   - App Authenticator

     1. Nella pagina Configura l'app di autenticazione, IAM Identity Center visualizza le informazioni di configurazione per il nuovo dispositivo MFA, inclusa una grafica con codice QR. L'immagine è una rappresentazione della chiave segreta disponibile per l'immissione manuale sui dispositivi che non supportano i codici QR.
     2. Utilizzando il dispositivo MFA fisico, procedi come segue:

        a. Apri un'app di autenticazione MFA compatibile. Per un elenco delle app testate che puoi utilizzare con i dispositivi MFA, consulta. App di autenticazione virtuale Se l'app MFA supporta più account (più dispositivi MFA), scegli l'opzione per creare un nuovo account (un nuovo dispositivo MFA).

        b. Stabilisci se l'app MFA supporta i codici QR, quindi esegui una delle seguenti operazioni nella pagina Configura l'app di autenticazione:

           i. 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.

           ii. Scegli Mostra chiave segreta, quindi digita quella chiave segreta nella tua app MFA.

> **Important**
>
> Quando configuri un dispositivo MFA per IAM Identity Center, ti consigliamo di salvare una copia del codice QR o della chiave segreta in un luogo sicuro.

Questo può essere utile se l'utente assegnato perde il telefono o deve reinstallare l'app di autenticazione MFA. Se si verifica una di queste situazioni, puoi riconfigurare rapidamente l'app per utilizzare la stessa configurazione MFA. Ciò evita la necessità di creare un nuovo dispositivo MFA in IAM Identity Center per l'utente.

3. Nella pagina Configura l'app di autenticazione, in Codice di autenticazione, digita la password monouso attualmente visualizzata sul dispositivo MFA fisico.

> **Important**
>
> Invia la richiesta immediatamente dopo la generazione del codice. Se si genera il codice e poi si attende troppo a lungo per inviare la richiesta, il dispositivo MFA viene associato correttamente all'utente. 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.

4. Scegliere Assign MFA (Assegna MFA). Il dispositivo MFA può ora iniziare a generare password monouso ed è ora pronto per l'uso con. AWS

- Chiave di sicurezza

1. Nella pagina Registra la chiave di sicurezza dell'utente, segui le istruzioni fornite dal browser o dalla piattaforma.

> **Note**
>
> L'esperienza qui varia in base ai diversi sistemi operativi e browser, quindi segui le istruzioni visualizzate dal tuo browser o dalla tua piattaforma. Dopo aver registrato correttamente il dispositivo dell'utente, avrai la possibilità di associare un nome visualizzato intuitivo al dispositivo appena registrato dell'utente. Se desideri modificare questa impostazione, scegli Rinomina, inserisci il nuovo nome, quindi scegli Salva. Se hai abilitato l'opzione per consentire agli utenti di gestire i propri dispositivi, l'utente vedrà questo nome descrittivo nel portale di AWS accesso.

Gestire il dispositivo MFA di un utente

Utilizzare le seguenti procedure quando è necessario rinominare o eliminare il dispositivo MFA di un utente.

Per rinominare un dispositivo MFA

1. Apri la console IAM Identity Center.
2. Nel riquadro di navigazione a sinistra, seleziona Users (Utenti). Scegli l'utente dall'elenco. Non selezionare la casella di controllo accanto all'utente per questo passaggio.
3. Nella pagina dei dettagli utente, scegli la scheda Dispositivi MFA, seleziona il dispositivo, quindi scegli Rinomina.
4. Quando richiesto, inserisci il nuovo nome e scegli Rinomina.

Eliminazione di un dispositivo MFA

1. Apri la console IAM Identity Center.
2. Nel riquadro di navigazione a sinistra, seleziona Users (Utenti). Scegli l'utente dall'elenco.
3. Nella pagina dei dettagli utente, scegli la scheda Dispositivi MFA, seleziona il dispositivo, quindi scegli Elimina.
4. Per confermare, digita ELIMINA, quindi scegli Elimina.

Gestisci l'accesso a Account AWS

AWS IAM Identity Center è integrato con AWS Organizations, il che consente di gestire centralmente le autorizzazioni su più account Account AWS senza configurare manualmente ciascuno dei propri account. È possibile definire le autorizzazioni e assegnarle agli utenti della forza lavoro per controllarne l'accesso a determinati utenti. Account AWS

Account AWS tipi

Esistono due tipi di Account AWS ingresso AWS Organizations:

- Account di gestione: viene utilizzato per creare l'organizzazione. Account AWS
- Account dei membri: Account AWS il resto appartiene a un'organizzazione.

Per ulteriori informazioni sui Account AWS tipi, vedere AWS Organizations Terminologia e concetti nella Guida per l'AWS Organizations utente.

Puoi anche scegliere di registrare un account membro come amministratore delegato per IAM Identity Center. Gli utenti di questo account possono eseguire la maggior parte delle attività amministrative di IAM Identity Center. Per ulteriori informazioni, consulta Amministrazione delegata.

Per ogni attività e tipo di account, la tabella seguente indica se l'attività amministrativa di IAM Identity Center può essere eseguita dagli utenti dell'account.

Attività amministrative di IAM Identity Center	Account membro	Account amministratore delegato	Gestione dell'account
Leggi utenti o gruppi (lettura del gruppo stesso e dei membri del gruppo)	 Sì	 Sì	 Sì
Aggiungere, modificare o eliminare utenti o gruppi	 No	 Sì	 Sì

Attività amministrative di IAM Identity Center	Account membro	Account amministratore delegato	Gestione dell'account
Abilita o disabilita l'accesso degli utenti	No	Sì	Sì
Abilita, disabilita o gestisci gli attributi in entrata	No	Sì	Sì
Modifica o gestisci le fonti di identità	No	Sì	Sì
Creare, modificare o eliminare applicazioni	No	Sì	Sì
Configurazione MFA	No	Sì	Sì
Gestisci i set di autorizzazioni non forniti nell'account di gestione	No	Sì	Sì
Gestisci i set di autorizzazioni forniti nell'account di gestione	No	No	Sì

Attività amministrative di IAM Identity Center	Account membro	Account amministratore delegato	Gestione dell'account
Abilita IAM Identity Center	 No	 No	 Sì
Elimina la configurazione di IAM Identity Center	 No	 No	 Sì
Abilita o disabilita l'accesso degli utenti nell'account di gestione	 No	 No	 Sì
Registrare o annullare la registrazione di un account membro come amministratore delegato	 No	 No	 Sì

Account AWS Assegnazione dell'accesso

È possibile utilizzare i set di autorizzazioni per semplificare il modo in cui si assegna l'accesso a Account AWS utenti e gruppi dell'organizzazione. I set di autorizzazioni sono archiviati in IAM Identity Center e definiscono il livello di accesso che utenti e gruppi hanno a un Account AWS. Puoi creare un singolo set di autorizzazioni e assegnarlo a più set Account AWS all'interno della tua organizzazione. È inoltre possibile assegnare più set di autorizzazioni allo stesso utente.

Per ulteriori informazioni sui set di autorizzazioni, consulta Crea, gestisci ed elimina i set di autorizzazioni.

> **Note**
>
> Puoi anche assegnare ai tuoi utenti l'accesso Single Sign-On alle applicazioni. Per informazioni, consulta Gestire l'accesso alle applicazioni.

Esperienza dell'utente finale

Il portale di AWS accesso fornisce agli utenti di IAM Identity Center l'accesso Single Sign-On a tutti i loro assegnati Account AWS e alle applicazioni tramite un portale web. Il portale di AWS accesso è diverso dal AWS Management Console, che è una raccolta di console di servizio per la gestione delle risorse. AWS

Quando si crea un set di autorizzazioni, il nome specificato per il set di autorizzazioni viene visualizzato nel portale di AWS accesso come ruolo disponibile. Gli utenti AWS accedono al portale di accesso, ne scelgono uno Account AWS e quindi scelgono il ruolo. Dopo aver scelto il ruolo, possono accedere ai AWS servizi utilizzando AWS Management Console o recuperare le credenziali temporanee per accedere ai AWS servizi in modo programmatico.

Per aprire AWS Management Console o recuperare le credenziali temporanee per l'accesso AWS programmatico, gli utenti completano i seguenti passaggi:

1. Gli utenti aprono una finestra del browser e utilizzano l'URL di accesso fornito per accedere al portale di accesso. AWS
2. Utilizzando le proprie credenziali di directory, accedono al portale di AWS accesso.
3. Dopo l'autenticazione, nella pagina del portale di AWS accesso, scelgono la scheda Account per visualizzare l'elenco Account AWS a cui hanno accesso.
4. Gli utenti scelgono quindi Account AWS quello che desiderano utilizzare.
5. Sotto il nome di Account AWS, tutti i set di autorizzazioni a cui sono assegnati gli utenti vengono visualizzati come ruoli disponibili. Ad esempio, se hai assegnato un utente `john_stiles` al set di `PowerUser` autorizzazioni, il ruolo viene visualizzato nel portale di AWS accesso come`PowerUser/john_stiles`. Gli utenti a cui sono assegnati più set di autorizzazioni scelgono il ruolo da utilizzare. Gli utenti possono scegliere il proprio ruolo per accedere a AWS Management Console.
6. Oltre al ruolo, gli utenti del portale di AWS accesso possono recuperare credenziali temporanee per l'accesso da riga di comando o programmatico scegliendo le chiavi di accesso.

Per step-by-step indicazioni da fornire agli utenti della forza lavoro, consulta e. Utilizzo del portale di AWS accesso Ottenere le credenziali utente di IAM Identity Center per gli SDK AWS CLI or AWS

Far rispettare e limitare l'accesso

Quando abiliti IAM Identity Center, IAM Identity Center crea un ruolo collegato al servizio. Puoi anche utilizzare le policy di controllo dei servizi (SCP).

Delegare e far rispettare l'accesso

Un ruolo collegato al servizio è un tipo di ruolo IAM collegato direttamente a un servizio. AWS Dopo aver abilitato IAM Identity Center, IAM Identity Center può creare un ruolo collegato ai servizi in ciascuno Account AWS dei membri dell'organizzazione. Questo ruolo fornisce autorizzazioni predefinite che consentono a IAM Identity Center di delegare e stabilire quali utenti hanno accesso Single Sign-On a determinati membri dell'organizzazione. Account AWS AWS OrganizationsÈ necessario assegnare a uno o più utenti l'accesso a un account per utilizzare questo ruolo. Per ulteriori informazioni, consulta Ruoli collegati ai servizi e Utilizzo di ruoli collegati ai servizi per IAM Identity Center.

Limitazione dell'accesso all'archivio di identità dagli account dei membri

Per il servizio di archiviazione delle identità utilizzato da IAM Identity Center, gli utenti che hanno accesso a un account membro possono utilizzare azioni API che richiedono autorizzazioni di lettura. Gli account dei membri hanno accesso alle azioni di lettura sugli spazi dei nomi sso-directory e identitystore. Per ulteriori informazioni, vedere Azioni, risorse e chiavi di condizione per la AWS IAM Identity Center directory e Azioni, risorse e chiavi di condizione per AWS Identity Store nel Service Authorization Reference.

Per impedire agli utenti degli account dei membri di utilizzare le operazioni API nell'archivio di identità, puoi allegare una policy di controllo del servizio (SCP). Un SCP è un tipo di politica organizzativa che è possibile utilizzare per gestire le autorizzazioni all'interno dell'organizzazione. L'esempio seguente SCP impedisce agli utenti degli account dei membri di accedere a qualsiasi operazione API nell'archivio di identità.

```
        {
            "Sid": "ExplicitlyBlockIdentityStoreAccess",
            "Effect": "Deny",
            "Action": "identitystore:*", "sso-directory:*"],
            "Resource": "*"
```

```
        }
```

> **Note**
>
> La limitazione dell'accesso agli account dei membri potrebbe compromettere la funzionalità delle applicazioni abilitate per IAM Identity Center.

Per ulteriori informazioni, consulta Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .

Amministrazione delegata

L'amministrazione delegata offre agli utenti assegnati in un account membro registrato un modo pratico per eseguire la maggior parte delle attività amministrative di IAM Identity Center. Quando abiliti IAM Identity Center, per impostazione predefinita, l'istanza IAM Identity Center viene AWS Organizations creata nell'account di gestione. Originariamente è stato progettato in questo modo per consentire a IAM Identity Center di effettuare il provisioning, il de-provisioning e l'aggiornamento dei ruoli in tutti gli account dei membri dell'organizzazione. Anche se l'istanza IAM Identity Center deve sempre risiedere nell'account di gestione, puoi scegliere di delegare l'amministrazione di IAM Identity Center a un account membro in AWS Organizations, estendendo così la capacità di gestire IAM Identity Center dall'esterno dell'account di gestione.

L'abilitazione dell'amministrazione delegata offre i seguenti vantaggi:

- Riduce al minimo il numero di persone che richiedono l'accesso all'account di gestione per contribuire a mitigare i problemi di sicurezza
- Consente ad amministratori selezionati di assegnare utenti e gruppi alle applicazioni e agli account dei membri dell'organizzazione

Per ulteriori informazioni su come funziona IAM Identity Center AWS Organizations, consulta. Gestisci l'accesso a Account AWS Per ulteriori informazioni e per esaminare uno scenario aziendale di esempio che mostra come configurare l'amministrazione delegata, consulta Guida introduttiva all'amministrazione delegata di IAM Identity Center nel AWS Security Blog.

Argomenti

- Best practice

Best practice

Ecco alcune best practice da considerare prima di configurare l'amministrazione delegata.

- Concedi il privilegio minimo all'account di gestione: sapendo che l'account di gestione è un account con privilegi elevati e per rispettare il principio del privilegio minimo, consigliamo vivamente di limitare l'accesso all'account di gestione al minor numero di persone possibile. La funzionalità di amministratore delegato ha lo scopo di ridurre al minimo il numero di persone che richiedono l'accesso all'account di gestione.
- Crea set di autorizzazioni da utilizzare solo nell'account di gestione: ciò semplifica l'amministrazione dei set di autorizzazioni personalizzati solo per gli utenti che accedono all'account di gestione e aiuta a differenziarli dai set di autorizzazioni gestiti dall'account amministratore delegato.
- Considera la tua posizione in Active Directory: se prevedi di utilizzare Active Directory come fonte di identità di IAM Identity Center, individua la directory nell'account membro in cui hai abilitato la funzionalità di amministratore delegato di IAM Identity Center. Se decidi di modificare l'origine dell'identità di IAM Identity Center da qualsiasi altra fonte ad Active Directory o di cambiarla da Active Directory a qualsiasi altra fonte, la directory deve risiedere (essere di proprietà di) l'account membro amministratore delegato di IAM Identity Center, se esistente; in caso contrario, deve essere nell'account di gestione.
- Crea assegnazioni utente solo nell'account di gestione: l'amministratore delegato non può modificare i set di autorizzazioni forniti nell'account di gestione. Tuttavia, gli amministratori delegati possono aggiungere, modificare ed eliminare gruppi e assegnazioni di gruppo.

Prerequisiti

Prima di poter registrare un account come amministratore delegato, è necessario disporre del seguente ambiente:

- AWS Organizations deve essere abilitato e configurato con almeno un account membro oltre all'account di gestione predefinito.

- Se l'origine dell'identità è impostata su Active Directory, la Sincronizzazione AD configurabile con IAM Identity Center funzionalità deve essere abilitata.

Registra un account membro

Per configurare l'amministrazione delegata, devi prima registrare un account membro nella tua organizzazione come amministratore delegato. Gli utenti di quell'account membro che dispongono di autorizzazioni sufficienti avranno accesso amministrativo a IAM Identity Center. Dopo che un account membro è stato registrato con successo per l'amministrazione delegata, viene denominato account amministratore delegato. Per ulteriori informazioni sulle attività che l'account amministratore delegato può eseguire, consulta. Account AWS tipi

IAM Identity Center supporta la registrazione di un solo account membro come amministratore delegato alla volta. Puoi registrare un account membro solo dopo aver effettuato l'accesso con le credenziali dell'account di gestione.

Utilizza la seguente procedura per concedere l'accesso amministrativo a IAM Identity Center registrando un account membro specifico nella tua AWS organizzazione come amministratore delegato.

> **Important**
>
> Questa operazione delega l'accesso amministrativo di IAM Identity Center agli utenti amministratori di questo account membro. Tutti gli utenti che dispongono di autorizzazioni sufficienti per questo account amministratore delegato possono eseguire tutte le attività amministrative di IAM Identity Center dall'account, ad eccezione di:
>
> - Abilitazione di IAM Identity Center
> - Eliminazione delle configurazioni di IAM Identity Center
> - Gestione dei set di autorizzazioni forniti nell'account di gestione
> - Registrazione o cancellazione degli account di altri membri come amministratori delegati
> - Abilitazione o disabilitazione dell'accesso utente nell'account di gestione
>
> L'amministratore delegato può modificare l'appartenenza al gruppo.

Per registrare un account membro

1. Accedi AWS Management Console utilizzando le credenziali del tuo account di gestione in AWS Organizations. Le credenziali dell'account di gestione sono necessarie per eseguire l'RegisterDelegatedAdministratorAPI.
2. Seleziona la regione in cui è abilitato IAM Identity Center, quindi apri la console IAM Identity Center.
3. Scegli Impostazioni, quindi seleziona la scheda Gestione.
4. Nella sezione Amministratore delegato, scegli Registra account.
5. Nella pagina Registra amministratore delegato, seleziona l'account Account AWS che desideri registrare, quindi scegli Registra account.

Annullamento della registrazione di un account membro

Puoi annullare la registrazione di un account membro solo dopo aver effettuato l'accesso con le credenziali dell'account di gestione.

Utilizza la seguente procedura per rimuovere l'accesso amministrativo da IAM Identity Center annullando la registrazione di un account membro AWS dell'organizzazione che era stato precedentemente designato come amministratore delegato.

> **Important**
>
> Quando annulli la registrazione di un account, rimuovi di fatto la possibilità per tutti gli utenti amministratori di gestire IAM Identity Center da quell'account. Di conseguenza, non possono più amministrare le identità di IAM Identity Center, la gestione degli accessi, l'autenticazione o l'accesso alle applicazioni da questo account. Questa operazione non influirà sulle autorizzazioni o sulle assegnazioni configurate in IAM Identity Center e pertanto non avrà alcun impatto sugli utenti finali, che continueranno ad avere accesso alle loro app e Account AWS dall'interno del portale di accesso. AWS

Per annullare la registrazione di un account membro

1. Accedi AWS Management Console utilizzando le credenziali del tuo account di gestione in. AWS Organizations Le credenziali dell'account di gestione sono necessarie per eseguire l'DeregisterDelegatedAdministratorAPI.

2. Seleziona la regione in cui è abilitato IAM Identity Center, quindi apri la console IAM Identity Center.
3. Scegli Impostazioni, quindi seleziona la scheda Gestione.
4. Nella sezione Amministratore delegato, scegli Annulla registrazione account.
5. Nella finestra di dialogo Annulla registrazione account, esamina le implicazioni sulla sicurezza, quindi inserisci il nome dell'account membro per confermare di aver compreso.
6. Scegli Annulla registrazione account.

Visualizza quale account membro è stato registrato come amministratore delegato

Utilizza la seguente procedura per trovare quale account membro del tuo AWS Organizations è stato configurato come amministratore delegato per IAM Identity Center.

Per visualizzare il tuo account di membro registrato

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella sezione Dettagli, individua il nome dell'account registrato in Amministratore delegato. È inoltre possibile individuare queste informazioni selezionando la scheda Gestione e visualizzandole nella sezione Amministratore delegato.

Accesso temporaneo elevato

Ogni accesso al tuo Account AWS implica un certo livello di privilegio. Le operazioni sensibili, come la modifica della configurazione per una risorsa di alto valore, ad esempio un ambiente di produzione, richiedono un trattamento speciale a causa della portata e del potenziale impatto. L'accesso temporaneo elevato (noto anche come just-in-time accesso) è un modo per richiedere, approvare e tenere traccia dell'uso di un'autorizzazione per eseguire un'attività specifica in un periodo di tempo specificato. L'accesso temporaneo con privilegi elevati integra altre forme di controllo degli accessi, come i set di autorizzazioni e l'autenticazione a più fattori.

AWS IAM Identity Center offre le seguenti opzioni per la gestione temporanea degli accessi elevati in diversi ambienti aziendali e tecnici:

- Soluzioni gestite e supportate dai fornitori: AWS ha convalidato le integrazioni IAM Identity Center di offerte di partner selezionati e ne ha valutato le funzionalità rispetto a una serie comune di requisiti dei clienti. Scegli la soluzione più adatta al tuo scenario e segui le indicazioni del provider per abilitare la funzionalità con IAM Identity Center.
- Gestione e supporto automatici: questa opzione fornisce un punto di partenza se sei interessato a un accesso temporaneo elevato AWS solo a un utente e puoi implementare, personalizzare e mantenere la funzionalità da solo. Per ulteriori informazioni, consulta Temporary Elevated Access Management (TEAM).

Partner di AWS sicurezza convalidati per un accesso temporaneo elevato

AWS I partner di sicurezza utilizzano approcci diversi per soddisfare una serie comune di requisiti di accesso temporanei elevati. Ti consigliamo di esaminare attentamente ogni soluzione partner, in modo da poter scegliere quella più adatta alle tue esigenze e preferenze, tra cui la tua attività, l'architettura del tuo ambiente cloud e il tuo budget.

> **Note**
>
> Per il disaster recovery, ti consigliamo di configurare l'accesso di emergenza a AWS Management Console prima che si verifichi un'interruzione.

AWS Identity ha convalidato le funzionalità e l'integrazione con IAM Identity Center per le seguenti just-in-time offerte dei partner di AWS sicurezza:

- CyberArk Secure Cloud Access— Parte delCyberArk Identity Security Platform, questa offerta fornisce un accesso elevato on-demand ad AWS ambienti multi-cloud. Le approvazioni vengono gestite tramite l'integrazione con ITSM o con strumenti. ChatOps Tutte le sessioni possono essere registrate per l'audit e la conformità.
- Tenable (previously Ermetic)— La Tenable piattaforma include la fornitura di just-in-time accessi privilegiati per le operazioni amministrative in ambienti AWS multi-cloud. I log delle sessioni di tutti gli ambienti cloud, inclusi i registri di AWS CloudTrail accesso, sono disponibili in un'unica interfaccia per l'analisi e l'audit. La funzionalità si integra con strumenti aziendali e di sviluppo come Slack e Microsoft Teams.
- OktaRichieste di accesso: parte di Okta Identity Governance, consente di configurare un flusso di lavoro di richiesta di just-in-time accesso utilizzando Okta un provider di identità (IdP) esterno di IAM Identity Center e i set di autorizzazioni IAM Identity Center.

Questo elenco verrà aggiornato per AWS convalidare le funzionalità di soluzioni partner aggiuntive e l'integrazione di tali soluzioni con IAM Identity Center.

> **Note**
>
> Se utilizzi politiche basate sulle risorse, Amazon Elastic Kubernetes Service (Amazon EKS) o (AWS Key Management Service Riferimento ai set di autorizzazioni nelle politiche delle risorse, Amazon EKS e AWS KMS)AWS KMS, consulta prima di scegliere la soluzione. just-in-time

Capacità di accesso temporaneo elevato valutate per la convalida dei partner AWS

AWS Identity ha verificato che le funzionalità di accesso temporaneo elevato offerte da e Access CyberArk Secure Cloud AccessRequests Tenablesoddisfano i Okta seguenti requisiti comuni dei clienti:

- Gli utenti possono richiedere l'accesso a un set di autorizzazioni per un periodo di tempo specificato dall'utente, specificando l' AWS account, il set di autorizzazioni, il periodo di tempo e il motivo.
- Gli utenti possono ricevere lo stato di approvazione per la loro richiesta.
- Gli utenti non possono richiamare una sessione con un determinato ambito, a meno che non esista una richiesta approvata con lo stesso ambito e non richiamino la sessione durante il periodo di tempo approvato.
- Esiste un modo per specificare chi può approvare le richieste.
- Gli approvatori non possono approvare le proprie richieste.
- Gli approvatori dispongono di un elenco di richieste in sospeso, approvate e rifiutate e possono esportarlo per i revisori.
- Gli approvatori possono approvare e rifiutare le richieste in sospeso.
- Gli approvatori possono aggiungere una nota che spiega la loro decisione.
- Gli approvatori possono revocare una richiesta approvata, impedendo l'uso futuro dell'accesso elevato.

> **Note**
>
> Se un utente ha effettuato l'accesso con accesso elevato quando una richiesta approvata viene revocata, la sua sessione rimane attiva fino a un'ora dopo la revoca dell'approvazione. Per informazioni sulle sessioni di autenticazione, consulta. Autenticazione

- Le azioni e le approvazioni degli utenti sono disponibili per la verifica.

Accesso Single Sign-On a Account AWS

È possibile assegnare agli utenti della directory connessa le autorizzazioni all'account di gestione o agli account dei membri dell'organizzazione in AWS Organizations base alle funzioni lavorative comuni. In alternativa, è possibile utilizzare autorizzazioni personalizzate per soddisfare i requisiti specifici di sicurezza. Ad esempio, puoi concedere agli amministratori di database ampie autorizzazioni ad Amazon RDS negli account di sviluppo, ma limitare le loro autorizzazioni negli account di produzione. IAM Identity Center configura automaticamente tutte le autorizzazioni utente necessarie. Account AWS

> **Note**
>
> Potrebbe essere necessario concedere a utenti o gruppi le autorizzazioni per operare nell' AWS Organizations account di gestione. Poiché si tratta di un account altamente privilegiato, ulteriori restrizioni di sicurezza richiedono che tu disponga della FullAccess policy IAM o di autorizzazioni equivalenti prima di poterlo configurare. Queste restrizioni di sicurezza aggiuntive non sono richieste per nessuno degli account membri dell'organizzazione. AWS

Assegna l'accesso utente a Account AWS

Utilizzare la procedura seguente per assegnare l'accesso Single Sign-On a utenti e gruppi nella directory connessa e utilizzare i set di autorizzazioni per determinarne il livello di accesso.

Per verificare l'accesso esistente di utenti e gruppi, vedere. Visualizza le assegnazioni di utenti e gruppi

> **Note**
>
> Per semplificare l'amministrazione delle autorizzazioni di accesso, ti consigliamo di assegnare l'accesso direttamente ai gruppi anziché ai singoli utenti. I gruppi ti consentono di concedere o negare autorizzazioni a più utenti senza dover applicare tali autorizzazioni a ogni singola persona. Se un utente passa a un'altra organizzazione, devi solo spostare tale utente in un altro gruppo affinché riceva automaticamente le autorizzazioni necessarie per la nuova organizzazione.

Per assegnare l'accesso a utenti o gruppi a Account AWS

1. Apri la console IAM Identity Center.

   > **Note**
   >
   > Assicurati che la console IAM Identity Center utilizzi la regione in cui si trova la tua AWS Managed Microsoft AD directory prima di passare alla fase successiva.

2. Nel pannello di navigazione, in Autorizzazioni multiaccount, scegli. Account AWS
3. Nella Account AWSpagina viene visualizzato un elenco ad albero della tua organizzazione. Seleziona la casella di controllo accanto a una o più Account AWS a cui desideri assegnare l'accesso Single Sign-On.

   > **Note**
   >
   > Puoi selezionarne fino a 10 Account AWS alla volta per set di autorizzazioni quando assegni l'accesso Single Sign-On a utenti e gruppi. Per assegnare più di 10 utenti e gruppi Account AWS allo stesso set di utenti e gruppi, ripeti questa procedura come richiesto per gli account aggiuntivi. Quando richiesto, seleziona gli stessi utenti, gruppi e set di autorizzazioni.

4. Scegli Assegna utenti o gruppi.
5. Per il Passaggio 1: Seleziona utenti e gruppi, nella pagina Assegna utenti e gruppi a "***AWS-account-name***", procedi come segue:

   1. Nella scheda Utenti, seleziona uno o più utenti a cui concedere l'accesso Single Sign-On.

Per filtrare i risultati, inizia a digitare il nome dell'utente che desideri nella casella di ricerca.

2. Nella scheda Gruppi, seleziona uno o più gruppi a cui concedere l'accesso Single Sign-On.

   Per filtrare i risultati, inizia a digitare il nome del gruppo che desideri nella casella di ricerca.

3. Per visualizzare gli utenti e i gruppi selezionati, scegli il triangolo laterale accanto a Utenti e gruppi selezionati.
4. Dopo aver confermato che sono stati selezionati gli utenti e i gruppi corretti, scegli Avanti.

6. Per il passaggio 2: selezione dei set di autorizzazioni, nella pagina Assegna set di autorizzazioni a "***AWS-account-name***", procedi come segue:

   1. Seleziona uno o più set di autorizzazioni. Se necessario, è possibile creare e selezionare nuovi set di autorizzazioni.
      - Per selezionare uno o più set di autorizzazioni esistenti, in Set di autorizzazioni, seleziona i set di autorizzazioni che desideri applicare agli utenti e ai gruppi selezionati nel passaggio precedente.
      - Per creare uno o più nuovi set di autorizzazioni, scegli Crea set di autorizzazioni e segui i passaggi indicatiCrea un set di autorizzazioni.. Dopo aver creato i set di autorizzazioni che desideri applicare, nella console IAM Identity Center, torna Account AWSe segui le istruzioni fino a raggiungere la Fase 2: Seleziona i set di autorizzazioni. Una volta raggiunto questo passaggio, seleziona i nuovi set di autorizzazioni che hai creato e procedi al passaggio successivo di questa procedura.
   2. Dopo aver confermato che sono stati selezionati i set di autorizzazioni corretti, scegli Avanti.

7. Per la Fase 3: Revisione e invio, nella pagina Rivedi e invia le assegnazioni a "***AWS-account-name***", procedi come segue:

   1. Rivedi gli utenti, i gruppi e i set di autorizzazioni selezionati.
   2. Dopo aver verificato che siano selezionati gli utenti, i gruppi e i set di autorizzazioni corretti, scegli Invia.

      > **Important**
      >
      > Il completamento del processo di assegnazione di utenti e gruppi potrebbe richiedere alcuni minuti. Lascia aperta questa pagina fino al completamento del processo.

> **Note**
>
> Potrebbe essere necessario concedere a utenti o gruppi le autorizzazioni per operare nell'account di AWS Organizations gestione. Poiché si tratta di un account altamente privilegiato, ulteriori restrizioni di sicurezza richiedono che tu disponga della FullAccess policy IAM o di autorizzazioni equivalenti prima di poterlo configurare. Queste restrizioni di sicurezza aggiuntive non sono richieste per nessuno degli account membri dell'organizzazione. AWS

Rimuovi l'accesso a utenti e gruppi

Utilizzare questa procedura per rimuovere l'accesso Single Sign-On a uno Account AWS o più utenti e gruppi nella directory connessa.

Per rimuovere l'accesso di utenti e gruppi a un Account AWS

1. Apri la console IAM Identity Center.
2. Nel riquadro di navigazione, in Autorizzazioni multiaccount, scegli. Account AWS
3. Nella Account AWSpagina viene visualizzato un elenco ad albero della tua organizzazione. Seleziona il nome dell'account Account AWS che contiene gli utenti e i gruppi per i quali desideri rimuovere l'accesso Single Sign-On.
4. Nella pagina Panoramica relativa a Account AWS, in Utenti e gruppi assegnati, seleziona il nome di uno o più utenti o gruppi e scegli Rimuovi accesso.
5. Nella finestra di dialogo Rimuovi accesso, conferma che i nomi degli utenti o dei gruppi siano corretti e scegli Rimuovi accesso.

Revoca le sessioni di ruolo IAM attive create dai set di autorizzazioni

Di seguito è riportata una procedura generale per revocare una sessione attiva del set di autorizzazioni per un utente IAM Identity Center. La procedura presuppone che si desideri rimuovere tutti gli accessi per un utente che ha credenziali compromesse o per un malintenzionato presente nel sistema. Il prerequisito è aver seguito le indicazioni contenute in. Preparati a revocare una sessione di ruolo IAM attiva creata da un set di autorizzazioni Partiamo dal presupposto che la politica di negazione totale sia presente in una politica di controllo del servizio (SCP).

> **Note**
>
> AWS consiglia di creare un'automazione per gestire tutti i passaggi tranne le operazioni relative alla sola console.

1. Ottieni l'ID utente della persona a cui devi revocare l'accesso. Puoi utilizzare le API dell'archivio di identità per trovare l'utente in base al suo nome utente.
2. Aggiorna la politica Deny per aggiungere l'ID utente dal passaggio 1 della tua policy di controllo del servizio (SCP). Dopo aver completato questo passaggio, l'utente di destinazione perde l'accesso e non è in grado di intraprendere azioni con i ruoli interessati dalla policy.
3. Rimuove tutte le assegnazioni dei set di autorizzazioni per l'utente. Se l'accesso viene assegnato tramite l'appartenenza ai gruppi, rimuovi l'utente da tutti i gruppi e da tutte le assegnazioni dirette dei set di autorizzazioni. Questo passaggio impedisce all'utente di assumere ruoli IAM aggiuntivi. Se un utente ha una sessione attiva del portale di AWS accesso e lo disabiliti, può continuare ad assumere nuovi ruoli fino a quando non rimuovi il suo accesso.
4. Se utilizzi un provider di identità (IdP) o Microsoft Active Directory come origine di identità, disabilita l'utente nell'origine dell'identità. La disabilitazione dell'utente impedisce la creazione di sessioni aggiuntive del portale di AWS accesso. Usa la documentazione dell'API IdP o Microsoft Active Directory per scoprire come automatizzare questo passaggio. Se utilizzi la directory IAM Identity Center come fonte di identità, non disabilitare ancora l'accesso degli utenti. Disabiliterai l'accesso degli utenti nel passaggio 6.
5. Nella console IAM Identity Center, trova l'utente ed elimina la sua sessione attiva.

    a. Scegliere Users (Utenti).

    b. Scegli l'utente di cui desideri eliminare la sessione attiva.

    c. Nella pagina dei dettagli dell'utente, scegli la scheda Sessioni attive.

    d. Seleziona le caselle di controllo accanto alle sessioni che desideri eliminare e scegli Elimina sessione.

    Ciò garantisce che la sessione del portale di AWS accesso dell'utente si interrompa entro circa 60 minuti. Scopri la durata della sessione.
6. Nella console IAM Identity Center, disabilita l'accesso degli utenti.

    a. Scegliere Users (Utenti).

b. Scegli l'utente di cui desideri disabilitare l'accesso.

c. Nella pagina dei dettagli dell'utente, espandi Informazioni generali e scegli il pulsante Disabilita l'accesso utente per impedire ulteriori accessi dell'utente.

7. Lascia in vigore la politica di rifiuto per almeno 12 ore. In caso contrario, l'utente con una sessione attiva del ruolo IAM avrà ripristinato le azioni con il ruolo IAM. Se attendi 12 ore, le sessioni attive scadono e l'utente non potrà più accedere al ruolo IAM.

> **Important**
>
> Se disabiliti l'accesso di un utente prima di interrompere la sessione utente (hai completato il passaggio 6 senza completare il passaggio 5), non puoi più interrompere la sessione utente tramite la console IAM Identity Center. Se disabiliti inavvertitamente l'accesso utente prima di interrompere la sessione utente, puoi riabilitare l'utente, interrompere la sua sessione e quindi disabilitare nuovamente il suo accesso.

Ora puoi modificare le credenziali dell'utente se la sua password è stata compromessa e ripristinare le sue assegnazioni.

Delega chi può assegnare l'accesso Single Sign-On a utenti e gruppi nell'account di gestione

L'assegnazione dell'accesso Single Sign-On all'account di gestione utilizzando la console IAM Identity Center è un'azione privilegiata. Per impostazione predefinita, solo uno Utente root dell'account AWS o un utente a cui sono associate le policy AWSSSOMasterAccountAdministratore le policy IAMFullAccess AWS gestite possono assegnare l'accesso Single Sign-On all'account di gestione. Le IAMFullAccesspolicy AWSSSOMasterAccountAdministratore gestiscono l'accesso Single Sign-On all'account di gestione all'interno di un'organizzazione. AWS Organizations

Utilizza i seguenti passaggi per delegare le autorizzazioni per gestire l'accesso Single Sign-On a utenti e gruppi nella tua directory.

Per concedere le autorizzazioni per gestire l'accesso Single Sign-On a utenti e gruppi presenti nella tua directory

1. Accedi alla console IAM Identity Center come utente root dell'account di gestione o con un altro utente che dispone delle autorizzazioni di amministratore per l'account di gestione.

2. Segui i passaggi indicati Crea un set di autorizzazioni. per creare un set di autorizzazioni, quindi procedi come segue:

   1. Nella pagina Crea nuovo set di autorizzazioni, seleziona la casella di controllo Crea un set di autorizzazioni personalizzato, quindi scegli Avanti: dettagli.
   2. Nella pagina Crea nuovo set di autorizzazioni, specifica un nome per il set di autorizzazioni personalizzato e, facoltativamente, una descrizione. Se necessario, modificate la durata della sessione e specificate un URL dello stato di inoltro.

      > **Note**
      >
      > Per l'URL dello stato di inoltro, è necessario specificare un URL che si trova in. AWS Management Console Per esempio:
      > **`https://console.aws.amazon.com/ec2/`**
      > Per ulteriori informazioni, consulta Imposta lo stato del relè.

   3. In Quali politiche desideri includere nel tuo set di autorizzazioni? , seleziona la casella di controllo Allega politiche AWS gestite.
   4. Nell'elenco delle politiche IAM, scegli sia le AWSSSOMasterAccountAdministratorpolitiche gestite che quelle IAMFullAccess AWS gestite. Queste politiche concedono le autorizzazioni a tutti gli utenti e i gruppi a cui verrà assegnato l'accesso a questo set di autorizzazioni in futuro.
   5. Scegli Successivo: Tag.
   6. In Aggiungi tag (opzionale), specifica i valori per Chiave e Valore (opzionale), quindi scegli Avanti: revisione. Per ulteriori informazioni sui tag, consulta Tagging delle risorse AWS IAM Identity Center.
   7. Controlla le selezioni effettuate, quindi scegli Crea.

3. Segui i passaggi indicati Assegna l'accesso utente a Account AWS per assegnare gli utenti e i gruppi appropriati al set di autorizzazioni appena creato.
4. Comunica quanto segue agli utenti assegnati: quando accedono al portale di AWS accesso e scelgono la scheda Account, devono scegliere il nome del ruolo appropriato da autenticare con le autorizzazioni che hai appena delegato.

Set di autorizzazioni

Un set di autorizzazioni è un modello creato e gestito che definisce una raccolta di una o più politiche IAM. I set di autorizzazioni semplificano l'assegnazione dell' Account AWS accesso a utenti e gruppi dell'organizzazione. Ad esempio, è possibile creare un set di autorizzazioni di amministratore del database che include le politiche per l'amministrazione dei servizi AWS RDS, DynamoDB e Aurora e utilizzare quel set di autorizzazioni singolo per concedere l'accesso a un elenco di oggetti all'interno dell'organizzazione per gli amministratori del database Account AWS .AWS

IAM Identity Center assegna l'accesso a un utente o a un gruppo in uno o più set di autorizzazioni. Account AWS Quando si assegna un set di autorizzazioni, IAM Identity Center crea i ruoli IAM corrispondenti controllati da IAM Identity Center in ciascun account e associa le politiche specificate nel set di autorizzazioni a tali ruoli. IAM Identity Center gestisce il ruolo e consente agli utenti autorizzati che hai definito di assumere il ruolo, utilizzando l'IAM Identity Center User Portal o la AWS CLI. Man mano che modifichi il set di autorizzazioni, IAM Identity Center garantisce che le politiche e i ruoli IAM corrispondenti vengano aggiornati di conseguenza.

Puoi aggiungere politiche AWS gestite, politiche gestite dai clienti, politiche in linea e politiche AWS gestite per le funzioni lavorative ai tuoi set di autorizzazioni. Puoi anche assegnare una politica AWS gestita o una politica gestita dal cliente come limite di autorizzazioni.

Per creare un set di autorizzazioni, vedere. Crea, gestisci ed elimina i set di autorizzazioni

Argomenti

Autorizzazioni predefinite

È possibile creare un set di autorizzazioni predefinito con AWS politiche gestite.

Quando si crea un set di autorizzazioni con autorizzazioni predefinite, si sceglie una politica da un elenco di AWS politiche gestite. All'interno delle politiche disponibili, puoi scegliere tra le politiche di autorizzazione comuni e le politiche delle funzioni Job.

Politiche di autorizzazione comuni

Scegliete da un elenco di politiche AWS gestite che consentono l'accesso completo alle risorse Account AWS. Puoi aggiungere una delle seguenti politiche:

- AdministratorAccess
- PowerUserAccess
- ReadOnlyAccess
- ViewOnlyAccess

Politiche relative alle funzioni lavorative

Scegliete da un elenco di politiche AWS gestite che consentono di accedere alle risorse della vostra azienda Account AWS che potrebbero essere pertinenti per un lavoro all'interno dell'organizzazione. Puoi aggiungere una delle seguenti politiche:

- Billing
- DataScientist
- DatabaseAdministrator
- NetworkAdministrator
- SecurityAudit
- SupportUser
- SystemAdministrator

Per descrizioni dettagliate delle politiche di autorizzazione comuni e delle politiche relative alle funzioni lavorative disponibili, consulta le politiche AWS gestite per le funzioni lavorative nella guida per l'AWS Identity and Access Management utente.

Per istruzioni su come creare un set di autorizzazioni, vedereCrea, gestisci ed elimina i set di autorizzazioni.

Autorizzazioni personalizzate

Puoi creare un set di autorizzazioni con autorizzazioni personalizzate, combinando tutte le politiche AWS gestite e gestite dai clienti presenti in AWS Identity and Access Management (IAM) con le politiche in linea. Puoi anche includere i limiti delle autorizzazioni, impostando le autorizzazioni massime possibili che altre politiche possono concedere agli utenti del tuo set di autorizzazioni.

Per istruzioni su come creare un set di autorizzazioni, vedere. Crea, gestisci ed elimina i set di autorizzazioni

Tipi di policy che puoi allegare al tuo set di autorizzazioni

Argomenti

- Policy inline
- AWS politiche gestite
- Policy gestite dal cliente
- Limiti delle autorizzazioni

Policy inline

È possibile allegare una politica in linea a un set di autorizzazioni. Una policy in linea è un blocco di testo formattato come policy IAM che aggiungi direttamente al tuo set di autorizzazioni. Puoi incollare una policy o generarne una nuova con lo strumento di creazione delle policy nella console IAM Identity Center quando crei un nuovo set di autorizzazioni. Puoi anche creare policy IAM con AWS Policy Generator.

Quando distribuisci un set di autorizzazioni con una policy in linea, IAM Identity Center crea una policy IAM nel punto in Account AWS cui assegni il tuo set di autorizzazioni. IAM Identity Center crea la policy quando assegni il set di autorizzazioni all'account. La policy viene quindi allegata al ruolo IAM assunto dall'utente Account AWS nell'account.

Quando crei una policy in linea e assegni il tuo set di autorizzazioni, IAM Identity Center configura le policy predefinite per te. Account AWS Quando crei il tuo set di autorizzazioni conPolicy gestite dal cliente, devi creare le politiche Account AWS da solo prima di assegnare il set di autorizzazioni.

AWS politiche gestite

È possibile allegare politiche AWS gestite al set di autorizzazioni. AWS le politiche gestite sono politiche IAM che AWS mantiene. Al contrario, le politiche IAM del tuo account Policy gestite dal cliente sono quelle che crei e gestisci. AWS le politiche gestite riguardano i casi d'uso con privilegi minimi comuni nel tuo Account AWS. Puoi assegnare una policy AWS gestita come autorizzazioni per il ruolo creato da IAM Identity Center o come limite di autorizzazioni.

AWS mantiene politiche AWS gestite per le funzioni lavorative che assegnano autorizzazioni di accesso specifiche del lavoro alle tue risorse. AWS È possibile aggiungere una politica relativa alla funzione lavorativa quando si sceglie di utilizzare le autorizzazioni predefinite con il set di

autorizzazioni. Quando scegli Autorizzazioni personalizzate, puoi aggiungere più di una politica relativa alla funzione lavorativa.

Il tuo contiene Account AWS anche un gran numero di policy IAM AWS gestite per specifiche Servizi AWS e combinazioni di. Servizi AWS Quando crei un set di autorizzazioni con autorizzazioni personalizzate, puoi scegliere tra molte politiche AWS gestite aggiuntive da assegnare al tuo set di autorizzazioni.

AWS compila ogni Account AWS con AWS policy gestite. Per distribuire un set di autorizzazioni con policy AWS gestite, non è necessario prima creare una policy nel proprio. Account AWS Quando si crea il set di autorizzazioni conPolicy gestite dal cliente, è necessario creare le politiche Account AWS autonomamente prima di assegnare il set di autorizzazioni.

Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

Policy gestite dal cliente

Puoi allegare politiche gestite dai clienti al tuo set di autorizzazioni. Le politiche gestite dai clienti sono le politiche IAM del tuo account che crei e gestisci. Al contrario, AWS politiche gestite sono le politiche IAM del tuo account a essere AWS gestite. Puoi assegnare una policy gestita dal cliente come autorizzazioni per il ruolo creato da IAM Identity Center o come limite di autorizzazioni.

Quando crei un set di autorizzazioni con una policy gestita dal cliente, devi creare una policy IAM con lo stesso nome e percorso in ciascuna delle aree in Account AWS cui IAM Identity Center assegna il tuo set di autorizzazioni. Se stai specificando un percorso personalizzato, assicurati di specificare lo stesso percorso in ciascuno di essi. Account AWS Per ulteriori informazioni, consulta Nomi descrittivi e percorsi nella Guida per l'utente IAM. IAM Identity Center associa la policy IAM al ruolo IAM che crea nel tuo. Account AWS Come best practice, applica le stesse autorizzazioni alla policy in ogni account a cui assegni il set di autorizzazioni. Per ulteriori informazioni, consulta Utilizza le politiche IAM nei set di autorizzazioni.

Per ulteriori informazioni, consulta le politiche gestite dai clienti nella Guida per l'utente IAM.

Limiti delle autorizzazioni

Puoi allegare un limite di autorizzazioni al tuo set di autorizzazioni. Un limite di autorizzazioni è una policy IAM AWS gestita o gestita dal cliente che stabilisce le autorizzazioni massime che una policy basata sull'identità può concedere a un principale IAM. Quando applichi un limite di autorizzazioni, non AWS politiche gestite puoi concedere alcuna autorizzazione che superi Policy

inline le autorizzazioni concesse dal limite delle autorizzazioni. Policy gestite dal cliente Un limite di autorizzazioni non concede alcuna autorizzazione, ma fa sì che IAM ignori tutte le autorizzazioni oltre il limite.

Quando crei un set di autorizzazioni con una policy gestita dal cliente come limite di autorizzazioni, devi creare una policy IAM con lo stesso nome in ognuna delle aree in Account AWS cui IAM Identity Center assegna il tuo set di autorizzazioni. IAM Identity Center collega la policy IAM come limite di autorizzazioni al ruolo IAM che crea nel tuo. Account AWS

Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.

Crea, gestisci ed elimina i set di autorizzazioni

I set di autorizzazioni definiscono il livello di accesso di utenti e gruppi a un Account AWS. I set di autorizzazioni sono archiviati in IAM Identity Center e possono essere assegnati a uno o più Account AWS. Puoi assegnare più set di autorizzazioni a un utente. Per ulteriori informazioni sui set di autorizzazioni e su come vengono utilizzati in IAM Identity Center, consultaSet di autorizzazioni.

Tieni a mente le seguenti considerazioni quando crei i set di autorizzazioni:

- Inizia con un set di autorizzazioni predefinito

  Con un set di autorizzazioni predefinito, che utilizza autorizzazioni predefinite, si sceglie una singola politica AWS gestita da un elenco di politiche disponibili. Ogni politica concede un livello specifico di accesso a AWS servizi e risorse o autorizzazioni per una funzione lavorativa comune. Per informazioni su ciascuna di queste politiche, consulta le politiche AWS gestite per le funzioni lavorative. Dopo aver raccolto i dati di utilizzo, puoi perfezionare il set di autorizzazioni per renderlo più restrittivo.
- Limita la durata della sessione di gestione a periodi di lavoro ragionevoli

  Quando gli utenti si federano Account AWS e utilizzano la console di AWS gestione o l'interfaccia a riga di AWS comando (AWS CLI), IAM Identity Center utilizza l'impostazione della durata della sessione nel set di autorizzazioni per controllare la durata della sessione. Quando la sessione utente raggiunge la durata della sessione, vengono disconnessi dalla console e gli viene chiesto di accedere nuovamente. Come procedura consigliata in materia di sicurezza, ti consigliamo di non impostare una durata della sessione superiore a quella necessaria per svolgere il ruolo. Per impostazione predefinita, il valore per la durata della sessione è di un'ora. È possibile specificare un valore massimo di 12 ore. Per ulteriori informazioni, consulta Imposta la durata della sessione.

- Limita la durata della sessione Workforce User Portal

  Gli utenti di Workforce utilizzano le sessioni del portale per scegliere i ruoli e accedere alle applicazioni. Per impostazione predefinita, il valore di Durata massima della sessione, che determina il periodo di tempo in cui un utente della forza lavoro può accedere al portale di AWS accesso prima di dover effettuare nuovamente l'autenticazione, è otto ore. È possibile specificare un valore massimo di 90 giorni. Per ulteriori informazioni, consulta Configura la durata della sessione del portale di AWS accesso e delle applicazioni integrate in IAM Identity Center.
- Utilizza il ruolo che fornisce le autorizzazioni con privilegi minimi

  Ogni set di autorizzazioni creato e assegnato all'utente viene visualizzato come ruolo disponibile nel portale di accesso. AWS Quando accedi al portale come utente, scegli il ruolo che corrisponde al set di autorizzazioni più restrittivo che puoi utilizzare per eseguire attività nell'account, anziché. `AdministratorAccess` Verifica i set di autorizzazioni per verificare che forniscano l'accesso necessario prima di inviare l'invito all'utente.

> **Note**
>
> È inoltre possibile utilizzare AWS CloudFormationper creare e assegnare set di autorizzazioni e assegnare utenti a tali set di autorizzazioni.

Argomenti

Crea un set di autorizzazioni.

Utilizza questa procedura per creare un set di autorizzazioni predefinito che utilizza una singola policy AWS gestita o un set di autorizzazioni personalizzato che utilizza fino a 10 policy AWS gestite o gestite dal cliente e una policy in linea. Puoi richiedere un adeguamento al numero massimo di 10 policy nella console Service Quotas per IAM.

Puoi creare un set di autorizzazioni nella console IAM Identity Center.

Per creare un set di autorizzazioni

1. Apri la console IAM Identity Center.
2. In Autorizzazioni per più account, scegli Set di autorizzazioni.
3. Scegli Create permission set (Crea set di autorizzazioni).
4. Nella pagina Seleziona il tipo di set di autorizzazioni, in Tipo di set di autorizzazioni, seleziona un tipo di set di autorizzazioni.
5. Scegli una o più politiche che desideri utilizzare per il set di autorizzazioni, in base al tipo di set di autorizzazioni:

   - Set di autorizzazioni predefinito

     1. In Policy for predefined permission set, seleziona una delle policy della funzione IAM Job o delle policy di autorizzazione comuni nell'elenco, quindi scegli Avanti. Per ulteriori informazioni, consulta le politiche AWS gestite per le funzioni lavorative e le politiche AWS gestite nella Guida per l'AWS Identity and Access Management utente.
     2. Vai al Passaggio 6 per completare la pagina Specificare i dettagli del set di autorizzazioni.

   - Set di autorizzazioni personalizzato

     1. Seleziona Successivo.
     2. Nella pagina Specificare le politiche e i limiti di autorizzazione, scegli i tipi di policy IAM che desideri applicare al tuo nuovo set di autorizzazioni. Per impostazione predefinita, puoi aggiungere qualsiasi combinazione di un massimo di 10 policy gestite e policy AWS gestite dal cliente al tuo set di autorizzazioni. Questa quota è impostata da IAM. Per aumentarlo, richiedi un aumento della quota IAM Managed policy allegate a un ruolo IAM nella console Service Quotas in ciascuna delle aree in Account AWS cui desideri assegnare il set di autorizzazioni.

        - Espandi le policy AWS gestite per aggiungere policy di IAM che AWS crea e gestisce. Per ulteriori informazioni, consulta AWS politiche gestite.

          a. Cerca e scegli le politiche AWS gestite che desideri applicare ai tuoi utenti nel set di autorizzazioni.

          b. Se desideri aggiungere un altro tipo di politica, scegli il relativo contenitore ed effettua la selezione. Scegli Avanti dopo aver scelto tutte le politiche che desideri applicare. Vai al passaggio 6 per completare la pagina Specificare i dettagli del set di autorizzazioni.

        - Espandi le policy gestite dai clienti per aggiungere le policy di IAM che crei e gestisci tu. Per ulteriori informazioni, consulta Policy gestite dal cliente.

a. Scegli Allega policy e inserisci il nome di una policy che desideri aggiungere al tuo set di autorizzazioni. In ogni account a cui desideri assegnare il set di autorizzazioni, crea una politica con il nome che hai inserito. Come procedura consigliata, assegna le stesse autorizzazioni alla politica di ciascun account.

b. Scegli Allega altro per aggiungere un'altra politica.

c. Se desideri aggiungere un altro tipo di politica, scegli il relativo contenitore ed effettua la selezione. Scegli Avanti dopo aver scelto tutte le politiche che desideri applicare. Vai al passaggio 6 per completare la pagina Specificare i dettagli del set di autorizzazioni.

- Espandi Inline policy per aggiungere un testo di policy personalizzato in formato JSON. Le policy in linea non corrispondono alle risorse IAM esistenti. Per creare una policy in linea, inserisci il linguaggio delle policy personalizzato nel modulo fornito. IAM Identity Center aggiunge la policy alle risorse IAM che crea negli account dei membri. Per ulteriori informazioni, consulta Policy inline.

  a. Aggiungi le azioni e le risorse desiderate all'interno dell'editor interattivo alla tua policy in linea. È possibile aggiungere dichiarazioni aggiuntive con Aggiungi nuova dichiarazione.

  b. Se desideri aggiungere un altro tipo di politica, scegli il relativo contenitore ed effettua la selezione. Scegli Avanti dopo aver scelto tutte le politiche che desideri applicare. Vai al passaggio 6 per completare la pagina Specificare i dettagli del set di autorizzazioni.

- Espandi il limite delle autorizzazioni per aggiungere una policy IAM AWS gestita o gestita dal cliente come autorizzazioni massime che le altre policy del set di autorizzazioni possono assegnare. Per ulteriori informazioni, consulta Limiti delle autorizzazioni.

  a. Scegli Usa un limite di autorizzazioni per controllare le autorizzazioni massime.

  b. Scegli una policy AWS gestita per impostare una policy di IAM che venga creata e AWSgestita come limite per le autorizzazioni. Scegli le politiche gestite dai clienti per impostare una policy di IAM da creare e mantenere come limite delle autorizzazioni.

  c. Se desideri aggiungere un altro tipo di politica, scegli il relativo contenitore ed effettua la selezione. Scegli Avanti dopo aver scelto tutte le politiche che desideri applicare. Vai al passaggio 6 per completare la pagina Specificare i dettagli del set di autorizzazioni.

6. Nella pagina Specificare i dettagli del set di autorizzazioni, effettuare le seguenti operazioni:

   1. In Nome del set di autorizzazioni, digita un nome per identificare questo set di autorizzazioni in IAM Identity Center. Il nome specificato per questo set di autorizzazioni viene visualizzato nel portale di AWS accesso come ruolo disponibile. Gli utenti AWS accedono al portale di accesso, ne scelgono uno Account AWS e quindi scelgono il ruolo.

2. (Facoltativo) Puoi anche digitare una descrizione. La descrizione appare solo nella console IAM Identity Center, non nel portale di AWS accesso.
3. (Facoltativo) Specificare il valore per la durata della sessione. Questo valore determina il periodo di tempo in cui un utente può accedere prima che la console lo disconnetta dalla sessione. Per ulteriori informazioni, consulta Imposta la durata della sessione.
4. (Facoltativo) Specificate il valore per lo stato di inoltro. Questo valore viene utilizzato nel processo di federazione per reindirizzare gli utenti all'interno dell'account. Per ulteriori informazioni, consulta Imposta lo stato del relè.

   > **Note**
   >
   > L'URL dello stato di inoltro deve trovarsi all'interno di. AWS Management Console Per esempio:
   > **`https://console.aws.amazon.com/ec2/`**

5. Espandi Tag (opzionale), scegli Aggiungi tag, quindi specifica i valori per Chiave e Valore (opzionale).

   Per ulteriori informazioni sui tag, consulta Tagging delle risorse AWS IAM Identity Center.
6. Seleziona Successivo.
7. Nella pagina Rivedi e crea, esamina le selezioni effettuate, quindi scegli Crea.
8. Per impostazione predefinita, quando crei un set di autorizzazioni, il set di autorizzazioni non viene fornito (utilizzato in nessuno Account AWS). Per fornire un set di autorizzazioni in un account Account AWS, devi assegnare l'accesso a IAM Identity Center agli utenti e ai gruppi dell'account e quindi applicare il set di autorizzazioni a tali utenti e gruppi. Per ulteriori informazioni, consulta Accesso Single Sign-On a Account AWS.

Delegare l'amministrazione dei set di autorizzazioni

IAM Identity Center ti consente di delegare la gestione dei set di autorizzazioni e delle assegnazioni negli account creando policy IAM che fanno riferimento agli Amazon Resource Names (ARN) delle risorse IAM Identity Center. Ad esempio, puoi creare policy che consentano a diversi amministratori di gestire le assegnazioni in account specifici per set di autorizzazioni con tag specifici.

È possibile utilizzare uno dei seguenti metodi per creare questi tipi di politiche.

- (Consigliato) Crea set di autorizzazioni in IAM Identity Center, ognuno con una policy diversa, e assegna i set di autorizzazioni a diversi utenti o gruppi. Ciò consente di gestire le autorizzazioni amministrative per gli utenti che accedono utilizzando la fonte di identità IAM Identity Center scelta.
- Crea policy personalizzate in IAM, quindi collegale ai ruoli IAM assunti dai tuoi amministratori. Per informazioni sui ruoli, consulta Ruoli IAM per ottenere le autorizzazioni amministrative assegnate a IAM Identity Center.

> **Important**
>
> Gli ARN di risorse IAM Identity Center distinguono tra maiuscole e minuscole.

Di seguito vengono illustrati i casi appropriati per fare riferimento al set di autorizzazioni di IAM Identity Center e ai tipi di risorse dell'account.

Tipi di risorsa	ARN	Chiavi contestuali
PermissionSet	`arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}`	`aws:ResourceTag/${TagKey}`
Account	`arn:${Partition}:sso:::account/${AccountId}`	Non applicabile

Utilizza le politiche IAM nei set di autorizzazioni

InCrea un set di autorizzazioni., hai imparato come aggiungere politiche, comprese le politiche gestite dai clienti e i limiti delle autorizzazioni, a un set di autorizzazioni. Quando aggiungi politiche e autorizzazioni gestite dai clienti a un set di autorizzazioni, IAM Identity Center non crea alcuna policy. Account AWSÈ invece necessario creare tali politiche in anticipo in ogni account a cui si desidera assegnare il set di autorizzazioni e abbinarle alle specifiche del nome e del percorso del set di autorizzazioni. Quando assegni un set di autorizzazioni Account AWS a un membro della tua organizzazione, IAM Identity Center crea un ruolo AWS Identity and Access Management (IAM) e associa le tue politiche IAM a quel ruolo.

> **Note**
>
> Prima di assegnare il set di autorizzazioni con le policy IAM, devi preparare il tuo account membro. Il nome di una policy IAM nel tuo account membro deve corrispondere, con distinzione tra maiuscole e minuscole, al nome della policy nel tuo account di gestione. IAM Identity Center non riesce ad assegnare il set di autorizzazioni se la policy non esiste nel tuo account membro.
> Le autorizzazioni concesse dalla policy non devono necessariamente corrispondere esattamente tra gli account.

Per assegnare una policy IAM a un set di autorizzazioni

1. Crea una policy IAM in ciascuna delle aree in Account AWS cui desideri assegnare il set di autorizzazioni.
2. Assegna le autorizzazioni alla policy IAM. Puoi assegnare autorizzazioni diverse a diversi account. Per un'esperienza coerente, configura e gestisci le stesse autorizzazioni in ogni policy. Puoi utilizzare risorse di automazione, AWS CloudFormation StackSets ad esempio per creare copie di una policy IAM con lo stesso nome e le stesse autorizzazioni in ogni account membro. Per ulteriori informazioni in merito CloudFormation StackSets, consulta Working with AWS CloudFormation StackSets nella guida per l'AWS CloudFormation utente.
3. Crea un set di autorizzazioni nel tuo account di gestione e aggiungi la tua policy IAM nella sezione Customer managed policies o Permissions boundary. Per maggiori dettagli su come creare un set di autorizzazioni, consulta. Crea un set di autorizzazioni.
4. Aggiungi eventuali policy in linea, policy AWS gestite o policy IAM aggiuntive che hai preparato.
5. Crea e assegna il tuo set di autorizzazioni.

Eliminare i set di autorizzazioni

Se si desidera revocare una sessione attiva del set di autorizzazioni, vedere. Revoca le sessioni di ruolo IAM attive create dai set di autorizzazioni

Prima di poter eliminare un set di autorizzazioni da IAM Identity Center, devi rimuoverlo da tutti coloro Account AWS che utilizzano il set di autorizzazioni. Per verificare l'accesso esistente di utenti e gruppi, consultaVisualizza le assegnazioni di utenti e gruppi.

Per rimuovere un set di autorizzazioni da un Account AWS

1. Apri la console IAM Identity Center.
2. In Autorizzazioni multiaccount, scegli. Account AWS
3. Nella Account AWSpagina viene visualizzato un elenco ad albero della tua organizzazione. Seleziona il nome del set di autorizzazioni Account AWS da cui desideri rimuovere il set di autorizzazioni.
4. Nella pagina Panoramica relativa a Account AWS, scegli la scheda Set di autorizzazioni.
5. Seleziona la casella di controllo accanto al set di autorizzazioni che desideri rimuovere, quindi scegli Rimuovi.
6. Nella finestra di dialogo Rimuovi set di autorizzazioni, conferma che sia selezionato il set di autorizzazioni corretto, digita **`Delete`** per confermare la rimozione, quindi scegli Rimuovi accesso.

Utilizza la procedura seguente per eliminare uno o più set di autorizzazioni in modo che non possano più essere utilizzati da nessuno Account AWS all'interno dell'organizzazione.

> **Note**
>
> Tutti gli utenti e i gruppi a cui Account AWS è stato assegnato questo set di autorizzazioni, indipendentemente da chi lo utilizza, non potranno più accedere. Per verificare l'accesso esistente di utenti e gruppi, vedereVisualizza le assegnazioni di utenti e gruppi.

Per eliminare un set di autorizzazioni da un Account AWS

1. Apri la console IAM Identity Center.
2. In Autorizzazioni per più account, scegli Set di autorizzazioni.
3. Seleziona il set di autorizzazioni che desideri eliminare, quindi scegli Elimina.
4. Nella finestra di dialogo Elimina set di autorizzazioni, digitate il nome del set di autorizzazioni per confermare l'eliminazione, quindi scegliete Elimina. Per il nome è prevista una distinzione tra maiuscole e minuscole.

Configura le proprietà del set di autorizzazioni

In IAM Identity Center puoi personalizzare l'esperienza utente configurando le seguenti proprietà del set di autorizzazioni.

Argomenti

Imposta la durata della sessione

Per ogni set di autorizzazioni, puoi specificare una durata della sessione per controllare il periodo di tempo in cui un utente può accedere a un Account AWS. Al termine della durata specificata, AWS disconnette l'utente dalla sessione.

Quando si crea un nuovo set di autorizzazioni, la durata della sessione è impostata su 1 ora (in secondi) per impostazione predefinita. La durata minima della sessione è di 1 ora e può essere impostata su un massimo di 12 ore. IAM Identity Center crea automaticamente i ruoli IAM in ogni account assegnato per ogni set di autorizzazioni e configura questi ruoli con una durata massima della sessione di 12 ore.

Quando gli utenti si federano nella propria Account AWS console o quando viene utilizzato AWS Command Line Interface (AWS CLI), IAM Identity Center utilizza l'impostazione della durata della sessione sul set di autorizzazioni per controllare la durata della sessione. Per impostazione predefinita, i ruoli IAM generati da IAM Identity Center per i set di autorizzazioni possono essere assunti solo dagli utenti di IAM Identity Center, il che garantisce l'applicazione della durata della sessione specificata nel set di autorizzazioni IAM Identity Center.

> **Important**
>
> Per una sicurezza ottimale, è consigliabile non impostare la durata delle sessioni più del tempo necessario per eseguire il ruolo.

Dopo aver creato un set di autorizzazioni, puoi aggiornarlo per applicare una nuova durata della sessione. Utilizzare la procedura seguente per modificare la durata della sessione per un set di autorizzazioni.

Impostazione della durata della sessione

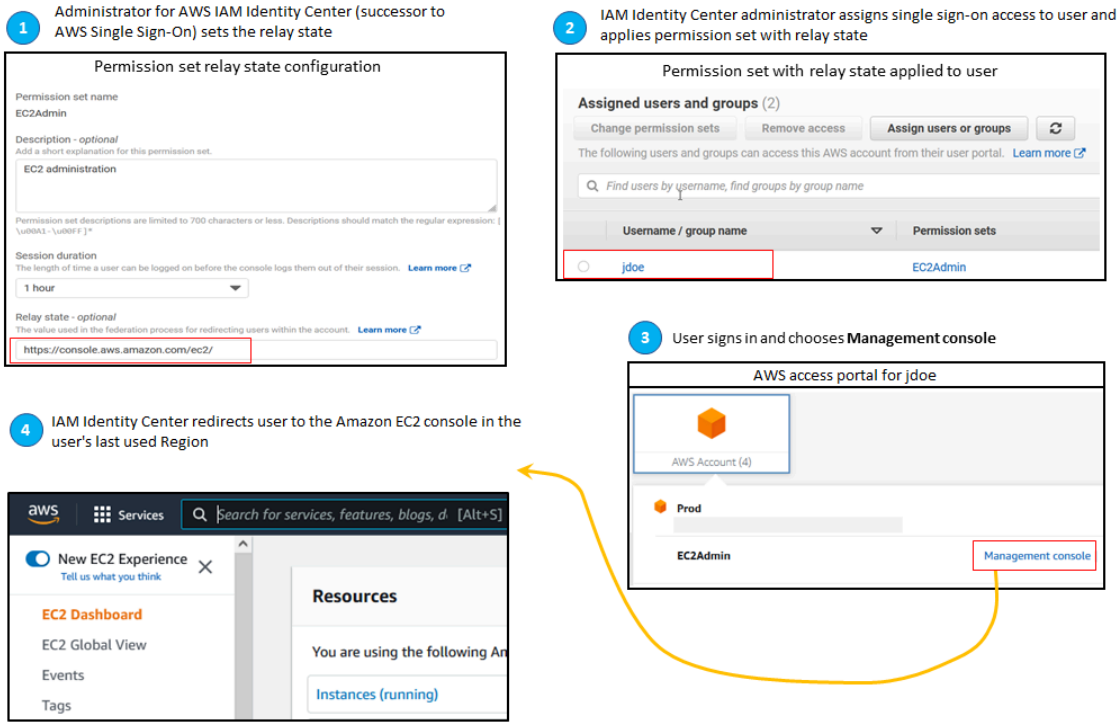
1. Apri la console IAM Identity Center.
2. In Autorizzazioni per più account, scegli Set di autorizzazioni.
3. Scegli il nome del set di autorizzazioni per il quale desideri modificare la durata della sessione.
4. Nella pagina dei dettagli del set di autorizzazioni, a destra dell'intestazione della sezione Impostazioni generali, scegli Modifica.
5. Nella pagina Modifica impostazioni generali del set di autorizzazioni, scegli un nuovo valore per la durata della sessione.
6. Se il set di autorizzazioni è fornito in uno qualsiasi dei due Account AWS, i nomi degli account vengono visualizzati nella sezione Account AWS Da riassegnare automaticamente. Dopo l'aggiornamento del valore della durata della sessione per il set di autorizzazioni, tutti coloro Account AWS che utilizzano il set di autorizzazioni vengono riassegnati. Ciò significa che il nuovo valore di questa impostazione viene applicato a tutti coloro Account AWS che utilizzano il set di autorizzazioni.
7. Seleziona Salvataggio delle modifiche.
8. Nella parte superiore della Account AWSpagina, viene visualizzata una notifica.

   - Se il set di autorizzazioni viene fornito in uno o più account Account AWS, la notifica conferma che il riassegnamento è Account AWS stato eseguito correttamente e che il set di autorizzazioni aggiornato è stato applicato agli account.
   - Se il set di autorizzazioni non è fornito in un Account AWS, la notifica conferma che le impostazioni del set di autorizzazioni sono state aggiornate.

Imposta lo stato del relè

Per impostazione predefinita, quando un utente AWS accede al portale di accesso, sceglie un account e quindi sceglie il ruolo AWS creato dal set di autorizzazioni assegnato, IAM Identity Center reindirizza il browser dell'utente a. AWS Management ConsoleÈ possibile modificare questo comportamento impostando lo stato di inoltro su un URL della console diverso. L'impostazione dello stato di inoltro consente di fornire all'utente un accesso rapido alla console più appropriata per il suo ruolo. Ad esempio, puoi impostare lo stato di inoltro sull'URL della console Amazon EC2 **`https://console.aws.amazon.com/ec2/`** () per reindirizzare l'utente a quella console quando sceglie il ruolo di amministratore di Amazon EC2. Durante il reindirizzamento all'URL predefinito o all'URL dello stato di inoltro, IAM Identity Center indirizza il browser dell'utente all'endpoint della console utilizzato

per ultimo dall'utente. Regione AWS Ad esempio, se un utente ha terminato l'ultima sessione di console nella regione Europa (Stoccolma) (eu-north-1), l'utente viene reindirizzato alla console Amazon EC2 in quella regione.



Per configurare IAM Identity Center in modo da reindirizzare l'utente a una console in un determinato modo Regione AWS, includi la specifica della regione come parte dell'URL. Ad esempio, per reindirizzare l'utente alla console Amazon EC2 nella regione Stati Uniti orientali (Ohio) (us-east-2), specifica l'URL per la console Amazon EC2 in quella regione (). **`https://us-east-2.console.aws.amazon.com/ec2/`** Se hai abilitato IAM Identity Center nella regione Stati Uniti occidentali (Oregon) (us-west-2) e desideri indirizzare l'utente verso quella regione, specifica. **`https://us-west-2.console.aws.amazon.com`**

Utilizza la seguente procedura per configurare l'URL dello stato di inoltro per un set di autorizzazioni.

Per configurare lo stato del relè

1. Apri la console IAM Identity Center.
2. In Autorizzazioni per più account, scegli Set di autorizzazioni.
3. Scegli il nome del set di autorizzazioni per il quale desideri impostare il nuovo URL dello stato di inoltro.

4. Nella pagina dei dettagli del set di autorizzazioni, a destra dell'intestazione della sezione Impostazioni generali, scegli Modifica.
5. Nella pagina Modifica impostazioni generali del set di autorizzazioni, in Stato di inoltro, digita l'URL della console per uno qualsiasi dei AWS servizi. Per esempio:

   `https://console.aws.amazon.com/ec2/`

   > **Note**
   >
   > L'URL dello stato di inoltro deve trovarsi all'interno di. AWS Management Console

6. Se il set di autorizzazioni è fornito in uno qualsiasi Account AWS, i nomi degli account vengono visualizzati in cui Account AWS riassegnare automaticamente il provisioning. Dopo l'aggiornamento dell'URL dello stato di inoltro per il set di autorizzazioni, viene riassegnato il provisioning a tutti Account AWS coloro che utilizzano il set di autorizzazioni. Ciò significa che il nuovo valore per questa impostazione viene applicato a tutti coloro Account AWS che utilizzano il set di autorizzazioni.
7. Seleziona Salvataggio delle modifiche.
8. Nella parte superiore della pagina AWS Organizzazione, viene visualizzata una notifica.

   - Se il set di autorizzazioni viene fornito in uno o più Account AWS, la notifica conferma che il riassegnamento è Account AWS stato eseguito correttamente e che il set di autorizzazioni aggiornato è stato applicato agli account.
   - Se il set di autorizzazioni non è fornito in un Account AWS, la notifica conferma che le impostazioni del set di autorizzazioni sono state aggiornate.

> **Note**
>
> Puoi automatizzare questo processo utilizzando l' AWS API, un AWS SDK o (). AWS Command Line InterfaceAWS CLI Per ulteriori informazioni, consultare:
>
> - Le `UpdatePermissionSet` azioni `CreatePermissionSet` o nella guida di riferimento all'API di IAM Identity Center
> - I `update-permission-set` comandi `create-permission-set` or nella sso-adminsezione del AWS CLI Command Reference.

Utilizza una politica Deny per revocare le autorizzazioni utente attive

Potrebbe essere necessario revocare l'accesso a un utente di IAM Identity Center Account AWS mentre l'utente utilizza attivamente un set di autorizzazioni. Puoi impedire loro di utilizzare le sessioni di ruolo IAM attive implementando in anticipo una policy Deny per un utente non specificato e, se necessario, puoi aggiornare la policy Deny per specificare l'utente di cui desideri bloccare l'accesso. Questo argomento spiega come creare una policy Deny e alcune considerazioni su come implementarla.

Preparati a revocare una sessione di ruolo IAM attiva creata da un set di autorizzazioni

Puoi impedire all'utente di intraprendere azioni con un ruolo IAM che sta utilizzando attivamente applicando una politica di negazione totale per un utente specifico mediante l'uso di una policy di controllo del servizio. Puoi anche impedire a un utente di utilizzare qualsiasi set di autorizzazioni finché non modifichi la sua password, in modo da rimuovere un malintenzionato che utilizza attivamente in modo improprio le credenziali rubate. Se è necessario negare l'accesso in generale e impedire a un utente di accedere nuovamente a un set di autorizzazioni o ad altri set di autorizzazioni, è inoltre possibile rimuovere tutti gli accessi utente, interrompere la sessione del portale di AWS accesso attivo e disabilitare l'accesso dell'utente. Scopri come utilizzare la politica di rifiuto insieme ad azioni aggiuntive per una più ampia revoca dell'accesso. Revoca le sessioni di ruolo IAM attive create dai set di autorizzazioni

Politica di negazione

Puoi utilizzare una policy Deny con una condizione che `UserID` corrisponda a quella dell'utente dell'archivio di identità di IAM Identity Center per impedire ulteriori azioni da parte di un ruolo IAM che l'utente sta utilizzando attivamente. L'utilizzo di questa policy evita l'impatto sugli altri utenti che potrebbero utilizzare lo stesso set di autorizzazioni quando si implementa la politica Deny. Questa politica utilizza l'ID utente segnaposto *`Add user ID here`*, `"identitystore:userId"` che dovrai aggiornare con l'ID utente per il quale desideri revocare l'accesso.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "*"
            ],
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "identitystore:userId": "Add user ID here"
                }
            }
        }
    ]
}
```

Sebbene sia possibile utilizzare un'altra chiave di condizione“`aws:userId`”, ad esempio, “`identitystore:userId`” is certain perché si tratta di un valore unico a livello globale associato a una persona. L'utilizzo della condizione può essere influenzato dal modo “`aws:userId`” in cui gli attributi utente vengono sincronizzati dall'origine delle identità e può cambiare se il nome utente o l'indirizzo e-mail dell'utente cambiano.

Dalla console IAM Identity Center, puoi trovare un utente `identitystore:userId` accedendo a Utenti, cercando l'utente per nome, espandendo la sezione Informazioni generali e copiando l'ID utente. È anche comodo interrompere la sessione del portale di AWS accesso di un utente e disabilitarne l'accesso all'accesso nella stessa sezione durante la ricerca dell'ID utente. Puoi automatizzare il processo di creazione di una policy Deny ottenendo l'ID utente dell'utente interrogando le API dell'identity store.

Implementazione della politica di negazione

È possibile utilizzare un ID utente segnaposto non valido, ad esempio per implementare in anticipo la politica Deny utilizzando una Service Control Policy (SCP) associata agli utenti a cui gli utenti potrebbero avere accesso. *`Add user ID here`* Account AWS Questo è l'approccio consigliato per la facilità e la velocità di impatto. Quando revochi l'accesso di un utente con la politica Nega, modificherai la politica per sostituire l'ID utente segnaposto con l'ID utente della persona di cui desideri revocare l'accesso. Ciò impedisce all'utente di intraprendere azioni con qualsiasi autorizzazione impostata in ogni account a cui colleghi l'SCP. Blocca le azioni dell'utente anche se utilizza la sessione del portale di AWS accesso attivo per accedere a diversi account e assumere ruoli diversi. Con l'accesso dell'utente completamente bloccato da SCP, è possibile disabilitare la sua capacità di accedere, revocare le assegnazioni e interrompere la sessione del portale di AWS accesso, se necessario.

In alternativa all'utilizzo di SCP, è possibile includere la politica Deny anche nella politica in linea dei set di autorizzazioni e nelle politiche gestite dai clienti utilizzate dai set di autorizzazioni a cui l'utente può accedere.

Se è necessario revocare l'accesso a più di una persona, è possibile utilizzare un elenco di valori nel blocco delle condizioni, ad esempio:

```
        "Condition": {
                "StringEquals": {
                    "identitystore:userId": [" user1 userId", "user2 userId"...]
                    }
    }
```

> **Important**
>
> Indipendentemente dai metodi utilizzati, è necessario intraprendere qualsiasi altra azione correttiva e mantenere l'ID utente dell'utente nella politica per almeno 12 ore. Dopo tale periodo, tutti i ruoli assunti dall'utente scadono e puoi quindi rimuovere il relativo ID utente dalla politica Deny.

Riferimento ai set di autorizzazioni nelle politiche delle risorse, Amazon EKS e AWS KMS

Quando assegni un set di autorizzazioni a un AWS account, IAM Identity Center crea un ruolo con un nome che inizia con. `AWSReservedSSO_`

Il nome completo e Amazon Resource Name (ARN) del ruolo utilizzano il seguente formato:

Nome	ARN
`AWSReservedSSO_` *`permission-set-name_unique-suffix`*	`arn:aws:iam::` *`aws-account-ID`*`:role/aws-reserved/sso.amazonaws.com/` *`aws-region`* `/AWSReservedSSO_` *`permission-set-name_unique-suffix`*

Ad esempio, se si crea un set di autorizzazioni che concede l'accesso tramite AWS account agli amministratori del database, viene creato un ruolo corrispondente con il nome e l'ARN seguenti:

Nome	ARN
`AWSReservedSSO_DatabaseAdministrator_1234567890abcdef`	`arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_1234567890abcdef`

Se si eliminano tutte le assegnazioni a questo set di autorizzazioni nell' AWS account, viene eliminato anche il ruolo corrispondente creato da IAM Identity Center. Se in un secondo momento effettui una nuova assegnazione allo stesso set di autorizzazioni, IAM Identity Center crea un nuovo ruolo per il set di autorizzazioni. Il nome e l'ARN del nuovo ruolo includono un suffisso diverso e univoco. In questo esempio, il suffisso univoco è abcdef0123456789.

Nome	ARN
`AWSReservedSSO_DatabaseAdministrator_` **`abcdef0123456789`**	`arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_` **`abcdef0123456789`**

La modifica del suffisso nel nuovo nome e nell'ARN per il ruolo farà sì che qualsiasi politica che faccia riferimento al nome e all'ARN originali out-of-date sia tale da interrompere l'accesso per le persone che utilizzano il set di autorizzazioni corrispondente. Ad esempio, una modifica dell'ARN per il ruolo interromperà l'accesso degli utenti del set di autorizzazioni se si fa riferimento all'ARN originale nelle seguenti configurazioni:

- Nel `aws-auth ConfigMap` file per Amazon Elastic Kubernetes Service (Amazon EKS)
- In una politica basata sulle risorse per una chiave (). AWS Key Management Service AWS KMS Questa politica viene anche definita politica chiave.

Sebbene sia possibile aggiornare le politiche basate sulle risorse per la maggior parte dei AWS servizi per fare riferimento a un nuovo ARN per un ruolo che corrisponde a un set di autorizzazioni, è necessario disporre di un ruolo di backup da creare in IAM per Amazon EKS e se AWS KMS l'ARN

cambia. Per Amazon EKS, il ruolo IAM di backup deve esistere in`aws-auth ConfigMap`. Perché AWS KMS deve esistere nelle tue politiche chiave. Se non disponi di un ruolo IAM di backup in entrambi i casi, devi contattare AWS Support.

Consigli per evitare interruzioni dell'accesso

Per evitare interruzioni dell'accesso dovute a modifiche all'ARN per un ruolo che corrisponde a un set di autorizzazioni, si consiglia di effettuare le seguenti operazioni.

- Mantieni almeno l'assegnazione di un set di autorizzazioni.

  Gestisci questa assegnazione negli AWS account che contengono i ruoli a cui fai riferimento in Amazon EKS, le politiche chiave o le politiche basate sulle risorse `aws-auth ConfigMap` per altri. AWS KMS Servizi AWS

  Ad esempio, se crei un set di `EKSAccess` autorizzazioni e fai riferimento all'ARN del ruolo corrispondente dall' AWS account`111122223333`, assegna in modo permanente un gruppo amministrativo al set di autorizzazioni in quell'account. Poiché l'assegnazione è permanente, IAM Identity Center non eliminerà il ruolo corrispondente, il che elimina il rischio di ridenominazione. Il gruppo amministrativo avrà sempre accesso senza il rischio di un aumento dei privilegi.
- Per Amazon EKS e AWS KMS: Includi un ruolo creato in IAM.

  Se fai riferimento agli ARN dei ruoli per i set di autorizzazioni in un cluster `aws-auth ConfigMap` per Amazon EKS o nelle politiche chiave per le AWS KMS chiavi, ti consigliamo di includere anche almeno un ruolo creato in IAM. Il ruolo deve consentirti di accedere al cluster Amazon EKS o gestire la policy AWS KMS chiave. Il set di autorizzazioni deve essere in grado di assumere questo ruolo. In questo modo, se il ruolo ARN per un set di autorizzazioni cambia, puoi aggiornare il riferimento all'ARN nella `aws-auth ConfigMap` politica o chiave. AWS KMS La sezione successiva fornisce un esempio di come è possibile creare una policy di fiducia per un ruolo creato in IAM. Il ruolo può essere assunto solo da un set di `AdministratorAccess` autorizzazioni.

Esempio di politica di fiducia personalizzata

Di seguito è riportato un esempio di policy di fiducia personalizzata che fornisce un set di `AdministratorAccess` autorizzazioni con accesso a un ruolo creato in IAM. Gli elementi chiave di questa politica includono:

- L'elemento principale di questa politica di fiducia specifica l'intestatario AWS del conto. In questa policy, i responsabili dell' AWS account `111122223333` con `sts:AssumeRole` autorizzazioni possono assumere il ruolo creato in IAM.
- La base `Condition element` di questa politica di fiducia specifica requisiti aggiuntivi per i responsabili che possono assumere il ruolo creato in IAM. In questo criterio, il ruolo può essere assunto dal set di autorizzazioni con il seguente ruolo ARN.

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/
AWSReservedSSO_AdministratorAccess_*"
```

> **Note**
>
> L'`Condition`elemento include l'operatore `ArnLike` condition e utilizza un carattere jolly alla fine del ruolo ARN del set di autorizzazioni, anziché un suffisso univoco. Ciò significa che la policy consente al set di autorizzazioni di assumere il ruolo creato in IAM anche se il ruolo ARN per il set di autorizzazioni cambia.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/aws-reserved/
sso.amazonaws.com/eu-west-2/AWSReservedSSO_AdministratorAccess_*"
        }
      }
    }
  ]
}
```

L'inclusione di un ruolo creato in IAM in tale politica ti fornirà l'accesso di emergenza ai tuoi cluster Amazon EKS o ad altre AWS risorse se un set di autorizzazioni o tutte le assegnazioni al set di autorizzazioni vengono eliminati e ricreati accidentalmente. AWS KMS keys

Controllo dell'accesso basato sugli attributi

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. Puoi utilizzare IAM Identity Center per gestire l'accesso alle tue AWS risorse su più livelli Account AWS utilizzando attributi utente che provengono da qualsiasi fonte di identità IAM Identity Center. In AWS, questi attributi sono chiamati tag. L'utilizzo degli attributi utente come tag AWS aiuta a semplificare il processo di creazione di autorizzazioni dettagliate AWS e garantisce che la forza lavoro abbia accesso solo alle risorse con tag corrispondenti. AWS

Ad esempio, puoi assegnare agli sviluppatori Bob e Sally, che fanno parte di due team diversi, lo stesso set di autorizzazioni in IAM Identity Center e quindi selezionare l'attributo del nome del team per il controllo degli accessi. Quando Bob e Sally accedono al loro Account AWS, IAM Identity Center invia l'attributo del nome del team AWS durante la sessione in modo che Bob e Sally possano accedere alle risorse AWS del progetto solo se l'attributo del nome del team corrisponde al tag del nome del team sulla risorsa del progetto. Se Bob passerà al team di Sally in futuro, puoi modificare il suo accesso semplicemente aggiornando l'attributo del nome del team nella directory aziendale. La prossima volta che Bob accederà, avrà automaticamente accesso alle risorse di progetto del suo nuovo team senza richiedere alcun aggiornamento delle autorizzazioni. AWS

Questo approccio aiuta anche a ridurre il numero di autorizzazioni distinte da creare e gestire in IAM Identity Center, poiché gli utenti associati agli stessi set di autorizzazioni possono ora disporre di autorizzazioni uniche in base ai loro attributi. Puoi utilizzare questi attributi utente nei set di autorizzazioni di IAM Identity Center e nelle politiche basate sulle risorse per implementare ABAC nelle AWS risorse e semplificare la gestione delle autorizzazioni su larga scala.

Vantaggi

Di seguito sono riportati i vantaggi aggiuntivi dell'utilizzo di ABAC in IAM Identity Center.

- ABAC richiede un minor numero di set di autorizzazioni: poiché non è necessario creare politiche diverse per diverse funzioni lavorative, si creano meno set di autorizzazioni. Ciò riduce la complessità della gestione delle autorizzazioni.

- Utilizzando ABAC, i team possono cambiare e crescere rapidamente: le autorizzazioni per le nuove risorse vengono concesse automaticamente in base agli attributi quando le risorse vengono etichettate in modo appropriato al momento della creazione.
- Usa gli attributi dei dipendenti dalla tua directory aziendale con ABAC: puoi utilizzare gli attributi dei dipendenti esistenti da qualsiasi fonte di identità configurata in IAM Identity Center per prendere decisioni sul controllo degli accessi in. AWS
- Tieni traccia di chi accede alle risorse: gli amministratori della sicurezza possono determinare facilmente l'identità di una sessione esaminando gli attributi utente in cui AWS CloudTrail tenere traccia delle attività degli utenti. AWS

Per informazioni su come configurare ABAC utilizzando la console IAM Identity Center, consulta. Attributi per il controllo degli accessi Per informazioni su come abilitare e configurare ABAC utilizzando le API IAM Identity Center, consulta la Guida di riferimento CreateInstanceAccessControlAttributeConfigurationall'API IAM Identity Center.

Argomenti

- Elenco di controllo: configurazione di ABAC utilizzando IAM Identity Center AWS
- Attributi per il controllo degli accessi

Elenco di controllo: configurazione di ABAC utilizzando IAM Identity Center AWS

Questa lista di controllo include le attività di configurazione necessarie per preparare AWS le risorse e configurare IAM Identity Center per l'accesso ABAC. Completa le attività in questa lista di controllo in ordine. Quando un link di riferimento rimanda a un argomento, torna su questo argomento in modo da poter procedere con le attività rimanenti di questa lista di controllo.

Fase	Attività	Documentazione di riferimento
1	Scopri come aggiungere tag a tutte le tue AWS risorse. Per implementare ABAC in IAM Identity Center, devi prima aggiungere tag a tutte le AWS risorse per le quali desideri implementare ABAC.	• Taggare le risorse AWS
2	Scopri come configurare la tua origine di identità in IAM Identity Center con le identità e gli attributi utente	• Gestisci la tua fonte di identità

Fase	Attività	Documentazione di riferimento
	associati nel tuo archivio di identità. IAM Identity Center ti consente di utilizzare gli attributi utente di qualsiasi fonte di identità IAM Identity Center supportata per ABAC in. AWS	
3	In base ai seguenti criteri, stabilisci quali attributi desideri utilizzare per prendere decisioni sul controllo degli accessi AWS e inviali a IAM Identity Center.	• Nozioni di base
	• Se utilizzi un provider di identità (IdP) esterno, decidi se desideri utilizzare gli attributi passati dall'IdP o selezionare gli attributi dall'interno di IAM Identity Center.	• Scelta degli attributi quando si utilizza un provider di identità esterno come fonte di identità
	• Se scegli di avere gli attributi di invio del tuo IdP, configura il tuo IdP per trasmettere gli attributi nelle asserzioni SAML. Consulta le `Optional` sezioni del tutorial relative al tuo IdP specifico.	• Tutorial introduttivi
	• Se utilizzi un IdP come fonte di identità e scegli di selezionare gli attributi in IAM Identity Center, scopri come configurare SCIM in modo che i valori degli attributi provengano dal tuo IdP. Se non puoi usare SCIM con il tuo IdP, aggiungi gli utenti e i loro attributi utilizzando la pagina Utente della console IAM Identity Center.	• Provisioning automatico • Attributi del provider di identità esterno supportati
	• Se utilizzi Active Directory o IAM Identity Center come fonte di identità oppure utilizzi un IdP e scegli di selezionare gli attributi in IAM Identity Center, esamina gli attributi disponibili che puoi configurare. Quindi passa immediatamente alla fase 4 per iniziare a configurare gli attributi ABAC utilizzando la console IAM Identity Center.	• Scelta degli attributi quando utilizzi IAM Identity Center come fonte di identità • Scelta degli attributi da utilizzare AWS Managed Microsoft AD come fonte di identità • Mappature predefinite

Fase	Attività	Documentazione di riferimento
4	Seleziona gli attributi da utilizzare per ABAC utilizzando la pagina Attributi per il controllo degli accessi nella console IAM Identity Center. Da questa pagina puoi selezionare gli attributi per il controllo degli accessi dalla fonte di identità che hai configurato nel passaggio 2. Dopo che le identità e i relativi attributi sono presenti in IAM Identity Center, è necessario creare coppie chiave-valore (mappature) che verranno passate all'utente Account AWS per utilizzarle nelle decisioni di controllo degli accessi.	• Abilita e configura gli attributi per il controllo degli accessi
5	Crea politiche di autorizzazione personalizzate all'interno del tuo set di autorizzazioni e utilizza gli attributi di controllo dell'accesso per creare regole ABAC in modo che gli utenti possano accedere solo alle risorse con tag corrispondenti. Gli attributi utente configurati nel passaggio 4 vengono utilizzati come tag nelle decisioni sul controllo degli AWS accessi. È possibile fare riferimento agli attributi di controllo dell'accesso nella politica delle autorizzazioni utilizzando la `aws:PrincipalTag/key` condizione.	• Crea politiche di autorizzazione per ABAC in IAM Identity Center
6	Tra le varie opzioni Account AWS, assegna gli utenti ai set di autorizzazioni creati nel passaggio 5. In questo modo, quando si uniscono ai propri account e accedono alle AWS risorse, ottengono l'accesso solo in base ai tag corrispondenti.	• Assegna l'accesso utente a Account AWS

Dopo aver completato questi passaggi, gli utenti che effettueranno la federazione in un sistema Account AWS Single Sign-On avranno accesso alle proprie AWS risorse in base agli attributi corrispondenti.

Attributi per il controllo degli accessi

Attributi per il controllo degli accessi è il nome della pagina nella console IAM Identity Center in cui selezioni gli attributi utente da utilizzare nelle policy per controllare l'accesso alle risorse. Puoi assegnare utenti ai carichi di lavoro in AWS base agli attributi esistenti nella fonte di identità degli utenti.

Ad esempio, supponiamo di voler assegnare l'accesso ai bucket S3 in base ai nomi dei reparti. Nella pagina Attributi per il controllo degli accessi, si seleziona l'attributo utente Department da utilizzare con il controllo degli accessi basato sugli attributi (ABAC). Nel set di autorizzazioni IAM Identity Center, scrivi quindi una policy che concede agli utenti l'accesso solo quando l'attributo Department corrisponde al tag department che hai assegnato ai tuoi bucket S3. IAM Identity Center passa l'attributo department dell'utente all'account a cui si accede. L'attributo viene quindi utilizzato per determinare l'accesso in base alla policy. Per ulteriori informazioni su ABAC, vedereControllo dell'accesso basato sugli attributi.

Nozioni di base

Il modo in cui si inizia a configurare gli attributi per il controllo degli accessi dipende dalla fonte di identità utilizzata. Indipendentemente dalla fonte di identità scelta, dopo aver selezionato gli attributi è necessario creare o modificare le politiche relative ai set di autorizzazioni. Queste politiche devono concedere alle identità degli utenti l'accesso alle AWS risorse.

Scelta degli attributi quando utilizzi IAM Identity Center come fonte di identità

Quando configuri IAM Identity Center come fonte di identità, devi prima aggiungere utenti e configurarne gli attributi. Successivamente, vai alla pagina Attributi per il controllo degli accessi e seleziona gli attributi che desideri utilizzare nelle politiche. Infine, vai alla Account AWSpagina per creare o modificare i set di autorizzazioni per utilizzare gli attributi per ABAC.

Scelta degli attributi da utilizzare AWS Managed Microsoft AD come fonte di identità

Quando configuri IAM Identity Center AWS Managed Microsoft AD come fonte di identità, per prima cosa mappi un set di attributi da Active Directory agli attributi utente in IAM Identity Center. Successivamente, vai alla pagina Attributi per il controllo degli accessi. Scegliete quindi quali attributi utilizzare nella configurazione ABAC in base al set esistente di attributi SSO mappati da Active Directory. Infine, crea le regole ABAC utilizzando gli attributi di controllo degli accessi nei set di autorizzazioni per concedere alle identità degli utenti l'accesso alle risorse. AWS Per un elenco delle mappature predefinite degli attributi utente in IAM Identity Center agli attributi utente nella directory AWS Managed Microsoft AD , consulta. Mappature predefinite

Scelta degli attributi quando si utilizza un provider di identità esterno come fonte di identità

Quando configuri IAM Identity Center con un provider di identità esterno (IdP) come fonte di identità, ci sono due modi per utilizzare gli attributi per ABAC.

- Puoi configurare il tuo IdP per inviare gli attributi tramite asserzioni SAML. In questo caso, IAM Identity Center trasmette il nome e il valore dell'attributo dall'IdP per la valutazione delle policy.

  > **Note**
  >
  > Gli attributi nelle asserzioni SAML non saranno visibili nella pagina Attributi per il controllo degli accessi. Dovrai conoscere questi attributi in anticipo e aggiungerli alle regole di controllo degli accessi quando crei le politiche. Se decidi di affidarti IdPs agli attributi esterni, questi attributi verranno sempre trasmessi quando gli utenti si uniscono Account AWS. Negli scenari in cui gli stessi attributi arrivano a IAM Identity Center tramite SAML e SCIM, il valore degli attributi SAML ha la precedenza nelle decisioni sul controllo degli accessi.

- È possibile configurare gli attributi da utilizzare dalla pagina Attributi per il controllo degli accessi nella console IAM Identity Center. I valori degli attributi che scegli qui sostituiscono i valori per tutti gli attributi corrispondenti che provengono da un IdP tramite un'asserzione. A seconda che stiate usando SCIM, considerate quanto segue:
  - Se si utilizza SCIM, l'IdP sincronizza automaticamente i valori degli attributi in IAM Identity Center. Gli attributi aggiuntivi necessari per il controllo degli accessi potrebbero non essere presenti nell'elenco degli attributi SCIM. In tal caso, prendi in considerazione la possibilità di collaborare con l'amministratore IT del tuo IdP per inviare tali attributi a IAM Identity Center tramite asserzioni SAML utilizzando il prefisso richiesto. `https://aws.amazon.com/SAML/Attributes/AccessControl:` Per informazioni su come configurare gli attributi utente per il controllo degli accessi nel tuo IdP da inviare tramite asserzioni SAML, consulta la sezione per Tutorial introduttivi il tuo IdP.
  - Se non utilizzi SCIM, devi aggiungere manualmente gli utenti e impostarne gli attributi proprio come se stessi utilizzando IAM Identity Center come fonte di identità. Successivamente, vai alla pagina Attributi per il controllo degli accessi e scegli gli attributi che desideri utilizzare nelle politiche.

Per un elenco completo degli attributi utente supportati dagli attributi utente in IAM Identity Center agli attributi utente esterni IdPs, consultaAttributi del provider di identità esterno supportati.

Per iniziare a usare ABAC in IAM Identity Center, consulta i seguenti argomenti.

Argomenti

- Abilita e configura gli attributi per il controllo degli accessi
- Crea politiche di autorizzazione per ABAC in IAM Identity Center

Abilita e configura gli attributi per il controllo degli accessi

Per utilizzare ABAC in tutti i casi, devi prima abilitare ABAC utilizzando la console IAM Identity Center o l'API IAM Identity Center. Se scegli di utilizzare IAM Identity Center per selezionare gli attributi, utilizzi la pagina Attributi per il controllo degli accessi nella console IAM Identity Center o nell'API IAM Identity Center. Se utilizzi un provider di identità esterno (IdP) come origine di identità e scegli di inviare gli attributi tramite le asserzioni SAML, configuri il tuo IdP per passare gli attributi. Se un'asserzione SAML trasmette uno di questi attributi, Centro identità IAM sostituirà il valore dell'attributo con il valore ricavato dall'archivio identità di Centro identità IAM. Quando gli utenti effettuano la federazione nei propri account, verranno inviati solo gli attributi configurati in IAM Identity Center per prendere decisioni sul controllo degli accessi.

> **Note**
>
> Non è possibile visualizzare gli attributi configurati e inviati da un IdP esterno dalla pagina Attributi per il controllo degli accessi nella console IAM Identity Center. Se stai passando gli attributi di controllo dell'accesso nelle asserzioni SAML dal tuo IdP esterno, tali attributi vengono inviati direttamente a Account AWS quando gli utenti si federano. Gli attributi non saranno disponibili in IAM Identity Center per la mappatura.

Abilita gli attributi per il controllo degli accessi

Utilizza la seguente procedura per abilitare la funzionalità di controllo degli attributi di accesso (ABAC) utilizzando la console IAM Identity Center.

> **Note**
>
> Se disponi di set di autorizzazioni esistenti e prevedi di abilitare ABAC nella tua istanza IAM Identity Center, ulteriori restrizioni di sicurezza richiedono che tu disponga innanzitutto della

`iam:UpdateAssumeRolePolicy` policy. Queste restrizioni di sicurezza aggiuntive non sono necessarie se non hai creato alcun set di autorizzazioni nel tuo account.

Per abilitare gli attributi per il controllo degli accessi

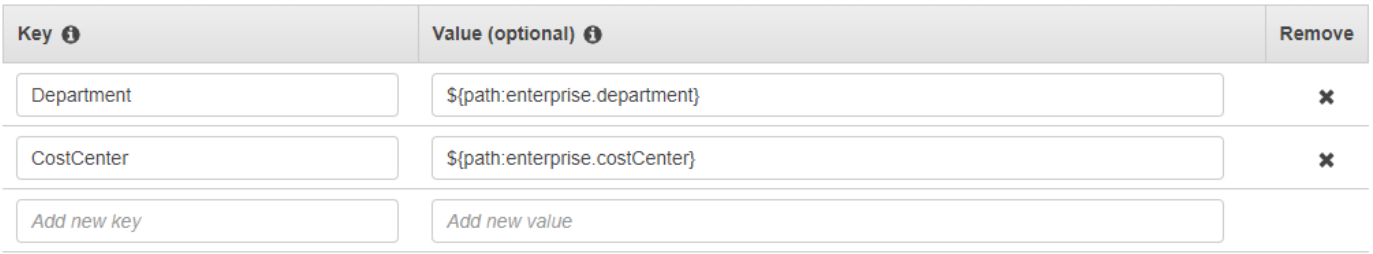
1. Apri la console IAM Identity Center.
2. Scegli Impostazioni
3. Nella pagina Impostazioni, individua la casella Attributi per le informazioni sul controllo di accesso, quindi scegli Abilita. Prosegui con la procedura successiva per configurarlo.

Seleziona i tuoi attributi

Utilizzate la seguente procedura per impostare gli attributi per la vostra configurazione ABAC.

Per selezionare gli attributi utilizzando la console IAM Identity Center

1. Apri la console IAM Identity Center.
2. Scegli Impostazioni
3. Nella pagina Impostazioni, scegli la scheda Attributi per il controllo degli accessi, quindi scegli Gestisci attributi.
4. Nella pagina Attributi per il controllo degli accessi, scegli Aggiungi attributo e inserisci i dettagli della chiave e del valore. Qui è dove mapperai l'attributo proveniente dalla tua origine di identità a un attributo che IAM Identity Center passa come tag di sessione.



La chiave rappresenta il nome che stai dando all'attributo da utilizzare nelle politiche. Può essere qualsiasi nome arbitrario, ma è necessario specificare quel nome esatto nelle politiche create per il controllo degli accessi. Ad esempio, supponiamo che tu stia utilizzando Okta (un IdP esterno) come fonte di identità e che sia necessario trasmettere i dati del centro di costo dell'organizzazione come tag di sessione. In Key, inseriresti un nome simile CostCenter a quello della tua chiave. È importante notare che qualunque nome tu scelga qui, deve avere lo stesso

nome nel tuo Chiave di condizione aws:PrincipalTag (ovvero,`"ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"`).

> **Note**
>
> Usa un attributo a valore singolo per la tua chiave, ad esempio. **`Manager`** IAM Identity Center non supporta attributi multivalore per ABAC, ad esempio. **`Manager, IT Systems`**

Il valore rappresenta il contenuto dell'attributo proveniente dalla fonte di identità configurata. Qui puoi inserire qualsiasi valore dalla tabella di origine dell'identità appropriata elencata inAWS Managed Microsoft AD Mappature degli attributi per le directory. Ad esempio, utilizzando il contesto fornito nell'esempio precedente, esamineresti l'elenco degli attributi IdP supportati e stabiliresti che sarebbe **`${path:enterprise.costCenter}`**la corrispondenza più vicina a un attributo supportato, quindi lo inseriresti nel campo Valore. Vedi lo screenshot fornito sopra come riferimento. Tieni presente che non puoi utilizzare valori di attributi IdP esterni al di fuori di questo elenco per ABAC a meno che non utilizzi l'opzione di passare gli attributi tramite l'asserzione SAML.

5. Seleziona Salvataggio delle modifiche.

Ora che hai configurato la mappatura degli attributi di controllo degli accessi, devi completare il processo di configurazione ABAC. A tale scopo, create le regole ABAC e aggiungetele ai set di autorizzazioni e/o alle politiche basate sulle risorse. Ciò è necessario per consentire alle identità degli utenti di accedere alle risorse. AWS Per ulteriori informazioni, consulta Crea politiche di autorizzazione per ABAC in IAM Identity Center.

Disabilitazione di attributi per il controllo degli accessi

Utilizzare la procedura seguente per disabilitare la funzione ABAC ed eliminare tutte le mappature degli attributi che sono state configurate.

Per disabilitare gli attributi per il controllo degli accessi

1. Apri la console IAM Identity Center.
2. Scegli Impostazioni

3. Nella pagina Impostazioni, scegli la scheda Attributi per il controllo degli accessi, quindi scegli Disabilita.
4. Nella finestra di dialogo Disabilita gli attributi per il controllo degli accessi, rivedi le informazioni e, quando sei pronto, inserisci ELIMINA, quindi scegli Conferma.

> **Important**
>
> Questo passaggio elimina tutti gli attributi che sono stati configurati. Una volta eliminati, gli attributi ricevuti da un'origine di identità e gli attributi personalizzati precedentemente configurati non verranno passati.

Crea politiche di autorizzazione per ABAC in IAM Identity Center

Puoi creare politiche di autorizzazione che determinano chi può accedere alle tue AWS risorse in base al valore dell'attributo configurato. Quando abiliti ABAC e specifichi gli attributi, IAM Identity Center trasmette il valore dell'attributo dell'utente autenticato a IAM per utilizzarlo nella valutazione delle policy.

Chiave di condizione aws:PrincipalTag

È possibile utilizzare gli attributi di controllo degli accessi nei set di autorizzazioni utilizzando la chiave di `aws:PrincipalTag` condizione per creare regole di controllo degli accessi. Ad esempio, nella seguente politica di fiducia è possibile etichettare tutte le risorse dell'organizzazione con i rispettivi centri di costo. È inoltre possibile utilizzare un unico set di autorizzazioni che consente agli sviluppatori di accedere alle risorse dei propri centri di costo. Ora, ogni volta che gli sviluppatori si uniscono all'account utilizzando il Single Sign-On e l'attributo relativo al centro di costo, ottengono l'accesso solo alle risorse dei rispettivi centri di costo. Man mano che il team aggiunge più sviluppatori e risorse al proprio progetto, devi solo etichettare le risorse con il centro di costo corretto. Quindi trasmetti le informazioni sui centri di costo nella AWS sessione in cui gli sviluppatori si uniscono Account AWS. Di conseguenza, man mano che l'organizzazione aggiunge nuove risorse e gli sviluppatori al centro di costo, gli sviluppatori possono gestire le risorse in linea con i propri centri di costo senza bisogno di aggiornamenti delle autorizzazioni.

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

```
            "Action": [
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"
                }
            }
        }
    ]
}
```

Per ulteriori informazioni, consulta aws:PrincipalTage EC2: Avvia o interrompi le istanze in base alla corrispondenza dei tag principali e di risorsa nella IAM User Guide.

Se le policy contengono attributi non validi nelle loro condizioni, la condizione della policy fallirà e l'accesso verrà negato. Per ulteriori informazioni, consulta Errore «Si è verificato un errore imprevisto» quando un utente tenta di accedere utilizzando un provider di identità esterno.

Provider di identità IAM

Quando aggiungi l'accesso Single Sign-On a un Account AWS IAM Identity Center crea un provider di identità IAM in ciascuno di essi. Account AWS Un provider di identità IAM aiuta a mantenere la tua Account AWS sicurezza perché non devi distribuire o incorporare credenziali di sicurezza a lungo termine, come le chiavi di accesso, nella tua applicazione.

Ripara il provider di identità IAM

Se elimini o modifichi accidentalmente il tuo provider di identità, devi riapplicare manualmente le assegnazioni a utenti e gruppi. La riapplicazione delle assegnazioni a utenti e gruppi ricrea il provider di identità. Per ulteriori informazioni, consultare:

- Gestisci l'accesso a Account AWS
- Gestire l'accesso alle applicazioni

Ruoli collegati ai servizi

I ruoli collegati ai servizi sono autorizzazioni IAM predefinite che consentono a IAM Identity Center di delegare e stabilire quali utenti hanno accesso Single Sign-On a determinati membri dell'organizzazione. Account AWS AWS Organizations Il servizio abilita questa funzionalità fornendo un ruolo collegato al servizio in ogni parte della sua organizzazione. Account AWS Il servizio consente quindi ad altri AWS servizi come IAM Identity Center di sfruttare tali ruoli per eseguire attività relative ai servizi. Per ulteriori informazioni, consulta AWS Organizations i ruoli collegati ai servizi.

Quando abiliti IAM Identity Center, IAM Identity Center crea un ruolo collegato ai servizi in tutti gli account all'interno dell'organizzazione in. AWS Organizations IAM Identity Center crea inoltre lo stesso ruolo collegato ai servizi in ogni account che viene successivamente aggiunto all'organizzazione. Questo ruolo consente a IAM Identity Center di accedere alle risorse di ciascun account per tuo conto. Per ulteriori informazioni, consulta Gestisci l'accesso a Account AWS.

I ruoli collegati ai servizi che vengono creati in ciascuno di essi Account AWS sono denominati. `AWSServiceRoleForSSO` Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per IAM Identity Center.

Gestire l'accesso alle applicazioni

Con AWS IAM Identity Center, puoi controllare chi può avere accesso Single Sign-On alle tue applicazioni. Gli utenti ottengono un accesso semplice a queste applicazioni dopo aver utilizzato le credenziali di directory per accedere.

IAM Identity Center comunica in modo sicuro con queste applicazioni attraverso una relazione di fiducia tra IAM Identity Center e il fornitore di servizi dell'applicazione. Questa fiducia può essere creata in diversi modi, a seconda del tipo di applicazione.

IAM Identity Center supporta due tipi di applicazioni: applicazioni AWS gestite e applicazioni gestite dai clienti. AWS le applicazioni gestite vengono configurate direttamente dall'interno delle console applicative pertinenti o tramite le API dell'applicazione. Le applicazioni gestite dal cliente devono essere aggiunte alla console IAM Identity Center e configurate con i metadati appropriati sia per IAM Identity Center che per il fornitore di servizi.

Dopo aver configurato le applicazioni per utilizzarle con IAM Identity Center, puoi gestire quali utenti o gruppi accedono alle applicazioni. Per impostazione predefinita, nessun utente è assegnato alle applicazioni.

Puoi anche concedere ai tuoi dipendenti l'accesso AWS Management Console a un gruppo specifico Account AWS dell'organizzazione. Per ulteriori informazioni, consulta Gestisci l'accesso a Account AWS.

Argomenti

AWS applicazioni gestite

AWS le applicazioni gestite si integrano con IAM Identity Center e possono utilizzarle per i servizi di autenticazione e directory.

L'integrazione delle applicazioni AWS gestite con IAM Identity Center offre un percorso più semplice per assegnare l'accesso agli utenti, senza la necessità di configurare una federazione o una sincronizzazione di utenti e gruppi separate per ciascuna applicazione. Puoi connettere la fonte di identità che desideri utilizzare per l'autenticazione una sola volta e riceverai una visualizzazione unica delle assegnazioni di utenti e gruppi. Gli amministratori delle applicazioni che consentono la propagazione affidabile delle identità sono in grado di definire e controllare l'accesso alle risorse delle proprie applicazioni in base all'appartenenza di un utente o al gruppo dell'utente, senza la necessità di mapparle ai ruoli IAM.

AWS le applicazioni gestite forniscono un'interfaccia utente amministrativa che è possibile utilizzare per gestire l'accesso alle risorse delle applicazioni. Ad esempio, QuickSight gli amministratori possono assegnare agli utenti l'accesso ai dashboard in base all'appartenenza al gruppo. La maggior parte delle applicazioni AWS gestite offre inoltre un' AWS Management Console esperienza che consente di assegnare utenti all'applicazione. L'esperienza da console per queste applicazioni potrebbe integrare entrambe le funzioni, per combinare le funzionalità di assegnazione degli utenti con la capacità di gestire l'accesso alle risorse delle applicazioni.

AWS le applicazioni gestite integrate con IAM Identity Center includono:

AWS applicazioni gestite che si integrano con IAM Identity Center

AWS applicazione gestita	Integrato con l'istanza organizzativa di IAM Identity Center	Integrato con le istanze di account di IAM Identity Center	Consente la propagazione affidabile delle identità tramite IAM Identity Center
Amazon Athena SQL	 S	 S	 Sì

AWS applicazione gestita	Integrato con l'istanza organizzativa di IAM Identity Center	Integrato con le istanze di account di IAM Identity Center	Consente la propagazione affidabile delle identità tramite IAM Identity Center
Amazon CodeCatalyst	 S	 S	 No
Notebook Amazon EMR	 S	 N	 No
Amazon EMR su Amazon EC2	 S	 S	 Sì
Amazon EMR Studio	 S	 S	 Sì
Amazon Kendra	 S	 N	 No
Grafana gestito da Amazon	 S	 N	 No
Amazon Monitron	 S	 N	 No

AWS applicazione gestita	Integrato con l'istanza organizzativa di IAM Identity Center	Integrato con le istanze di account di IAM Identity Center	Consente la propagazione affidabile delle identità tramite IAM Identity Center
Amazon Nimble Studio	 S	 N	 No
Amazon Pinpoint	 S	 N	 No
Amazon Q Business	 S	 S	 No
Sviluppatore Amazon Q	 S	 S	 No
Amazon QuickSight	 S	 S	 Sì
Amazon Redshift	 S	 S	 Sì
Concessioni di accesso ad Amazon S3	 S	 S	 Sì

AWS applicazione gestita	Integrato con l'istanza organizzativa di IAM Identity Center	Integrato con le istanze di account di IAM Identity Center	Consente la propagazione affidabile delle identità tramite IAM Identity Center
Amazon SageMaker Studio	 S	 N	 No
Amazon WorkSpaces Web	 S	 N	 No
AWS CLI	 S	 N	 No
AWS Deadline Cloud	 S	 S	 No
AWS IoT Events	 S	 N	 No
AWS IoT Fleet Hub	 S	 N	 No
AWS IoT SiteWise	 S	 N	 No

AWS applicazione gestita	Integrato con l'istanza organizzativa di IAM Identity Center	Integrato con le istanze di account di IAM Identity Center	Consente la propagazione affidabile delle identità tramite IAM Identity Center
AWS Lake Formation	 S	 S	 Sì
Catena di approvvigionamento di AWS	 S	 N	 No
AWS Systems Manager	 S	 N	 No
Accesso verificato da AWS	 S	 N	 No

* Le istanze di account di IAM Identity Center sono supportate a meno che gli utenti non richiedano l'accesso ad Amazon Q dalla AWS console.

Argomenti

- Controllo dell'accesso
- Coordinamento delle attività amministrative
- Configurazione di IAM Identity Center per condividere le informazioni sull'identità
- Considerazioni sulla condivisione delle informazioni sull'identità in Account AWS
- Attivazione di sessioni di console con riconoscimento dell'identità
- Limitazione dell'uso di applicazioni gestite AWS
- Visualizzazione dei dettagli su un'applicazione AWS gestita
- Disabilitazione di un'applicazione gestita AWS

Controllo dell'accesso

L'accesso alle applicazioni AWS gestite è controllato in due modi:

- Accesso iniziale all'applicazione: IAM Identity Center lo gestisce tramite assegnazioni all'applicazione. Per impostazione predefinita, le assegnazioni sono obbligatorie per le applicazioni AWS gestite.
- Accesso alle risorse dell'applicazione: l'applicazione lo gestisce tramite assegnazioni di risorse indipendenti che controlla.

Coordinamento delle attività amministrative

Se sei un amministratore dell'applicazione, puoi scegliere se richiedere assegnazioni a un'applicazione. Se sono richieste assegnazioni, quando gli utenti AWS accedono al portale di accesso, solo gli utenti assegnati all'applicazione direttamente o tramite un'assegnazione di gruppo possono visualizzare il riquadro dell'applicazione. In alternativa, se le assegnazioni non sono richieste, puoi consentire a tutti gli utenti di IAM Identity Center di accedere all'applicazione. In questo caso, l'applicazione gestisce l'accesso alle risorse e il riquadro dell'applicazione è visibile a tutti gli utenti che visitano il portale di AWS accesso.

Se sei un amministratore di IAM Identity Center, puoi utilizzare la console IAM Identity Center per rimuovere le assegnazioni alle applicazioni AWS gestite. Prima di rimuovere le assegnazioni, ti consigliamo di coordinarti con l'amministratore dell'applicazione. È inoltre necessario coordinarsi con l'amministratore dell'applicazione se si intende modificare l'impostazione che determina se sono necessarie le assegnazioni o automatizzare le assegnazioni delle applicazioni.

Configurazione di IAM Identity Center per condividere le informazioni sull'identità

IAM Identity Center fornisce un archivio di identità che contiene gli attributi di utenti e gruppi, escluse le credenziali di accesso. Puoi utilizzare uno dei seguenti metodi per mantenere aggiornati gli utenti e i gruppi nel tuo archivio di identità IAM Identity Center:

- Utilizza l'archivio di identità IAM Identity Center come fonte di identità principale. Se scegli questo metodo, gestisci gli utenti, le loro credenziali di accesso e i gruppi dall'interno della console IAM Identity Center o AWS Command Line Interface ()AWS CLI. Per ulteriori informazioni, consulta Gestisci le identità in IAM Identity Center.

- Imposta il provisioning (sincronizzazione) di utenti e gruppi provenienti da una delle seguenti fonti di identità nel tuo archivio di identità IAM Identity Center:
  - Active Directory: per ulteriori informazioni, consulta. Connect a una Microsoft AD directory
  - Provider di identità esterno: per ulteriori informazioni, vedereConnect a un provider di identità esterno.

  Se scegli questo metodo di provisioning, continui a gestire utenti e gruppi dall'interno della tua fonte di identità e tali modifiche vengono sincronizzate con l'archivio di identità di IAM Identity Center.

Qualunque sia la fonte di identità scelta, IAM Identity Center può condividere le informazioni su utenti e gruppi con AWS applicazioni gestite. In questo modo, puoi connettere una fonte di identità a IAM Identity Center una sola volta e poi condividere le informazioni sull'identità con più applicazioni in. Cloud AWS Ciò elimina la necessità di configurare in modo indipendente la federazione e il provisioning delle identità con ciascuna applicazione. Questa funzionalità di condivisione semplifica inoltre l'accesso degli utenti a molte applicazioni diverse Account AWS.

Considerazioni sulla condivisione delle informazioni sull'identità in Account AWS

IAM Identity Center supporta gli attributi più comunemente utilizzati in tutte le applicazioni. Questi attributi includono nome e cognome, numero di telefono, indirizzo e-mail, indirizzo e lingua preferita. Valuta attentamente quali applicazioni e quali account possono utilizzare queste informazioni di identificazione personale.

È possibile controllare l'accesso a queste informazioni in uno dei seguenti modi. Puoi scegliere di abilitare l'accesso solo nell'account di AWS Organizations gestione o in tutti gli account in AWS Organizations. In alternativa, è possibile utilizzare le policy di controllo dei servizi (SCP) per controllare quali applicazioni possono accedere alle informazioni in quali account. AWS Organizations Ad esempio, se si abilita l'accesso solo nell'account di AWS Organizations gestione, le applicazioni negli account dei membri non hanno accesso alle informazioni. Tuttavia, se abiliti l'accesso in tutti gli account, puoi utilizzare SCP per impedire l'accesso a tutte le applicazioni ad eccezione di quelle che desideri autorizzare.

Attivazione di sessioni di console con riconoscimento dell'identità

Una sessione con riconoscimento dell'identità per la console migliora la sessione di AWS console di un utente fornendo un contesto utente aggiuntivo per personalizzare l'esperienza dell'utente. Questa funzionalità è attualmente supportata per gli utenti di Amazon Q nella AWS console.

Oggi puoi abilitare sessioni di console con riconoscimento dell'identità senza apportare modifiche ai modelli di accesso esistenti o alla federazione nella AWS console. Se i tuoi utenti accedono alla AWS console con IAM (ad esempio, se accedono come utenti IAM o tramite accesso federato con IAM), possono continuare a utilizzare questi metodi. Se i tuoi utenti AWS accedono al portale di accesso, possono continuare a utilizzare le proprie credenziali utente IAM Identity Center.

Argomenti

Prerequisiti e considerazioni

Prima di abilitare le sessioni della console con riconoscimento dell'identità, esamina i seguenti prerequisiti e considerazioni:

- È necessario abilitare le sessioni di console con riconoscimento dell'identità per gli utenti che richiedono l'accesso ad Amazon Q nella console. AWS
- Le sessioni di console con riconoscimento dell'identità sono attualmente supportate solo per l'uso con Amazon Q nella console. AWS
- Le sessioni di console con riconoscimento dell'identità richiedono un'istanza organizzativa di IAM Identity Center.
- L'integrazione con Amazon Q non è supportata se abiliti IAM Identity Center in un opt-in Regione AWS.
- Dopo aver abilitato le sessioni di console con riconoscimento dell'identità, non puoi disabilitare questa funzionalità.
- Per abilitare le sessioni di console con riconoscimento dell'identità, devi disporre delle seguenti autorizzazioni:
  - `sso:CreateApplication`

- `sso:GetSharedSsoConfiguration`
- `sso:ListApplications`
- `sso:PutApplicationAssignmentConfiguration`
- `sso:PutApplicationAuthenticationMethod`
- `sso:PutApplicationGrant`
- `sso:PutApplicationAccessScope`
- `signin:CreateTrustedIdentityPropagationApplicationForConsole`
- `signin:ListTrustedIdentityPropagationApplicationForConsole`
-

- Per consentire agli utenti di utilizzare sessioni di console con riconoscimento dell'identità, è necessario concedere loro l'autorizzazione in base a una politica basata sull'identità. `sts:setContext` Per informazioni, consulta Concessione agli utenti delle autorizzazioni per l'utilizzo di sessioni di console con riconoscimento dell'identità.

Come abilitare le sessioni identity-aware-console

Puoi abilitare sessioni di console con riconoscimento dell'identità nella console Amazon Q o nella console IAM Identity Center.

Abilita sessioni di console con riconoscimento dell'identità nella console Amazon Q

Prima di abilitare le sessioni di console con riconoscimento dell'identità, è necessario disporre di un'istanza organizzativa di IAM Identity Center con una fonte di identità connessa. Se hai già configurato IAM Identity Center, vai al passaggio 3.

1. Apri la console IAM Identity Center. Scegli Enable e crea un'istanza organizzativa di IAM Identity Center. Per informazioni, consulta Abilitazione AWS IAM Identity Center.
2. Connetti la tua fonte di identità a IAM Identity Center e fornisci agli utenti IAM Identity Center. Puoi scegliere la directory IAM Identity Center predefinita come fonte di identità oppure puoi utilizzare un altro provider di identità. Per ulteriori informazioni, consulta Tutorial introduttivi.
3. Dopo aver completato la configurazione di IAM Identity Center, apri la console Amazon Q e segui i passaggi in Abbonamenti nella Amazon Q Developer User Guide. Assicurati di abilitare le sessioni di console con riconoscimento dell'identità.

> **Note**
>
> Se non disponi di autorizzazioni sufficienti per abilitare le sessioni di console con riconoscimento dell'identità, potresti dover chiedere a un amministratore di IAM Identity Center di eseguire questa attività per te nella console IAM Identity Center. Per ulteriori informazioni, consulta la procedura successiva.

Abilita le sessioni di console con riconoscimento dell'identità nella console IAM Identity Center

Se sei un amministratore di IAM Identity Center, un altro amministratore potrebbe chiederti di abilitare le sessioni di console con riconoscimento dell'identità nella console IAM Identity Center.

1. Apri la console IAM Identity Center.
2. Nel pannello di navigazione scegli Impostazioni.
3. In Abilita sessioni con riconoscimento dell'identità, scegli Abilita.
4. Nel secondo messaggio, scegli Abilita.
5. Dopo aver abilitato le sessioni della console con riconoscimento dell'identità, viene visualizzato un messaggio di conferma nella parte superiore della pagina Impostazioni.
6. Nella sezione Dettagli, lo stato delle sessioni con riconoscimento dell'identità è Abilitato.

Come funzionano le sessioni di console con riconoscimento dell'identità

Con le sessioni di console con riconoscimento dell'identità, gli utenti di Amazon Q nella AWS console possono accedere AWS, aprire il sito AWS Management Console o un altro AWS sito Web, scegliere l'icona di Amazon Q e avviare una chat o utilizzare altre funzionalità supportate. Per ulteriori informazioni, consulta la Amazon Q Developer User Guide.

IAM Identity Center migliora la sessione corrente della console di un utente per includere l'ID dell'utente IAM Identity Center attivo e l'ID di sessione IAM Identity Center.

Le sessioni di console con riconoscimento dell'identità includono i seguenti tre valori:

- Identity Store user ID (archivio di identità: UserId): questo valore viene utilizzato per identificare in modo univoco un utente nella fonte di identità connessa a IAM Identity Center.

- Identity store directory ARN (archivio di identità: IdentityStoreArn): questo valore è l'ARN dell'archivio di identità connesso a IAM Identity Center e per cui è possibile cercare gli attributi. `identitystore:UserId`
- ID di sessione IAM Identity Center: questo valore indica se la sessione IAM Identity Center dell'utente è ancora valida.

I valori sono gli stessi, ma ottenuti in modi diversi e aggiunti in diversi punti del processo, a seconda di come l'utente accede:

- IAM Identity Center (portale di AWS accesso): in questo caso, l'ID utente e i valori ARN dell'archivio di identità dell'utente sono già forniti nella sessione attiva di IAM Identity Center. IAM Identity Center migliora la sessione corrente aggiungendo solo l'ID di sessione.
- Altri metodi di accesso: se l'utente accede AWS come utente IAM, con un ruolo IAM o come utente federato con IAM, nessuno di questi valori viene fornito. IAM Identity Center migliora la sessione corrente aggiungendo l'ID utente dell'archivio di identità, l'ARN della directory dell'archivio di identità e l'ID della sessione.

Limitazione dell'uso di applicazioni gestite AWS

Quando si abilita IAM Identity Center per la prima volta, AWS consente l'uso automatico delle applicazioni AWS gestite in tutti gli account di. AWS Organizations Per limitare le applicazioni, è necessario implementare gli SCP. Puoi utilizzare gli SCP per bloccare l'accesso alle informazioni su utenti e gruppi di IAM Identity Center e impedire l'avvio dell'applicazione, tranne che negli account designati.

Visualizzazione dei dettagli su un'applicazione AWS gestita

Dopo aver connesso un'applicazione AWS gestita a IAM Identity Center utilizzando la console o le API dell'applicazione, l'applicazione viene registrata con IAM Identity Center. Dopo aver registrato un'applicazione con IAM Identity Center, è possibile visualizzare informazioni dettagliate sull'applicazione nella console IAM Identity Center.

Per visualizzare informazioni su un'applicazione AWS gestita nella console IAM Identity Center

1. Apri la console IAM Identity Center.
2. Selezionare Applications (Applicazioni).
3. Scegli la scheda Applicazioni AWS gestite.

4. Nell'elenco delle applicazioni, scegli il nome dell'applicazione per la quale desideri visualizzare informazioni dettagliate.
5. Le informazioni sull'applicazione includono se sono necessarie le assegnazioni di utenti e gruppi e, se applicabile, utenti e gruppi assegnati e applicazioni affidabili per la propagazione delle identità. Per informazioni sulla propagazione delle identità affidabili, vedere. Propagazione delle identità attendibili tra le applicazioni

Disabilitazione di un'applicazione gestita AWS

Per impedire agli utenti di autenticarsi su un'applicazione AWS gestita, puoi disabilitare l'applicazione nella console IAM Identity Center.

> **Warning**
>
> La disabilitazione di un'applicazione elimina tutte le autorizzazioni utente per questa applicazione, disconnette l'applicazione da IAM Identity Center e rende l'applicazione inaccessibile. Se sei un amministratore di IAM Identity Center, ti consigliamo di coordinarti con l'amministratore dell'applicazione prima di eseguire questa attività.

Per disabilitare un'applicazione AWS gestita

1. Apri la console IAM Identity Center.
2. Selezionare Applications (Applicazioni).
3. Nella pagina Applicazioni, in Applicazioni AWS gestite, scegli l'applicazione che desideri disabilitare.
4. Con l'applicazione selezionata, scegli Azioni, quindi scegli Disabilita.
5. Nella finestra di dialogo Sospendi l'applicazione, scegliete Sospendi.
6. Nell'elenco delle applicazioni AWS gestite, lo stato dell'applicazione appare come Inattivo.

Applicazioni gestite dal cliente

Con IAM Identity Center, puoi creare o connettere gli utenti della forza lavoro e gestire centralmente il loro accesso a tutte le loro Account AWS applicazioni. IAM Identity Center funge da servizio di identità centrale e offre diversi modi per autenticare gli utenti. Se utilizzi già un provider di identità

(IdP), IAM Identity Center può integrarsi con il tuo IdP in modo da poter fornire utenti e gruppi in IAM Identity Center e utilizzare il tuo IdP per l'autenticazione.

Se utilizzi applicazioni gestite dai clienti che supportano SAML 2.0, puoi federare il tuo IdP a IAM Identity Center tramite SAML 2.0 e utilizzare IAM Identity Center per gestire l'accesso degli utenti a tali applicazioni. IAM Identity Center fornisce un catalogo di applicazioni di uso comune che supportano SAML 2.0, come Salesforce e Microsoft 365. Questo catalogo è disponibile nella console IAM Identity Center. Puoi anche configurare le tue applicazioni SAML 2.0.

> **Note**
>
> Se disponi di applicazioni gestite dai clienti che supportano OAuth 2.0 e i tuoi utenti devono accedere da queste applicazioni ai AWS servizi, puoi utilizzare la propagazione affidabile delle identità. Con la propagazione affidabile delle identità, un utente può accedere a un'applicazione e tale applicazione può trasmettere l'identità degli utenti nelle richieste di accesso ai dati nei servizi. AWS Per ulteriori informazioni, consulta Utilizzo della propagazione affidabile delle identità con applicazioni gestite dal cliente.

Argomenti

SAML 2.0 e OAuth 2.0

IAM Identity Center ti consente di fornire ai tuoi utenti l'accesso Single Sign-On alle applicazioni SAML 2.0 o OAuth 2.0. I seguenti argomenti forniscono una panoramica di alto livello di SAML 2.0 e OAuth 2.0.

Argomenti

SAML 2.0

SAML 2.0 è uno standard di settore utilizzato per lo scambio sicuro di asserzioni SAML che trasmettono informazioni su un utente tra un'autorità SAML (chiamata provider di identità o IdP) e

un consumatore SAML 2.0 (chiamato service provider o SP). IAM Identity Center utilizza queste informazioni per fornire un accesso single sign-on federato agli utenti autorizzati a utilizzare le applicazioni all'interno del portale di accesso. AWS

OAuth 2.0

OAuth 2.0 è un protocollo che consente alle applicazioni di accedere e condividere i dati degli utenti in modo sicuro senza condividere le password. Questa funzionalità offre agli utenti un modo sicuro e standardizzato per consentire alle applicazioni di accedere alle proprie risorse. L'accesso è facilitato da diversi flussi di concessione OAuth 2.0.

IAM Identity Center consente alle applicazioni eseguite su client pubblici di recuperare credenziali temporanee per l'accesso Account AWS e i servizi in modo programmatico per conto dei propri utenti. I client pubblici sono in genere desktop, laptop o altri dispositivi mobili utilizzati per eseguire applicazioni localmente. Esempi di AWS applicazioni eseguite su client pubblici includono AWS Command Line Interface (AWS CLI) e i AWS Software Development Kit (SDK). Kit di strumenti AWS Per consentire a queste applicazioni di ottenere credenziali, IAM Identity Center supporta parti dei seguenti flussi OAuth 2.0:

- Concessione del codice di autorizzazione con Proof Key for Code Exchange (PKCE) (RFC 6749 e RFC 7636)
- Concessione di autorizzazione del dispositivo (RFC 8628)

> **Note**
>
> Questi tipi di concessione possono essere utilizzati solo con chi supporta Servizi AWS questa funzionalità. Questi servizi potrebbero non supportare affatto questo tipo di sovvenzione Regioni AWS. Consulta la documentazione Servizi AWS relativa alle differenze regionali.

OpenID Connect (OIDC) è un protocollo di autenticazione basato sul framework OAuth 2.0. OIDC specifica come utilizzare OAuth 2.0 per l'autenticazione. Tramite le API del servizio OIDC di IAM Identity Center, un'applicazione registra un client OAuth 2.0 e utilizza uno di questi flussi per ottenere un token di accesso che fornisce le autorizzazioni alle API protette di IAM Identity Center. Un'applicazione specifica gli ambiti di accesso per dichiarare l'utente API previsto. Dopo che, in qualità di amministratore di IAM Identity Center, hai configurato la fonte di identità, gli utenti finali dell'applicazione devono completare una procedura di accesso, se non l'hanno già fatto. Gli utenti

finali devono quindi fornire il proprio consenso per consentire all'applicazione di effettuare chiamate API. Queste chiamate API vengono effettuate utilizzando le autorizzazioni degli utenti. In risposta, IAM Identity Center restituisce un token di accesso all'applicazione che contiene gli ambiti di accesso a cui gli utenti hanno acconsentito.

Utilizzo di un flusso di concessioni OAuth 2.0

I flussi di concessione OAuth 2.0 sono disponibili solo tramite applicazioni AWS gestite che supportano i flussi. Per utilizzare un flusso OAuth 2.0, l'istanza di IAM Identity Center e tutte le applicazioni AWS gestite supportate che utilizzi devono essere distribuite in un'unica soluzione. Regione AWS Consulta la documentazione relativa a ciascuna di esse Servizio AWS per determinare la disponibilità regionale delle applicazioni AWS gestite e l'istanza di IAM Identity Center che desideri utilizzare.

Per utilizzare un'applicazione che utilizza un flusso OAuth 2.0, l'utente finale deve inserire l'URL a cui l'applicazione si connetterà e si registrerà con l'istanza di IAM Identity Center. A seconda dell'applicazione, in qualità di amministratore, devi fornire ai tuoi utenti l'URL del portale di AWS accesso o l'URL dell'emittente della tua istanza di IAM Identity Center. Puoi trovare queste due impostazioni nella pagina delle impostazioni della console IAM Identity Center. Per ulteriori informazioni sulla configurazione di un'applicazione client, consulta la documentazione dell'applicazione.

L'esperienza dell'utente finale per accedere a un'applicazione e fornire il consenso dipende dal fatto che l'applicazione utilizzi Concessione del codice di autorizzazione con PKCE o Concessione di autorizzazione del dispositivo meno.

Concessione del codice di autorizzazione con PKCE

Questo flusso viene utilizzato dalle applicazioni eseguite su un dispositivo dotato di browser.

1. Si apre una finestra del browser.
2. Se l'utente non si è autenticato, il browser lo reindirizza per completare l'autenticazione dell'utente.
3. Dopo l'autenticazione, all'utente viene presentata una schermata di consenso che mostra le seguenti informazioni:
   - Il nome dell'applicazione
   - Gli ambiti di accesso per i quali l'applicazione richiede il consenso all'uso
4. L'utente può annullare la procedura di consenso o dare il proprio consenso e l'applicazione procede con l'accesso in base alle autorizzazioni dell'utente.

Concessione di autorizzazione del dispositivo

Questo flusso può essere utilizzato dalle applicazioni eseguite su un dispositivo con o senza browser. Quando l'applicazione avvia il flusso, presenta un URL e un codice utente che l'utente deve verificare successivamente nel flusso. Il codice utente è necessario perché l'applicazione che avvia il flusso potrebbe essere in esecuzione su un dispositivo diverso da quello su cui l'utente fornisce il consenso. Il codice garantisce che l'utente acconsenta al flusso avviato sull'altro dispositivo.

1. Quando il flusso inizia da un dispositivo dotato di browser, si apre una finestra del browser. Quando il flusso inizia da un dispositivo senza browser, l'utente deve aprire un browser su un dispositivo diverso e accedere all'URL presentato dall'applicazione.
2. In entrambi i casi, se l'utente non si è autenticato, il browser lo reindirizza per completare l'autenticazione dell'utente.
3. Dopo l'autenticazione, all'utente viene presentata una schermata di consenso che mostra le seguenti informazioni:
   - Il nome dell'applicazione
   - Gli ambiti di accesso per i quali l'applicazione richiede il consenso all'uso
   - Il codice utente che l'applicazione ha presentato all'utente
4. L'utente può annullare la procedura di consenso oppure può dare il proprio consenso e l'applicazione procede con l'accesso in base alle autorizzazioni dell'utente.

Ambiti di accesso

Un ambito definisce l'accesso a un servizio per un servizio a cui è possibile accedere tramite un flusso OAuth 2.0. Gli ambiti sono un modo per il servizio, chiamato anche server di risorse, di raggruppare le autorizzazioni relative alle azioni e alle risorse del servizio e specificano le operazioni generiche che i client OAuth 2.0 possono richiedere. Quando un client OAuth 2.0 si registra con il servizio OIDC di IAM Identity Center, specifica gli ambiti per dichiarare le azioni previste, per le quali l'utente deve fornire il consenso.

I client OAuth 2.0 utilizzano i `scope` valori definiti nella sezione 3.3 di OAuth 2.0 (RFC 6749) per specificare quali autorizzazioni vengono richieste per un token di accesso. I client possono specificare un massimo di 25 ambiti quando richiedono un token di accesso. Quando un utente fornisce il consenso durante un flusso di concessione del codice di autorizzazione con PKCE o Device Authorization Grant, IAM Identity Center codifica gli ambiti nel token di accesso restituito.

AWS aggiunge gli ambiti a IAM Identity Center per il supporto. Servizi AWS La tabella seguente elenca gli ambiti supportati dal servizio IAM Identity Center OIDC quando si registra un client pubblico.

Ambiti di accesso supportati dal servizio OIDC di IAM Identity Center durante la registrazione di un client pubblico

Ambito	Descrizione	Servizi supportati da
`sso:account:access`	Accedi agli account e ai set di autorizzazioni gestiti da IAM Identity Center.	IAM Identity Center
`codewhisperer:analysis`	Abilita l'accesso all'analisi del codice di Amazon Q Developer.	ID Builder AWS e IAM Identity Center
`codewhisperer:completions`	Abilita l'accesso ai suggerimenti sul codice in linea di Amazon Q.	ID Builder AWS e IAM Identity Center
`codewhisperer:conversations`	Abilita l'accesso alla chat di Amazon Q.	ID Builder AWS e IAM Identity Center
`codewhisperer:taskassist`	Abilita l'accesso ad Amazon Q Developer Agent per lo sviluppo del software.	ID Builder AWS e IAM Identity Center
`codewhisperer:transformations`	Abilita l'accesso ad Amazon Q Developer Agent per la trasformazione del codice.	ID Builder AWS e IAM Identity Center
`codecatalyst:read_write`	Leggi e scrivi sulle tue CodeCatalyst risorse Amazon, permettendo l'accesso a tutte le tue risorse esistenti.	ID Builder AWS e IAM Identity Center

Configurazione di applicazioni SAML 2.0 gestite dal cliente

Se utilizzi applicazioni gestite dai clienti che supportano SAML 2.0, puoi federare il tuo IdP a IAM Identity Center tramite SAML 2.0 e utilizzare IAM Identity Center per gestire l'accesso degli utenti a tali applicazioni. Puoi selezionare un'applicazione SAML 2.0 da un catalogo di applicazioni di uso comune nella console IAM Identity Center oppure puoi configurare la tua applicazione SAML 2.0.

> **Note**
>
> Se disponi di applicazioni gestite dai clienti che supportano OAuth 2.0 e i tuoi utenti devono accedere da queste applicazioni ai AWS servizi, puoi utilizzare la propagazione affidabile delle identità. Con la propagazione affidabile delle identità, un utente può accedere a un'applicazione e tale applicazione può trasmettere l'identità degli utenti nelle richieste di accesso ai dati nei servizi. AWS Per ulteriori informazioni, consulta Utilizzo della propagazione affidabile delle identità con applicazioni gestite dal cliente.

Argomenti

Catalogo di applicazioni IAM Identity Center

Puoi utilizzare il catalogo delle applicazioni nella console IAM Identity Center per aggiungere molte applicazioni SAML 2.0 di uso comune che funzionano con IAM Identity Center. Gli esempi includono Salesforce, Box e Microsoft 365.

La maggior parte delle applicazioni fornisce informazioni dettagliate su come impostare la fiducia tra IAM Identity Center e il fornitore di servizi dell'applicazione. Queste informazioni sono disponibili nella pagina di configurazione dell'applicazione, dopo aver selezionato l'applicazione nel catalogo. Dopo aver configurato l'applicazione, puoi assegnare l'accesso a utenti o gruppi in IAM Identity Center in base alle esigenze.

Argomenti

Configura un'applicazione dal catalogo delle applicazioni

Utilizza questa procedura per configurare una relazione di trust SAML 2.0 tra IAM Identity Center e il fornitore di servizi dell'applicazione.

Prima di iniziare questa procedura, è utile disporre del file di scambio di metadati del fornitore di servizi in modo da poter configurare il trust in modo più efficiente. Se non disponi di questo file, puoi comunque utilizzare questa procedura per configurare manualmente il trust it.

Per aggiungere e configurare un'applicazione dal catalogo delle applicazioni

1. Apri la console IAM Identity Center.
2. Selezionare Applications (Applicazioni).
3. Scegli la scheda Gestito dal cliente.
4. Scegli Aggiungi applicazione.
5. Nella pagina Seleziona il tipo di applicazione, in Preferenze di configurazione, scegli Desidero selezionare un'applicazione dal catalogo.
6. In Catalogo delle applicazioni, iniziate a digitare il nome dell'applicazione che desiderate aggiungere nella casella di ricerca.
7. Scegliete il nome dell'applicazione dall'elenco quando appare nei risultati della ricerca, quindi scegliete Avanti.
8. Nella pagina Configura applicazione, i campi Nome visualizzato e Descrizione sono precompilati con i dettagli pertinenti per l'applicazione. È possibile modificare queste informazioni.
9. Nei metadati di IAM Identity Center, procedi come segue:

    a. Nel file di metadati SAML di IAM Identity Center, scegli Scarica per scaricare i metadati del provider di identità.

    b. In Certificato IAM Identity Center, scegli Scarica certificato per scaricare il certificato del provider di identità.

> **Note**
>
> Questi file ti serviranno in seguito, quando configurerai l'applicazione dal sito Web del fornitore di servizi. Segui le istruzioni fornite dal provider.

10. (Facoltativo) In Proprietà dell'applicazione, è possibile specificare l'URL di avvio dell'applicazione, lo stato di inoltro e la durata della sessione. Per ulteriori informazioni, consulta Configura le proprietà dell'applicazione nella console IAM Identity Center.
11. In Metadati dell'applicazione, effettuate una delle seguenti operazioni:
    a. Se disponi di un file di metadati, scegli Carica il file di metadati SAML dell'applicazione. Quindi, seleziona Scegli il file per trovare e seleziona il file di metadati.
    b. Se non disponi di un file di metadati, scegli Digita manualmente i valori dei metadati, quindi fornisci i valori dell'URL dell'applicazione ACS e dell'audience SAML dell'applicazione.
12. Scegli Invia. Verrai indirizzato alla pagina dei dettagli dell'applicazione che hai appena aggiunto.

Configura la tua applicazione SAML 2.0

Puoi configurare le tue applicazioni che consentono la federazione delle identità utilizzando SAML 2.0 e aggiungerle a IAM Identity Center. La maggior parte dei passaggi per configurare le proprie applicazioni SAML 2.0 sono gli stessi della configurazione di un'applicazione SAML 2.0 dal catalogo delle applicazioni nella console IAM Identity Center. Tuttavia, è necessario fornire anche mappature degli attributi SAML aggiuntive per le proprie applicazioni SAML 2.0. Queste mappature consentono a IAM Identity Center di compilare correttamente l'asserzione SAML 2.0 per l'applicazione. Puoi fornire questa mappatura aggiuntiva degli attributi SAML quando configuri l'applicazione per la prima volta. Puoi anche fornire mappature degli attributi SAML 2.0 nella pagina dei dettagli dell'applicazione nella console IAM Identity Center.

Utilizza la seguente procedura per configurare una relazione di trust SAML 2.0 tra IAM Identity Center e il provider di servizi dell'applicazione SAML 2.0. Prima di iniziare questa procedura, verifica di disporre del certificato e dei file di scambio dei metadati del provider di servizi in modo poter completare la configurazione del livello di attendibilità.

Per configurare la tua applicazione SAML 2.0

1. Apri la console IAM Identity Center.
2. Selezionare Applications (Applicazioni).
3. Scegli la scheda Gestito dal cliente.
4. Scegli Aggiungi applicazione.
5. Nella pagina Seleziona il tipo di applicazione, in Preferenze di configurazione, scegli Ho un'applicazione che voglio configurare.

6. In Tipo di applicazione, scegli SAML 2.0.
7. Seleziona Successivo.
8. Nella pagina Configura applicazione, in Configura applicazione, inserisci un nome visualizzato per l'applicazione, ad esempio**`MyApp`**. Quindi, inserisci una descrizione.
9. Sotto i metadati di IAM Identity Center, procedi come segue:

    a. Nel file di metadati SAML di IAM Identity Center, scegli Scarica per scaricare i metadati del provider di identità.

    b. In Certificato IAM Identity Center, scegli Scarica per scaricare il certificato del provider di identità.

    > **Note**
    >
    > Questi file saranno necessari più tardi durante la configurazione dell'applicazione personalizzata dal sito web del provider di servizi.

10. (Facoltativo) In Proprietà dell'applicazione, puoi anche specificare l'URL di avvio dell'applicazione, lo stato di inoltro e la durata della sessione. Per ulteriori informazioni, consulta Configura le proprietà dell'applicazione nella console IAM Identity Center.
11. In Metadati dell'applicazione, scegli Digita manualmente i valori dei metadati. Quindi, fornisci i valori di pubblico Application ACS URL e Application SAML dell'applicazione.
12. Scegli Invia. Verrai indirizzato alla pagina dei dettagli dell'applicazione che hai appena aggiunto.

Propagazione delle identità attendibili tra le applicazioni

La propagazione affidabile delle identità consente ai AWS servizi di eseguire le seguenti operazioni:

- Autorizza l'accesso alle AWS risorse in base al contesto di identità dell'utente.
- Condividi in modo sicuro il contesto dell'identità dell'utente con altri AWS servizi.

Queste funzionalità consentono di definire, concedere e registrare più facilmente l'accesso degli utenti.

Con la propagazione affidabile delle identità, un utente può accedere a un'applicazione e tale applicazione può trasmettere il contesto dell'identità degli utenti nelle richieste di accesso ai dati nei

servizi. AWS Poiché l'accesso è gestito in base all'identità dell'utente, gli utenti non devono utilizzare le credenziali utente locali del database o assumere un ruolo IAM per accedere ai dati.

Argomenti

Panoramica sulla propagazione delle identità affidabili

Con la propagazione affidabile delle identità, l'accesso degli utenti alle AWS risorse può essere definito, concesso e registrato più facilmente. La propagazione affidabile delle identità si basa sul framework di autorizzazione OAuth 2.0, che consente alle applicazioni di accedere e condividere i dati degli utenti in modo sicuro senza condividere le password. OAuth 2.0 fornisce un accesso delegato sicuro alle risorse delle applicazioni. L'accesso è delegato perché l'amministratore delle risorse approva o delega l'accesso all'altra applicazione a cui l'utente accede.

Per evitare la condivisione delle password degli utenti, la propagazione delle identità affidabili utilizza i token. I token forniscono un modo standard per un'applicazione attendibile di dichiarare chi è l'utente e quali richieste sono consentite tra due applicazioni. AWS le applicazioni gestite che si integrano con la propagazione affidabile delle identità ottengono i token direttamente da IAM Identity Center. IAM Identity Center offre anche un'opzione per le applicazioni per lo scambio di token di identità e i token di accesso che provengono da un server di autorizzazione OAuth 2.0 esterno. Ciò consente a un'applicazione di autenticarsi e ottenere token dall'esterno AWS, scambiare il token con un token IAM Identity Center e utilizzare il nuovo token per effettuare richieste ai servizi. AWS Per ulteriori informazioni, consulta Utilizzo di applicazioni con un emittente di token affidabile.

Il processo OAuth 2.0 inizia quando un utente accede a un'applicazione. L'applicazione a cui l'utente accede avvia una richiesta di accesso alle risorse dell'altra applicazione. L'applicazione che ha avviato (richiedente) può accedere all'applicazione ricevente per conto dell'utente richiedendo un token dal server di autorizzazione. Il server di autorizzazione restituisce il token e l'applicazione di avvio passa tale token, con una richiesta di accesso, all'applicazione ricevente.

Casi d'uso affidabili per la propagazione dell'identità

In qualità di amministratore di IAM Identity Center, ti potrebbe essere chiesto di aiutarti a configurare la propagazione dell'identità affidabile tra le seguenti applicazioni di avvio che supportano questa funzionalità e i servizi connessi. AWS Le seguenti sezioni forniscono ulteriori informazioni sui casi d'uso specifici supportati dalle applicazioni in grado di avviare la propagazione delle identità affidabili.

Argomenti

Amazon EMR

Puoi utilizzare Amazon EMR come applicazione di avvio per i seguenti casi d'uso di propagazione di identità affidabili.

Descrizione	Altri servizi utilizzati AWS	Ulteriori informazioni
Esegui analisi interattive con Apache Spark su Amazon EMR su cluster Amazon EC2 tramite Amazon EMR Studio. Applica il controllo degli accessi basato sulle identità della forza lavoro e sugli attributi associati per Catalog Through. AWS Glue AWS Lake Formation	Amazon EMR su Amazon EC2 autorizza to tramite, Amazon S3 Access Grants, AWS Lake Formation Amazon S3, AWS Service Catalog **Note** • Richiede l'accesso tramite	• Integra Amazon EMR con IAM Identity Center nella Amazon EMR Management Guide. • Amazon S3 Access Grants e identità di directory aziendali nella Guida per l'utente di Amazon Simple Storage Service. • Connessione AWS Lake Formation con IAM Identity Center nella Guida per gli sviluppatori AWS Lake Formation

Descrizione	Altri servizi utilizzati AWS	Ulteriori informazioni
	Amazon EMR Studio. • Solo controllo degli accessi a livello di tabella. • Apache Hive, PrestoSQL/ Trino ed EMR Serverles s non sono supportati.	• Usa le tue identità aziendali per l'analisi con Amazon EMR e IAM Identity Center nel blog AWS sui Big Data

Descrizione	Altri servizi utilizzati AWS	Ulteriori informazioni
Esegui analisi ad hoc con Trino su Athena tramite Amazon EMR Studio. Applica il controllo degli accessi basato sulle identità della forza lavoro e sugli attributi associati per Catalog tramite. AWS Glue AWS Lake Formation Accesso sicuro alla posizione del bucket dei risultati di una query Athena in Amazon S3 utilizzando Amazon S3 Access Grants.	Athena autorizzata tramite Amazon S3 AWS Lake Formation Access Grants **Note** Richiede l'accesso tramite Amazon EMR Studio. L'accesso diretto dalla Amazon Athena console non è supportato.	• Integra Amazon EMR con IAM Identity Center nella Amazon EMR Management Guide. • Utilizzo dei gruppi di lavoro Athena abilitati per IAM Identity Center nella Amazon Athena User Guide. • Amazon S3 Access Grants e identità di directory aziendali nella Guida per l'utente di Amazon Simple Storage Service. • Connessione AWS Lake Formation con IAM Identity Center nella Guida per gli sviluppatori AWS Lake Formation . • Porta l'identità della tua forza lavoro in Amazon EMR Studio e Athena nel AWS blog sui Big Data.

Amazon QuickSight

Puoi utilizzare Amazon QuickSight come applicazione di avvio per i seguenti casi d'uso attendibili di propagazione delle identità.

Descrizione	Altri servizi utilizzati AWS	Ulteriori informazioni
QuickSight Gli utenti Amazon possono interrogare i dati di	Amazon Redshift	• Connetti Redshift con IAM Identity Center per offrire agli

Descrizione	Altri servizi utilizzati AWS	Ulteriori informazioni
Amazon Redshift. L'accesso ai dati viene concesso in Amazon Redshift da un amministratore di Amazon Redshift.		utenti un'esperienza di single sign-on nella Amazon Redshift Management Guide. • Connetti Amazon Redshift con IAM Identity Center tramite Amazon QuickSight nella Amazon Redshift Management Guide.
QuickSight Gli utenti Amazon possono interrogare Amazon Redshift Spectrum per dati strutturati in Amazon S3, con accesso autorizzato AWS Lake Formation da un amministratore.	Amazon Redshift Spectrum, dati strutturati Amazon S3 *Tramite Amazon Redshift Spectrum autorizzato tramite AWS Lake Formation	• Connetti Redshift con IAM Identity Center per offrire agli utenti un'esperienza di single sign-on nella Amazon Redshift Management Guide. • Connetti Amazon Redshift con IAM Identity Center tramite Amazon QuickSight nella Amazon Redshift Management Guide. • Connessione AWS Lake Formation con IAM Identity Center nella Guida per gli AWS Lake Formation sviluppatori. • Semplifica la gestione degli accessi con Amazon Redshift e AWS Lake Formation per gli utenti di un provider di identità esterno nel blog AWS Big Data.

Descrizione	Altri servizi utilizzati AWS	Ulteriori informazioni
QuickSight Gli utenti Amazon possono interrogare le condivisioni di dati Amazon Redshift per dati strutturati in Amazon S3, con accesso autorizzato da un amministratore. AWS Lake Formation	Condivisioni di dati Amazon Redshift, dati strutturati Amazon S3 *Tramite Amazon Redshift autorizzato tramite AWS Lake Formation	• Connetti Amazon Redshift con IAM Identity Center tramite Amazon QuickSight nella Amazon Redshift Management Guide. • Connessione AWS Lake Formation con IAM Identity Center nella Guida per gli AWS Lake Formation sviluppatori. • Semplifica la gestione degli accessi con Amazon Redshift e AWS Lake Formation per gli utenti di un provider di identità esterno nel blog AWS Big Data.

Editor di query v2 di Amazon Redshift

Puoi utilizzare Amazon Redshift Query Editor v2 come applicazione di avvio per i seguenti casi d'uso attendibili di propagazione delle identità.

Descrizione	Altri servizi utilizzati AWS	Ulteriori informazioni
Gli utenti di Amazon Redshift Query Editor v2 possono interrogare i dati di Amazon Redshift. L'accesso ai dati viene concesso in Amazon Redshift da un amministratore di Amazon Redshift.	Amazon Redshift	• Connetti Redshift con IAM Identity Center per offrire agli utenti un'esperienza di single sign-on nella Amazon Redshift Management Guide. • Connettiti a un database Amazon Redshift nella Amazon Redshift Management Guide.

Descrizione	Altri servizi utilizzati AWS	Ulteriori informazioni
		• Esegui Okta l'integrazione con Amazon Redshift Query Editor V2 utilizzando il AWS IAM Identity Center Single Sign-On senza interruzioni nel blog sui Big Data.AWS
Gli utenti di Amazon Redshift Query Editor v2 possono interrogare tabelle esterne Amazon Redshift Spectrum per dati strutturati in Amazon S3, con accesso autorizzato da un amministratore. AWS Lake Formation	Amazon Redshift Spectrum, dati strutturati Amazon S3 *Tramite Amazon Redshift Spectrum autorizzato tramite AWS Lake Formation	• Connetti Redshift con IAM Identity Center per offrire agli utenti un'esperienza di single sign-on nella Amazon Redshift Management Guide. • Connettiti a un database Amazon Redshift nella Amazon Redshift Management Guide. • Connessione AWS Lake Formation con IAM Identity Center nella Guida per gli AWS Lake Formation sviluppatori.
Gli utenti di Amazon Redshift Query Editor v2 possono interrogare le condivisioni di dati Amazon Redshift con accesso autorizzato da un amministratore. AWS Lake Formation	condivisioni di dati Amazon Redshift, AWS Lake Formation	• Connettiti a un database Amazon Redshift nella Amazon Redshift Management Guide. • Connessione AWS Lake Formation con IAM Identity Center nella Guida per gli AWS Lake Formation sviluppatori.

Applicazioni di business intelligence di terze parti

Puoi utilizzare un'applicazione di business intelligence di terze parti come Tableau, come applicazione di avvio per specifici casi d'uso di propagazione delle identità affidabili. Le applicazioni di business intelligence modificate di terze parti possono trasmettere al driver Amazon Redshift l'identità

di un utente tramite token di identità OAuth o token di accesso, per interrogare Amazon Redshift per i dati, con accesso autorizzato da un amministratore di Amazon Redshift.

Applicazioni sviluppate su misura

È possibile utilizzare le proprie applicazioni sviluppate su misura come applicazione di avvio per i seguenti casi d'uso attendibili di propagazione delle identità.

Descrizione	Altri servizi utilizzati AWS	Ulteriori informazioni
Crea un'applicazione che autentichi gli utenti tramite un server di autorizzazione OAuth, quindi utilizza un IAM per ottenere una credenziale di AWS IAM Identity Center ruolo IAM con identità migliorata. Questa credenziale viene utilizzata per richiedere l'accesso ai dati non strutturati in Amazon S3, con accesso autorizzato da un amministratore di Amazon S3 Access Grants.	AWS IAM Identity Center, Amazon S3 dati non strutturati *Autorizzato tramite Amazon S3 Access Grants	• Amazon S3 Access Grants e identità di directory aziendali nella Guida per l'utente di Amazon Simple Storage Service. • Come sviluppare un'applicazione dati rivolta agli utenti con IAM Identity Center e Amazon S3 Access Grants (parte 1) e (parte 2) nel AWS blog sullo storage.
Crea un'applicazione personalizzata che interagisce con Amazon Q Business per rispondere alle domande degli utenti in base ai tuoi contenuti e alle autorizzazioni dell'utente.	Centro di identità IAM, Amazon Q Business	• Abilita e configura un'istanza IAM Identity Center nella Amazon Q Business User Guide. • Come utilizzare le applicazioni AWS gestite con IAM Identity Center: abilita Amazon Q senza migrare i flussi federativi IAM esistenti nel AWS Security Blog.

Configura una propagazione affidabile delle identità

La propagazione affidabile delle identità supporta diversi modi di autenticazione delle applicazioni in modo che possano trasmettere l'identità di un utente ai servizi. AWS La configurazione per la propagazione delle identità affidabili varia in base ai tipi di applicazione e al modo in cui vengono autenticate.

> **Note**
>
> È necessario configurare un emittente di token affidabile se si dispone di applicazioni gestite dai clienti che richiedono l'accesso alle applicazioni AWS gestite, ma non utilizzano AWS API per la connessione.

Argomenti

Prerequisiti e considerazioni

Prima di configurare la propagazione affidabile delle identità, esamina i prerequisiti e le considerazioni seguenti.

Argomenti

Prerequisiti

Per utilizzare la propagazione affidabile delle identità, assicuratevi che l'ambiente soddisfi i seguenti prerequisiti.

- Implementazione di IAM Identity Center con utenti e gruppi predisposti

Per utilizzare la propagazione affidabile delle identità, devi abilitare IAM Identity Center ed effettuare il provisioning di utenti e gruppi. Per informazioni, consulta Inizia con le attività più comuni in IAM Identity Center.

Istanza dell'organizzazione consigliata: ti consigliamo di utilizzare un'istanza organizzativa di IAM Identity Center da abilitare nell'account di gestione di AWS Organizations. Se prevedi di utilizzare la propagazione affidabile delle identità per consentire agli utenti di accedere ai AWS servizi e alle risorse correlate all' Account AWS interno della stessa organizzazione, puoi delegare l'amministrazione dell'istanza di IAM Identity Center a un account membro.

Se prevedi di utilizzare un'istanza con account singolo di IAM Identity Center, tutti i AWS servizi e le risorse a cui desideri che gli utenti accedano tramite la propagazione dell'identità affidabile devono risiedere nello stesso account standalone Account AWS o nello stesso account membro dell'organizzazione in cui hai abilitato IAM Identity Center. Per ulteriori informazioni, consulta Istanze di account di IAM Identity Center.

- Per applicazioni AWS gestite; connessione a IAM Identity Center

  Per utilizzare una propagazione affidabile delle identità, le applicazioni AWS gestite devono integrarsi con IAM Identity Center.

Ulteriori considerazioni

Tieni a mente le seguenti considerazioni aggiuntive per l'utilizzo della propagazione affidabile delle identità.

- Non modificare l'impostazione Richiedi assegnazioni per le applicazioni gestite AWS

  AWS le applicazioni gestite hanno una configurazione di impostazione predefinita che determina se le assegnazioni sono necessarie per utenti e gruppi. Si consiglia di non modificare questa impostazione. Anche se sono state configurate autorizzazioni dettagliate che consentono l'accesso degli utenti a risorse specifiche, la modifica dell'impostazione Richiedi assegnazioni potrebbe causare comportamenti imprevisti, tra cui l'interruzione dell'accesso degli utenti a tali risorse.

- Autorizzazioni per più account (set di autorizzazioni) non richieste

  La propagazione affidabile delle identità non richiede la configurazione di autorizzazioni per più account (set di autorizzazioni). Puoi abilitare IAM Identity Center e utilizzarlo solo per la propagazione di identità affidabili.

Utilizzo della propagazione affidabile delle identità con AWS applicazioni gestite

La propagazione affidabile dell'identità consente a un'applicazione AWS gestita di richiedere l'accesso ai dati nei AWS servizi per conto di un utente. La gestione dell'accesso ai dati si basa sull'identità dell'utente, quindi gli amministratori possono concedere l'accesso in base all'appartenenza esistente degli utenti e ai gruppi. L'identità dell'utente, le azioni eseguite per suo conto e altri eventi vengono registrati in registri ed eventi specifici del servizio. CloudTrail

La propagazione affidabile delle identità si basa sullo standard OAuth 2.0. Per utilizzare questa funzionalità, le applicazioni AWS gestite devono integrarsi con IAM Identity Center. AWS i servizi di analisi potrebbero fornire interfacce basate su driver che consentono a un'applicazione compatibile di utilizzare la propagazione affidabile delle identità. Ad esempio, i driver JDBC, ODBC e Python consentono agli strumenti di interrogazione compatibili di utilizzare la propagazione affidabile delle identità senza la necessità di completare ulteriori passaggi di configurazione.

Argomenti

Configura applicazioni AWS gestite per la propagazione affidabile delle identità

AWS i servizi che supportano la propagazione affidabile delle identità forniscono un'interfaccia utente amministrativa e API che è possibile utilizzare per configurare questa funzionalità. Non è richiesta alcuna configurazione all'interno di IAM Identity Center per questi servizi.

Di seguito è riportato il processo di alto livello per la configurazione di un AWS servizio per la propagazione affidabile delle identità. I passaggi specifici variano a seconda dell'interfaccia amministrativa e delle API fornite dall'applicazione.

1. Utilizza la console dell'applicazione o le API per connettere l'applicazione alla tua istanza di IAM Identity Center

   Utilizza la console per l'applicazione AWS gestita o le API dell'applicazione per connettere l'applicazione alla tua istanza di IAM Identity Center. Quando utilizzi la console per l'applicazione,

l'interfaccia utente amministrativa include un widget che semplifica il processo di configurazione e connessione.

2. Utilizzate la console dell'applicazione o le API per configurare l'accesso degli utenti alle risorse dell'applicazione

   Completa questo passaggio per autorizzare a quali risorse o dati può accedere un utente. L'accesso si basa sull'identità dell'utente o sull'appartenenza al gruppo. Il modello di autorizzazione varia in base all'applicazione.

   > **Important**
   >
   > È necessario completare questo passaggio per consentire agli utenti di accedere alle risorse del AWS servizio. In caso contrario, gli utenti non possono accedere alle risorse, anche se l'applicazione richiedente è autorizzata a richiedere l'accesso al servizio.

Flussi di richieste di propagazione dell'identità affidabili per applicazioni AWS gestite

Tutti i flussi di propagazione delle identità affidabili verso le applicazioni AWS gestite devono iniziare con un'applicazione che ottiene un token da IAM Identity Center. Questo token è necessario perché contiene un riferimento a un utente noto a IAM Identity Center e alle applicazioni registrate con IAM Identity Center.

Le sezioni seguenti descrivono i modi in cui un'applicazione AWS gestita può ottenere un token da IAM Identity Center per avviare la propagazione di identità affidabili.

Argomenti

- Autenticazione IAM Identity Center basata sul Web
- Richieste di autenticazione basate sulla console e avviate dall'utente

Autenticazione IAM Identity Center basata sul Web

Per questo flusso, l'applicazione AWS gestita fornisce un'esperienza Single Sign-On basata sul Web utilizzando IAM Identity Center per l'autenticazione.

Quando un utente apre un'applicazione AWS gestita, viene attivato un flusso Single Sign-On che utilizza IAM Identity Center. Se non c'è una sessione attiva per l'utente in IAM Identity Center,

all'utente viene presentata una pagina di accesso basata sulla fonte di identità che hai specificato e IAM Identity Center crea una sessione per l'utente.

IAM Identity Center fornisce all'applicazione AWS gestita un token che include l'identità dell'utente e un elenco di destinatari (Auds) e degli ambiti correlati per i quali l'applicazione è registrata. L'applicazione può quindi utilizzare il token per effettuare richieste ad altri servizi di ricezione. AWS

Richieste di autenticazione basate sulla console e avviate dall'utente

Per questo flusso, l'applicazione AWS gestita fornisce un'esperienza di console avviata dagli utenti.

In questo caso, l'applicazione AWS gestita viene inserita dalla console di AWS gestione dopo aver assunto un ruolo. Affinché l'applicazione ottenga un token, l'utente deve avviare un processo per attivare l'autenticazione dell'utente da parte dell'applicazione. Questo avvia l'autenticazione tramite IAM Identity Center, che reindirizzerà l'utente alla fonte di identità che hai configurato.

Dopo che un'applicazione ha ottenuto un token

Dopo che un'applicazione richiedente ottiene un token da IAM Identity Center, l'applicazione aggiorna periodicamente il token, che può essere utilizzato per tutta la durata della sessione dell'utente. Durante questo periodo, l'applicazione potrebbe:

- Ottenere ulteriori informazioni sul token per determinare chi è l'utente e quali ambiti l'applicazione può utilizzare con altre applicazioni AWS gestite riceventi.
- Passa il token nelle chiamate ad altre applicazioni AWS gestite di ricezione che supportano l'uso dei token.
- Ottieni sessioni di ruolo IAM con identità migliorata da utilizzare per effettuare richieste ad altre applicazioni AWS gestite che utilizzano AWS Signature Version 4.

  Una sessione di ruolo IAM con identità migliorata è una sessione di ruolo IAM che contiene l'identità propagata dell'utente archiviata in un token creato da IAM Identity Center.

Sessioni di ruolo IAM con identità migliorata

AWS Security Token Service Consente a un'applicazione di ottenere una sessione di ruolo IAM con identità migliorata. AWS le applicazioni gestite che supportano il contesto utente in una sessione di ruolo possono utilizzare le informazioni sull'identità per autorizzare l'accesso in base all'utente che partecipa alla sessione di ruolo. Questo nuovo contesto consente alle applicazioni di effettuare richieste ad applicazioni AWS gestite che supportano la propagazione dell'identità affidabile tramite le richieste API AWS Signature Version 4.

Quando un'applicazione AWS gestita utilizza una sessione di ruolo IAM con identità avanzata per accedere a una risorsa, CloudTrail registra l'identità dell'utente (ID utente), la sessione di avvio e l'azione intrapresa.

Quando un'applicazione effettua una richiesta utilizzando una sessione di ruolo IAM con identità avanzata a un'applicazione ricevente, aggiunge un contesto alla sessione in modo che l'applicazione ricevente possa autorizzare l'accesso in base all'identità o all'appartenenza al gruppo dell'utente o al ruolo IAM. Le applicazioni di ricezione che supportano la propagazione dell'identità affidabile restituiranno un errore se l'applicazione ricevente o la risorsa richiesta non sono configurate per autorizzare l'accesso in base all'identità o all'appartenenza al gruppo dell'utente.

Per evitare questo problema, effettuate una delle seguenti operazioni:

- Verifica che l'applicazione ricevente sia connessa a IAM Identity Center.
- Utilizza la console per l'applicazione ricevente o le API dell'applicazione per configurare l'applicazione in modo da autorizzare l'accesso alle risorse in base all'identità dell'utente o all'appartenenza al gruppo. I requisiti di configurazione a tale scopo variano in base all'applicazione.

Per ulteriori informazioni, consulta la documentazione dell'applicazione AWS gestita ricevente.

Tipi di sessioni di ruolo IAM con identità migliorata

Un'applicazione ottiene una sessione di ruolo IAM con identità migliorata effettuando una richiesta all' AWS STS `AssumeRole`API e passando un'asserzione di contesto nel parametro della richiesta. `ProvidedContexts` `AssumeRole` L'asserzione di contesto è ottenuta dall'`idToken`affermazione disponibile nella risposta alla richiesta. `SSO OIDC` `CreateTokenWithIAM`

AWS STS può creare due diversi tipi di sessioni di ruolo IAM con identità migliorata, a seconda dell'asserzione di contesto fornita alla richiesta: `AssumeRole`

- Sessioni che registrano solo l'identità dell'utente. CloudTrail
- Sessioni che abilitano l'autorizzazione in base all'identità dell'utente propagata e a CloudTrail cui la registrano.

Per ottenere una sessione di ruolo IAM con identità migliorata AWS STS che fornisca solo informazioni di controllo registrate in un CloudTrail percorso, fornisci il valore del claim alla `sts:audit_context` richiesta. `AssumeRole` Per ottenere una sessione che consenta anche al

AWS servizio ricevente di autorizzare l'utente di IAM Identity Center a eseguire un'azione, fornisci il valore del claim alla richiesta. `sts:identity_context` `AssumeRole` Puoi fornire solo un contesto.

Sessioni di ruolo IAM con identità avanzate create con **`sts:audit_context`**

Quando viene effettuata una richiesta a un AWS servizio utilizzando una sessione di ruolo IAM con identità avanzata creata con`sts:audit_context`, l'IAM Identity Center dell'utente `userId` viene registrato nell'elemento. CloudTrail `OnBehalfOf`

```
"userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROAEXAMPLE:MyRole",
      "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
      "accountId": "111111111111",
      "accessKeyId": "ASIAEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAEXAMPLE",
            "arn": "arn:aws:iam::111111111111:role/MyRole",
            "accountId": "111111111111",
            "userName": "MyRole"
        },
        "attributes": {
            "creationDate": "2023-12-12T13:55:22Z",
            "mfaAuthenticated": "false"
        }
    },
    "onBehalfOf": {
        "userId": "11111111-1111-1111-1111-1111111111",
        "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/
d-111111111"
    }
}
```

> **Note**
>
> Queste sessioni non possono essere utilizzate per autorizzare l'utente dell'Identity Center. Possono ancora essere utilizzate per autorizzare il ruolo IAM.

Per ottenere questo tipo di sessione di ruolo da AWS STS, fornisci il valore del `sts:audit_context` campo alla `AssumeRole` richiesta nel parametro di `ProvidedContexts` richiesta. Usa `arn:aws:iam::aws:contextProvider/IdentityStore` come valore per`ProviderArn`.

Sessioni di ruolo IAM con identità avanzate create con **`sts:identity_context`**

Quando un utente effettua una richiesta a un AWS servizio utilizzando una sessione di ruolo IAM con identità avanzata creata con`sts:identity_context`, l'IAM Identity Center dell'utente `userId` viene registrato CloudTrail nell'`onBehalfO`felemento allo stesso modo di una sessione creata con. `sts:audit_context`

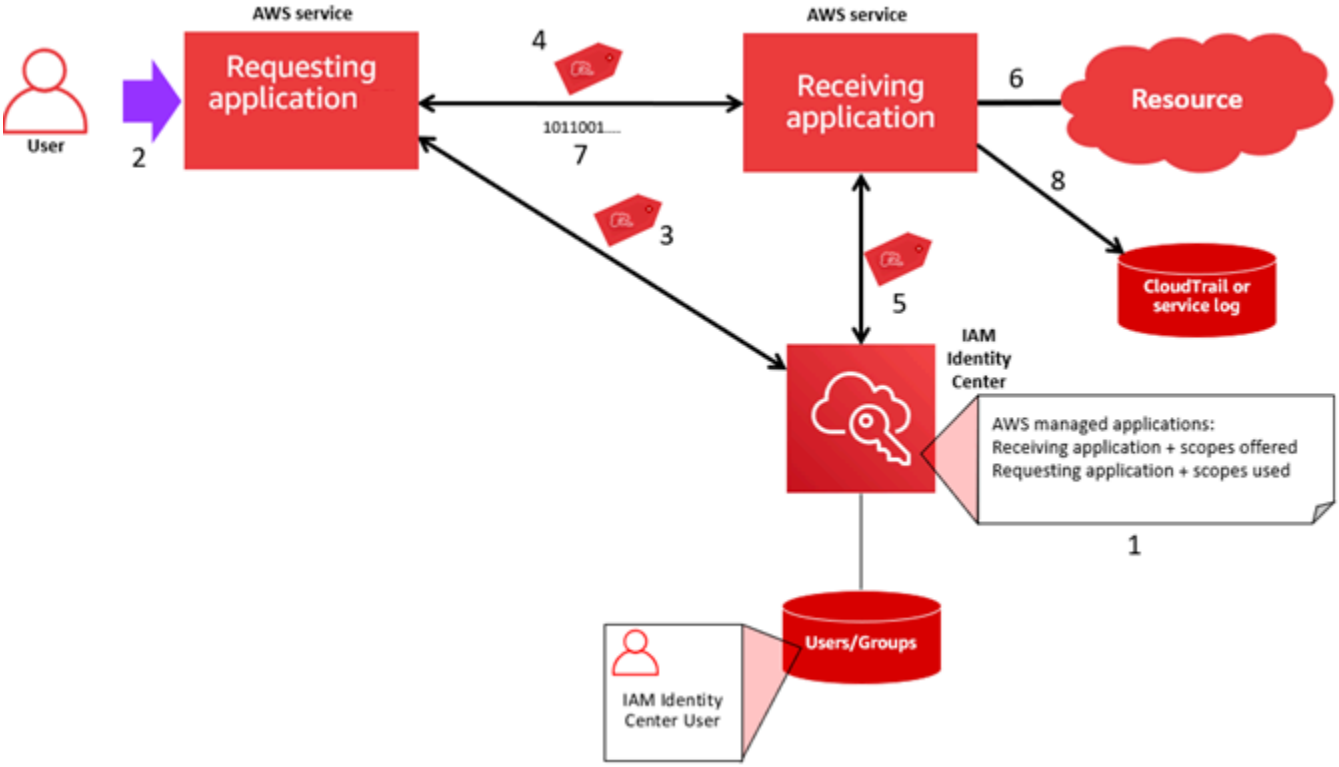
Oltre a registrare gli utenti di IAM Identity Center CloudTrail, questo tipo `userId` di sessione viene utilizzato anche dalle API supportate per autorizzare azioni basate sull'identità utente propagata. Per un elenco delle azioni IAM per le API supportate, consulta la policy gestita. `AWSIAMIdentityCenterAllowListForIdentityContext` AWS Questa policy AWS gestita viene fornita come policy di sessione quando viene creata una sessione di ruolo IAM con identità migliorata con. `sts:identity_context` La policy impedisce di utilizzare la sessione di ruolo con servizi non supportati. AWS

Per ottenere questo tipo di sessione di ruolo da AWS STS, fornite il valore del `sts:identity_context` campo alla `AssumeRole` richiesta nel parametro `ProvidedContexts` request. Usa `arn:aws:iam::aws:contextProvider/IdentityStore` come valore per`ProviderArn`.

Processo di configurazione e flusso di richieste per le applicazioni AWS gestite

Questa sezione descrive il processo di configurazione e il flusso di richieste per le applicazioni AWS gestite che utilizzano la propagazione affidabile delle identità e che forniscono un'esperienza Single Sign-On basata sul Web.

Il diagramma seguente fornisce una panoramica di questo processo.



I passaggi seguenti forniscono informazioni aggiuntive su questo processo.

1. Utilizzate la console per l'applicazione AWS gestita o le API dell'applicazione per effettuare le seguenti operazioni:
   a. Connect l'applicazione alla tua istanza di IAM Identity Center.
   b. Imposta le autorizzazioni per autorizzare le risorse dell'applicazione a cui un utente può accedere.
2. Il flusso di richieste inizia quando un utente apre un'applicazione AWS gestita in grado di richiedere l'accesso alle risorse (un'applicazione richiedente).
3. Per ottenere un token per accedere all'applicazione AWS gestita ricevente, l'applicazione AWS gestita richiedente avvia una richiesta di accesso a IAM Identity Center.

   Se l'utente non ha effettuato l'accesso, IAM Identity Center attiva un flusso di autenticazione utente verso la fonte di identità che hai specificato. Questo crea una nuova sessione del portale di AWS accesso per l'utente con la durata configurata in IAM Identity Center. IAM Identity Center genera quindi un token associato alla sessione e l'applicazione può funzionare per la durata restante della sessione del portale di AWS accesso dell'utente. Se l'utente si disconnette dall'applicazione o se elimini la sessione, la sessione termina automaticamente entro due ore.

4. L'applicazione AWS gestita avvia una richiesta all'applicazione ricevente e fornisce il relativo token.
5. L'applicazione ricevente effettua chiamate a IAM Identity Center per ottenere l'identità dell'utente e gli ambiti codificati nel token. L'applicazione ricevente potrebbe anche effettuare richieste per ottenere gli attributi utente o l'appartenenza ai gruppi dell'utente dalla directory di Identity Center.
6. L'applicazione ricevente utilizza la propria configurazione di autorizzazione per determinare se l'utente è autorizzato ad accedere alla risorsa dell'applicazione richiesta.
7. Se l'utente è autorizzato ad accedere alla risorsa dell'applicazione richiesta, l'applicazione ricevente risponde alla richiesta.
8. L'identità dell'utente, le azioni eseguite per suo conto e altri eventi registrati nei registri e AWS CloudTrail negli eventi dell'applicazione ricevente. Il modo specifico in cui queste informazioni vengono registrate varia in base all'applicazione.

Utilizzo della propagazione affidabile delle identità con applicazioni gestite dal cliente

La propagazione affidabile delle identità consente a un'applicazione gestita dal cliente di richiedere l'accesso ai dati nei AWS servizi per conto di un utente. La gestione dell'accesso ai dati si basa sull'identità dell'utente, pertanto gli amministratori possono concedere l'accesso in base all'appartenenza esistente degli utenti e ai gruppi. L'identità dell'utente, le azioni eseguite per suo conto e altri eventi vengono registrati in registri ed eventi specifici del servizio. CloudTrail

Con la propagazione affidabile delle identità, un utente può accedere a un'applicazione gestita dal cliente e tale applicazione può trasmettere l'identità dell'utente nelle richieste di accesso ai dati nei servizi. AWS

> **Important**
>
> Per accedere a un AWS servizio, le applicazioni gestite dal cliente devono ottenere un token da un emittente di token affidabile, esterno a IAM Identity Center. Un emittente di token affidabile è un server di autorizzazione OAuth 2.0 che crea token firmati. Questi token autorizzano le applicazioni che avviano richieste di accesso ai servizi (applicazioni di ricezione). AWS Per ulteriori informazioni, consulta Utilizzo di applicazioni con un emittente di token affidabile.

Argomenti

- Configura applicazioni OAuth 2.0 gestite dal cliente per la propagazione affidabile delle identità

- Specificare applicazioni attendibili

Configura applicazioni OAuth 2.0 gestite dal cliente per la propagazione affidabile delle identità

Per configurare un'applicazione OAuth 2.0 gestita dal cliente per la propagazione di identità affidabili, devi prima aggiungerla a IAM Identity Center. Utilizza la seguente procedura per aggiungere l'applicazione a IAM Identity Center.

Argomenti

- Fase 1: Seleziona il tipo di applicazione
- Fase 2: Specificare i dettagli dell'applicazione
- Passaggio 3: Specificare le impostazioni di autenticazione
- Passaggio 4: Specificare le credenziali dell'applicazione
- Passaggio 5: revisione e configurazione

Fase 1: Seleziona il tipo di applicazione

1. Apri la console IAM Identity Center.
2. Selezionare Applications (Applicazioni).
3. Scegli la scheda Gestito dal cliente.
4. Scegli Aggiungi applicazione.
5. Nella pagina Seleziona il tipo di applicazione, in Preferenze di configurazione, scegli Ho un'applicazione che voglio configurare.
6. In Tipo di applicazione, scegli OAuth 2.0.
7. Scegli Avanti per passare alla pagina successiva,. Fase 2: Specificare i dettagli dell'applicazione

Fase 2: Specificare i dettagli dell'applicazione

1. Nella pagina Specificare i dettagli dell'applicazione, in Nome e descrizione dell'applicazione, immettere un nome visualizzato per l'applicazione, ad esempio**`MyApp`**. Quindi, inserisci una descrizione.
2. In Metodo di assegnazione a utenti e gruppi, scegli una delle seguenti opzioni:
   - Richiedi assegnazioni: consenti solo agli utenti e ai gruppi di IAM Identity Center assegnati a questa applicazione di accedere all'applicazione.

Visibilità dei riquadri dell'applicazione: solo gli utenti assegnati all'applicazione direttamente o tramite un'assegnazione di gruppo possono visualizzare il riquadro dell'applicazione nel portale di AWS accesso, a condizione che la visibilità dell'applicazione nel portale di AWS accesso sia impostata su Visibile.

- Non richiedono assegnazioni: consenti a tutti gli utenti e i gruppi autorizzati di IAM Identity Center di accedere a questa applicazione.

  Visibilità del riquadro dell'applicazione: il riquadro dell'applicazione è visibile a tutti gli utenti che AWS accedono al portale di accesso, a meno che la visibilità dell'applicazione nel portale di AWS accesso non sia impostata su Non visibile.

3. Nel portale di AWS accesso, inserisci l'URL a cui gli utenti possono accedere all'applicazione e specifica se il riquadro dell'applicazione sarà visibile o meno nel portale di AWS accesso. Se scegliete Non visibile, nemmeno gli utenti assegnati possono visualizzare il riquadro dell'applicazione.
4. In Tag (opzionale), scegli Aggiungi nuovo tag, quindi specifica i valori per Chiave e Valore (opzionale).

   Per ulteriori informazioni sui tag, consulta Tagging delle risorse AWS IAM Identity Center.
5. Scegliete Avanti e passate alla pagina successiva,Passaggio 3: Specificare le impostazioni di autenticazione.

Passaggio 3: Specificare le impostazioni di autenticazione

Per aggiungere un'applicazione gestita dal cliente che supporti OAuth 2.0 a IAM Identity Center, devi specificare un emittente di token affidabile. Un emittente di token affidabile è un server di autorizzazione OAuth 2.0 che crea token firmati. Questi token autorizzano le applicazioni che avviano richieste (richieste di applicazioni) per l'accesso alle applicazioni gestite (applicazioni di ricezione). AWS

1. Nella pagina Specificare le impostazioni di autenticazione, in Trusted token issuers, esegui una delle seguenti operazioni:

   - Per utilizzare un emittente di token affidabile esistente:

     Seleziona la casella di controllo accanto al nome dell'emittente di token affidabile che desideri utilizzare.
   - Per aggiungere un nuovo emittente affidabile di token:

1. Scegli Crea un emittente di token affidabile.
2. Si apre una nuova scheda del browser. Segui i passaggi da 5 a 8 pollici[Come aggiungere un emittente di token affidabile alla console IAM Identity Center](#).
3. Dopo aver completato questi passaggi, torna alla finestra del browser che stai utilizzando per la configurazione dell'applicazione e seleziona l'emittente di token affidabile che hai appena aggiunto.
4. Nell'elenco degli emittenti di token affidabili, seleziona la casella di controllo accanto al nome dell'emittente di token affidabile che hai appena aggiunto.

   Dopo aver selezionato un emittente di token attendibile, viene visualizzata la sezione Configura gli emittenti di token affidabili selezionati.

2. In Configura emittenti di token affidabili selezionati, inserisci il reclamo Aud. L'attestazione Aud identifica il pubblico (destinatari) previsto per il token generato dall'emittente affidabile del token. Per ulteriori informazioni, consulta [Reclamo Audi](#).
3. Per evitare che gli utenti debbano riautenticarsi quando utilizzano questa applicazione, seleziona Aggiorna automaticamente l'autenticazione utente per la sessione attiva dell'applicazione. Se selezionata, questa opzione aggiorna il token di accesso per la sessione ogni 60 minuti, fino alla scadenza della sessione o alla fine della sessione da parte dell'utente.
4. Scegliete Avanti e passate alla pagina successiva,. [Passaggio 4: Specificare le credenziali dell'applicazione](#)

Passaggio 4: Specificare le credenziali dell'applicazione

Completate i passaggi di questa procedura per specificare le credenziali utilizzate dall'applicazione per eseguire azioni di scambio di token con applicazioni attendibili. Queste credenziali vengono utilizzate in una politica basata sulle risorse. La politica richiede che l'utente specifichi un responsabile che disponga delle autorizzazioni necessarie per eseguire le azioni specificate nella politica. È necessario specificare un principale, anche se le applicazioni attendibili si trovano nella stessa Account AWS.

> **Note**
>
> Quando imposti le autorizzazioni con le politiche, concedi solo le autorizzazioni necessarie per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su

risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi.

Questa politica richiede l'azione. `sso-oauth:CreateTokenWithIAM`

1. Nella pagina Specificare le credenziali dell'applicazione, effettuate una delle seguenti operazioni:
   - Per specificare rapidamente uno o più ruoli IAM:
     1. Scegli Inserisci uno o più ruoli IAM.
     2. In Inserisci ruoli IAM, specifica l'Amazon Resource Name (ARN) di un ruolo IAM esistente. Per specificare l'ARN, utilizzare la sintassi seguente. La porzione di regione dell'ARN è vuota perché le risorse IAM sono globali.

        ```
        arn:aws:iam::account:role/role-name-with-path
        ```

        Per ulteriori informazioni, consulta Accesso tra account tramite policy basate su risorse e ARN IAM nella Guida per l'utente.AWS Identity and Access Management
   - Per modificare manualmente la policy (richiesta se si specificano non credenziali):AWS
     1. Seleziona Modifica la politica dell'applicazione.
     2. Modifica la tua politica digitando o incollando il testo nella casella di testo JSON.
     3. Risolvi eventuali avvisi di sicurezza, errori o avvisi generali generati durante la convalida delle politiche. Per ulteriori informazioni, consulta la sezione Convalida delle politiche IAM nella Guida per l'utente.AWS Identity and Access Management
2. Scegli Avanti e passa alla pagina successiva,Passaggio 5: revisione e configurazione.

Passaggio 5: revisione e configurazione

1. Nella pagina Rivedi e configura, esamina le scelte che hai fatto. Per apportare modifiche, scegli la sezione di configurazione desiderata, scegli Modifica e apporta le modifiche richieste.
2. Al termine, scegli Aggiungi applicazione.
3. L'applicazione che hai aggiunto viene visualizzata nell'elenco delle applicazioni gestite dal cliente.
4. Dopo aver configurato l'applicazione gestita dal cliente in IAM Identity Center, devi specificare uno o più AWS servizi, o applicazioni affidabili, per la propagazione dell'identità. Ciò consente

agli utenti di accedere all'applicazione gestita dal cliente e accedere ai dati nell'applicazione affidabile.

Per ulteriori informazioni, consulta Specificare applicazioni attendibili .

Specificare applicazioni attendibili

Dopo aver configurato l'applicazione gestita dal cliente, è necessario specificare uno o più AWS servizi o applicazioni attendibili per la propagazione delle identità. Specificate un AWS servizio con dati a cui gli utenti delle applicazioni gestite dai clienti devono accedere. Quando gli utenti accedono all'applicazione gestita dal cliente, tale applicazione trasmetterà l'identità degli utenti all'applicazione attendibile.

Utilizzate la procedura seguente per selezionare un servizio, quindi specificate le singole applicazioni da considerare affidabili per quel servizio.

1. Apri la console IAM Identity Center.
2. Selezionare Applications (Applicazioni).
3. Scegli la scheda Gestito dal cliente.
4. Nell'elenco Applicazioni gestite dal cliente, seleziona l'applicazione OAuth 2.0 per la quale desideri avviare le richieste di accesso. Questa è l'applicazione a cui accedono i tuoi utenti.
5. Nella pagina Dettagli, in Applicazioni attendibili per la propagazione dell'identità, scegli Specificare applicazioni affidabili.
6. In Tipo di installazione, seleziona Applicazioni individuali e specifica l'accesso, quindi scegli Avanti.
7. Nella pagina Seleziona servizio, scegli il AWS servizio con applicazioni che l'applicazione gestita dal cliente può considerare attendibili per la propagazione delle identità, quindi scegli Avanti.

   Il servizio selezionato definisce le applicazioni affidabili. Selezionerai le applicazioni nel passaggio successivo.
8. Nella pagina Seleziona applicazioni, scegli Applicazioni individuali, seleziona la casella di controllo per ogni applicazione che può ricevere richieste di accesso, quindi scegli Avanti.
9. Nella pagina Configura accesso, in Metodo di configurazione, esegui una delle seguenti operazioni:

   - Seleziona l'accesso per applicazione: seleziona questa opzione per configurare diversi livelli di accesso per ciascuna applicazione. Scegli l'applicazione per la quale desideri configurare il

livello di accesso, quindi scegli Modifica accesso. In Livello di accesso da applicare, modifica i livelli di accesso in base alle esigenze, quindi scegli Salva modifiche.

- Applica lo stesso livello di accesso a tutte le applicazioni: seleziona questa opzione se non devi configurare i livelli di accesso per singola applicazione.

10. Seleziona Successivo.
11. Nella pagina Rivedi la configurazione, esamina le scelte che hai fatto. Per apportare modifiche, scegli la sezione di configurazione desiderata, scegli Modifica accesso e quindi apporta le modifiche richieste.
12. Al termine, scegli Trust applications.

Utilizzo di applicazioni con un emittente di token affidabile

Gli emittenti di token affidabili consentono di utilizzare la propagazione delle identità affidabili con applicazioni che eseguono l'autenticazione all'esterno di. AWS Con gli emittenti di token affidabili, puoi autorizzare queste applicazioni a effettuare richieste per conto dei rispettivi utenti per accedere alle applicazioni gestite. AWS

I seguenti argomenti descrivono come funzionano gli emittenti di token affidabili e forniscono indicazioni sulla configurazione.

Argomenti

Panoramica degli emittenti di token affidabili

La propagazione affidabile delle identità fornisce un meccanismo che consente alle applicazioni che effettuano l'autenticazione all'esterno di AWS effettuare richieste per conto dei propri utenti utilizzando un emittente di token affidabile. Un emittente di token affidabile è un server di autorizzazione OAuth 2.0 che crea token firmati. Questi token autorizzano le applicazioni che avviano richieste (richieste di applicazioni) per l'accesso ai servizi (applicazioni di ricezione). AWS Le

applicazioni richiedenti avviano le richieste di accesso per conto degli utenti autenticati dall'emittente di token affidabile. Gli utenti sono noti sia all'emittente di token affidabile che a IAM Identity Center.

AWS i servizi che ricevono richieste gestiscono l'autorizzazione granulare alle proprie risorse in base agli utenti e all'appartenenza ai gruppi, come indicato nella directory Identity Center. AWS i servizi non possono utilizzare direttamente i token dell'emittente esterno del token.

Per risolvere questo problema, IAM Identity Center offre all'applicazione richiedente, o al AWS driver utilizzato dall'applicazione richiedente, un modo per scambiare il token emesso dall'emittente affidabile del token con un token generato da IAM Identity Center. Il token generato da IAM Identity Center si riferisce all'utente IAM Identity Center corrispondente. L'applicazione richiedente, o il driver, utilizza il nuovo token per avviare una richiesta all'applicazione ricevente. Poiché il nuovo token fa riferimento all'utente corrispondente in IAM Identity Center, l'applicazione ricevente può autorizzare l'accesso richiesto in base all'appartenenza dell'utente o al suo gruppo, come rappresentato in IAM Identity Center.

> **Important**
>
> La scelta di un server di autorizzazione OAuth 2.0 da aggiungere come emittente di token affidabile è una decisione di sicurezza che richiede un'attenta considerazione. Scegli solo emittenti di token affidabili di cui ti fidi per eseguire le seguenti attività:
>
> - Autentica l'utente specificato nel token.
> - Autorizza l'accesso di quell'utente all'applicazione ricevente.
> - Genera un token che IAM Identity Center può scambiare con un token creato da IAM Identity Center.

Prerequisiti e considerazioni per emittenti di token affidabili

Prima di configurare un emittente di token affidabile, esamina i seguenti prerequisiti e considerazioni.

- Configurazione dell'emittente di token affidabile

  È necessario configurare un server di autorizzazione OAuth 2.0 (l'emittente di token affidabile). Sebbene l'emittente affidabile di token sia in genere il provider di identità utilizzato come fonte di identità per IAM Identity Center, non è necessario che lo sia. Per informazioni su come configurare l'emittente di token affidabile, consulta la documentazione del provider di identità pertinente.

> **Note**
>
> Puoi configurare fino a 10 emittenti di token affidabili da utilizzare con IAM Identity Center, purché mappi l'identità di ogni utente nell'emittente di token affidabili a un utente corrispondente in IAM Identity Center.

- Il server di autorizzazione OAuth 2.0 (l'emittente affidabile del token) che crea il token deve disporre di un endpoint di rilevamento OpenID Connect (OIDC) che IAM Identity Center può utilizzare per ottenere le chiavi pubbliche per verificare le firme dei token. Per ulteriori informazioni, consulta URL dell'endpoint di rilevamento OIDC (URL dell'emittente).
- Token emessi dall'emittente di token affidabile

  I token emessi dall'emittente affidabile di token devono soddisfare i seguenti requisiti:

  - Il token deve essere firmato e in formato JSON Web Token (JWT) utilizzando l'algoritmo RS256.
  - Il token deve contenere le seguenti attestazioni:
    - Emittente (iss): l'entità che ha emesso il token. Questo valore deve corrispondere al valore configurato nell'endpoint di rilevamento OIDC (URL dell'emittente) nell'emittente del token affidabile.
    - Soggetto (sub): l'utente autenticato.
    - Pubblico (aud): il destinatario previsto del token. Questo è il AWS servizio a cui si accederà dopo lo scambio del token con un token di IAM Identity Center. Per ulteriori informazioni, consulta Reclamo Audi.
    - Ora di scadenza (exp): l'ora dopo la quale scade il token.
    -
  - Il token può essere un token di identità o un token di accesso.
  - Il token deve avere un attributo che può essere mappato in modo univoco a un utente IAM Identity Center.
- Affermazioni opzionali

  IAM Identity Center supporta tutte le attestazioni opzionali definite nella RFC 7523. Per ulteriori informazioni, consulta la Sezione 3: Formato JWT e requisiti di elaborazione di questa RFC.

  Ad esempio, il token può contenere un claim JTI (JWT ID). Questa affermazione, se presente, impedisce che i token con lo stesso JTI vengano riutilizzati per lo scambio di token. Per ulteriori informazioni sulle dichiarazioni JTI, consulta. Dettagli del reclamo JTI

- Configurazione di IAM Identity Center per l'utilizzo con un emittente di token affidabile

  È inoltre necessario abilitare IAM Identity Center, configurare la fonte di identità per IAM Identity Center ed effettuare il provisioning degli utenti che corrispondono agli utenti nella directory dell'emittente del token affidabile.

  A tale scopo, devi eseguire una delle seguenti operazioni:

  - Sincronizza gli utenti in IAM Identity Center utilizzando il protocollo System for Cross-domain Identity Management (SCIM) 2.0.
  - Crea gli utenti direttamente in IAM Identity Center.

  > **Note**
  >
  > Gli emittenti di token affidabili non sono supportati se utilizzi il servizio di dominio Active Directory come fonte di identità.

Dettagli del reclamo JTI

Se IAM Identity Center riceve una richiesta di scambio di un token che IAM Identity Center ha già scambiato, la richiesta fallisce. Per rilevare e impedire il riutilizzo di un token per lo scambio di token, puoi includere un claim JTI. IAM Identity Center protegge dalla riproduzione dei token in base alle affermazioni contenute nel token.

Non tutti i server di autorizzazione OAuth 2.0 aggiungono un'attestazione JTI ai token. Alcuni server di autorizzazione OAuth 2.0 potrebbero non consentire di aggiungere un JTI come attestazione personalizzata. I server di autorizzazione OAuth 2.0 che supportano l'uso di un'attestazione JTI potrebbero aggiungere questa dichiarazione solo ai token di identità, solo ai token di accesso o a entrambi. Per ulteriori informazioni, consulta la documentazione del tuo server di autorizzazione OAuth 2.0.

Per informazioni sulla creazione di applicazioni che scambiano token, consulta la documentazione dell'API IAM Identity Center. Per informazioni sulla configurazione di un'applicazione gestita dal cliente per ottenere e scambiare i token corretti, consulta la documentazione dell'applicazione.

Impostazioni di configurazione dell'emittente di token affidabili

Le sezioni seguenti descrivono le impostazioni necessarie per configurare e utilizzare un emittente di token affidabile.

Argomenti

URL dell'endpoint di rilevamento OIDC (URL dell'emittente)

Quando aggiungi un emittente di token affidabile alla console IAM Identity Center, devi specificare l'URL dell'endpoint di rilevamento OIDC. A questo URL si fa comunemente riferimento con il relativo URL,. `/.well-known/openid-configuration` Nella console IAM Identity Center, questo URL è chiamato URL emittente.

> **Note**
>
> È necessario incollare l'URL dell'endpoint di rilevamento fino alla fine. `.well-known/openid-configuration` Se `.well-known/openid-configuration` è inclusa nell'URL, la configurazione dell'emittente del token affidabile non funzionerà. Poiché IAM Identity Center non convalida questo URL, se l'URL non è formato correttamente, la configurazione dell'emittente di token affidabile fallirà senza notifica.

IAM Identity Center utilizza questo URL per ottenere informazioni aggiuntive sull'emittente affidabile del token. Ad esempio, IAM Identity Center utilizza questo URL per ottenere le informazioni necessarie per verificare i token generati dall'emittente di token affidabile. Quando aggiungi un emittente di token affidabile a IAM Identity Center, devi specificare questo URL. Per trovare l'URL, consulta la documentazione del provider del server di autorizzazione OAuth 2.0 che utilizzi per generare i token per la tua applicazione oppure contatta direttamente il provider per ricevere assistenza.

Mappatura degli attributi

Le mappature degli attributi consentono a IAM Identity Center di abbinare l'utente rappresentato in un token emesso da un emittente di token affidabile a un singolo utente in IAM Identity Center. È necessario specificare la mappatura degli attributi quando si aggiunge l'emittente di token affidabile a IAM Identity Center. Questa mappatura degli attributi viene utilizzata in un claim nel token generato dall'emittente affidabile del token. Il valore nell'attestazione viene utilizzato per effettuare ricerche in IAM Identity Center. La ricerca utilizza l'attributo specificato per recuperare un singolo utente in IAM Identity Center, che verrà utilizzato come utente all'interno AWS. L'affermazione scelta deve essere

mappata a un attributo in un elenco fisso di attributi disponibili nell'archivio di identità di IAM Identity Center. Puoi scegliere uno dei seguenti attributi dell'archivio di identità di IAM Identity Center: nome utente, email e ID esterno. Il valore dell'attributo specificato in IAM Identity Center deve essere unico per ogni utente.

Reclamo Audi

Un claim aud identifica il pubblico (destinatari) a cui è destinato un token. Quando l'applicazione che richiede l'accesso viene autenticata tramite un provider di identità non federato a IAM Identity Center, tale provider di identità deve essere configurato come emittente di token affidabile. L'applicazione che riceve la richiesta di accesso (l'applicazione ricevente) deve scambiare il token generato dall'emittente affidabile del token con un token generato da IAM Identity Center.

Per informazioni su come ottenere i valori delle dichiarazioni aud per l'applicazione ricevente quando sono registrati nel Trusted Token Emittent, consulta la documentazione dell'emittente del token affidabile o contatta l'amministratore dell'emittente del token affidabile per ricevere assistenza.

Configurazione di un emittente di token affidabile

Per abilitare la propagazione affidabile dell'identità per un'applicazione che si autentica esternamente su IAM Identity Center, uno o più amministratori devono configurare un emittente di token affidabile. Un emittente di token affidabile è un server di autorizzazione OAuth 2.0 che rilascia token alle applicazioni che avviano le richieste (applicazioni richiedenti). I token autorizzano queste applicazioni a inviare richieste per conto dei loro utenti a un'applicazione (un servizio) ricevente. AWS

Argomenti

- Coordinamento dei ruoli e delle responsabilità amministrative
- Attività per la configurazione di un emittente di token affidabile
- Come aggiungere un emittente di token affidabile alla console IAM Identity Center
- Come visualizzare o modificare le impostazioni dell'emittente di token affidabili nella console IAM Identity Center
- Processo di configurazione e flusso di richiesta per le applicazioni che utilizzano un emittente di token affidabile

Coordinamento dei ruoli e delle responsabilità amministrative

In alcuni casi, un singolo amministratore può eseguire tutte le attività necessarie per configurare un emittente di token affidabile. Se più amministratori svolgono queste attività, è necessario uno stretto

coordinamento. La tabella seguente descrive come più amministratori potrebbero coordinarsi per configurare un emittente di token affidabile e configurare il AWS servizio per utilizzarlo.

> **Note**
>
> L'applicazione può essere qualsiasi AWS servizio integrato con IAM Identity Center e che supporta la propagazione affidabile delle identità.

Per ulteriori informazioni, consulta Attività per la configurazione di un emittente di token affidabile.

Ruolo	Esegue queste attività	Si coordina con
Amministratore di IAM Identity Center	Aggiunge l'IdP esterno come emittente di token affidabile alla console IAM Identity Center. Aiuta a configurare la corretta mappatura degli attributi tra IAM Identity Center e l'IdP esterno. Notifica all'amministratore del AWS servizio quando l'emittente affidabile del token viene aggiunto alla console IAM Identity Center.	Amministratore IdP esterno (trusted token issuer) AWS amministratore del servizio
Amministratore IdP esterno (trusted token issuer)	Configura l'IdP esterno per l'emissione di token. Aiuta a configurare la corretta mappatura degli attributi tra IAM Identity Center e l'IdP esterno. Fornisce il nome del pubblico (Aud claim) all'amministratore del AWS servizio.	Amministratore di IAM Identity Center AWS amministratore del servizio
AWS amministratore del servizio	Verifica nella console AWS di servizio l'emittente affidabile del	Amministratore di IAM Identity Center

Ruolo	Esegue queste attività	Si coordina con
	token. L'emittente affidabile del token sarà visibile nella console di AWS servizio dopo che l'amministratore di IAM Identity Center lo avrà aggiunto alla console IAM Identity Center. Configura il AWS servizio per utilizzare l'emittente di token affidabile.	Amministratore IdP esterno (trusted token issuer)

Attività per la configurazione di un emittente di token affidabile

Per configurare un emittente di token affidabile, un amministratore di IAM Identity Center, un amministratore IdP esterno (trusted token issuer) e un amministratore dell'applicazione devono completare le seguenti attività.

> **Note**
>
> L'applicazione può essere qualsiasi AWS servizio integrato con IAM Identity Center e che supporta la propagazione affidabile delle identità.

1. Aggiungi l'emittente di token affidabile a IAM Identity Center: l'amministratore di IAM Identity Center aggiunge l'emittente di token affidabile utilizzando la console o le API IAM Identity Center. Questa configurazione richiede di specificare quanto segue:
   - Un nome per l'emittente affidabile del token
   - L'URL dell'endpoint di rilevamento OIDC (nella console IAM Identity Center, questo URL è chiamato URL dell'emittente).
   - Mappatura degli attributi per la ricerca degli utenti. Questa mappatura degli attributi viene utilizzata in un claim nel token generato dall'emittente affidabile del token. Il valore nell'attestazione viene utilizzato per effettuare ricerche in IAM Identity Center. La ricerca utilizza l'attributo specificato per recuperare un singolo utente in IAM Identity Center.

2. Connetti il AWS servizio a IAM Identity Center: l'amministratore del AWS servizio deve connettere l'applicazione a IAM Identity Center utilizzando la console per l'applicazione o le API dell'applicazione.

   Dopo che l'emittente affidabile del token è stato aggiunto alla console IAM Identity Center, è visibile anche nella console di AWS servizio e può essere selezionato dall'amministratore del AWS servizio.

3. Configura l'uso dello scambio di token: nella console di AWS servizio, l'amministratore del servizio configura AWS il AWS servizio in modo che accetti i token emessi dall'emittente di token affidabile. Questi token vengono scambiati con token generati da IAM Identity Center. Ciò richiede di specificare il nome dell'emittente affidabile del token riportato nella fase 1 e il valore del claim Aud corrispondente al servizio. AWS

   L'emittente affidabile del token inserisce il valore del claim Aud nel token emesso per indicare che il token è destinato all'uso da parte del servizio. AWS Per ottenere questo valore, contatta l'amministratore dell'emittente del token affidabile.

Come aggiungere un emittente di token affidabile alla console IAM Identity Center

In un'organizzazione con più amministratori, questa attività viene eseguita da un amministratore di IAM Identity Center. Se sei l'amministratore di IAM Identity Center, devi scegliere quale IdP esterno utilizzare come emittente di token affidabile.

Per aggiungere un emittente di token affidabile alla console IAM Identity Center

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Autenticazione.
4. In Trusted token issuers, scegli Crea un emittente di token affidabile.
5. Nella pagina Configura un IdP esterno per l'emissione di token affidabili, in Dettagli sull'emittente del token affidabile, procedi come segue:

   - Per l'URL dell'emittente, specifica l'URL di rilevamento OIDC dell'IdP esterno che emetterà i token per la propagazione delle identità affidabili. È necessario specificare l'URL dell'endpoint di rilevamento fino alla versione precedente. `.well-known/openid-configuration` L'amministratore dell'IdP esterno può fornire questo URL.

> **Note**
>
> Nota Questo URL deve corrispondere all'URL nell'attestazione Issuer (iss) nei token emessi per la propagazione di identità affidabili.

- Per il nome dell'emittente affidabile del token, inserisci un nome per identificare questo emittente di token affidabile in IAM Identity Center e nella console dell'applicazione.

6. In Attributi della mappa, procedi come segue:
   - Per l'attributo del provider di identità, seleziona un attributo dall'elenco da mappare a un attributo nell'archivio di identità di IAM Identity Center.
   - Per l'attributo IAM Identity Center, seleziona l'attributo corrispondente per la mappatura degli attributi.
7. In Tag (opzionale), scegli Aggiungi nuovo tag, specifica un valore per Chiave e, facoltativamente, per Valore.

   Per ulteriori informazioni sui tag, consulta Tagging delle risorse AWS IAM Identity Center.
8. Scegli Crea un emittente di token affidabile.
9. Dopo aver completato la creazione dell'emittente di token affidabile, contatta l'amministratore dell'applicazione per comunicargli il nome dell'emittente del token affidabile, in modo che possa confermare che l'emittente del token affidabile è visibile nella console applicabile.
10. L'amministratore dell'applicazione deve selezionare questo emittente di token affidabile nella console applicabile per consentire l'accesso degli utenti all'applicazione dalle applicazioni configurate per la propagazione delle identità affidabili.

Come visualizzare o modificare le impostazioni dell'emittente di token affidabili nella console IAM Identity Center

Dopo aver aggiunto un emittente di token affidabile alla console IAM Identity Center, puoi visualizzare e modificare le impostazioni pertinenti.

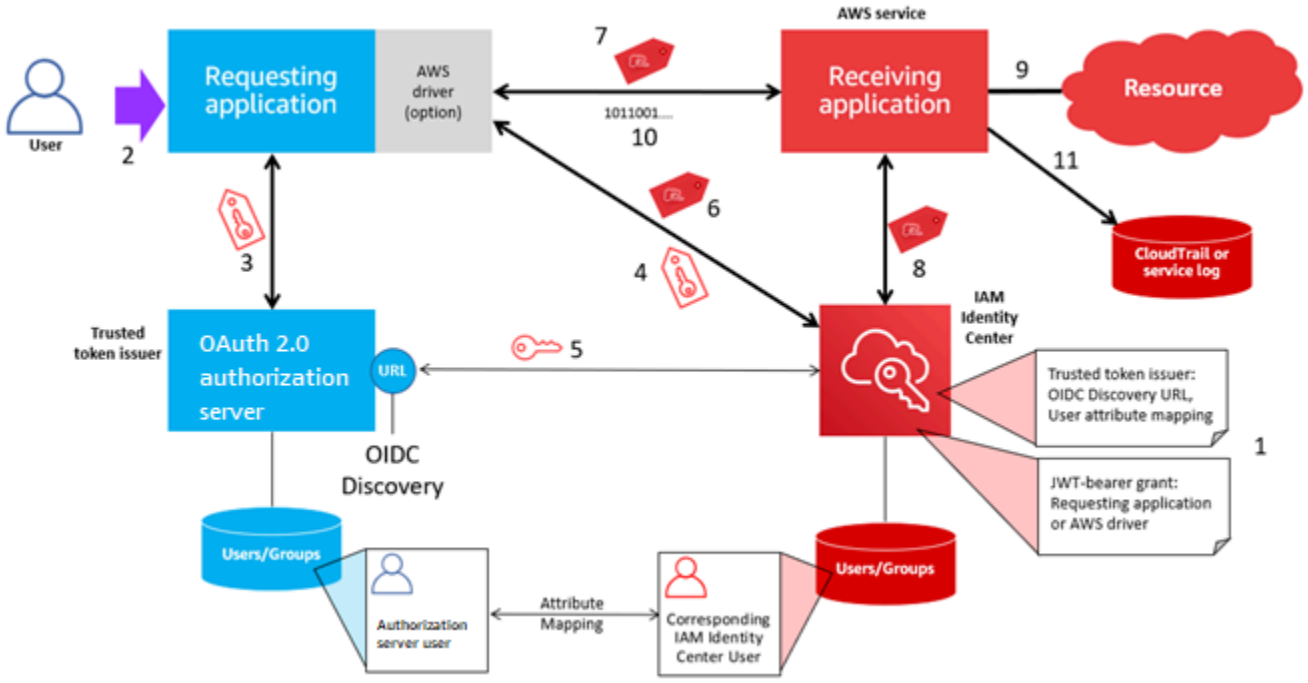
Se prevedi di modificare le impostazioni dell'emittente di token affidabili, tieni presente che così facendo gli utenti potrebbero perdere l'accesso a tutte le applicazioni configurate per utilizzare l'emittente di token affidabili. Per evitare di interrompere l'accesso degli utenti, consigliamo di coordinarsi con gli amministratori di tutte le applicazioni configurate per utilizzare l'emittente di token affidabile prima di modificare le impostazioni.

Per visualizzare o modificare le impostazioni dell'emittente di token affidabili nella console IAM Identity Center

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Autenticazione.
4. In Emittenti di token affidabili, seleziona l'emittente di token affidabile che desideri visualizzare o modificare.
5. Seleziona Azioni, quindi scegli Modifica.
6. Nella pagina Modifica emittente di token affidabili, visualizza o modifica le impostazioni secondo necessità. È possibile modificare il nome dell'emittente del token affidabile, le mappature degli attributi e i tag.
7. Seleziona Salvataggio delle modifiche.
8. Nella finestra di dialogo Modifica emittente di token affidabili, ti viene richiesto di confermare che desideri apportare modifiche. Scegli Conferma.

Processo di configurazione e flusso di richiesta per le applicazioni che utilizzano un emittente di token affidabile

Questa sezione descrive il processo di configurazione e il flusso di richiesta per le applicazioni che utilizzano un emittente di token affidabile per la propagazione dell'identità affidabile. Il diagramma seguente fornisce una panoramica di questo processo.



I passaggi seguenti forniscono informazioni aggiuntive su questo processo.

1. Configura IAM Identity Center e l'applicazione AWS gestita ricevente per utilizzare un emittente di token affidabile. Per informazioni, consulta Attività per la configurazione di un emittente di token affidabile.
2. Il flusso di richieste inizia quando un utente apre l'applicazione richiedente.
3. L'applicazione richiedente richiede un token all'emittente affidabile del token per avviare le richieste all'applicazione gestita ricevente. AWS Se l'utente non si è ancora autenticato, questo processo attiva un flusso di autenticazione. Il token contiene le seguenti informazioni:
   - L'oggetto (Sub) dell'utente.
   - L'attributo utilizzato da IAM Identity Center per cercare l'utente corrispondente in IAM Identity Center.
   - Un'affermazione di tipo audience (Aud) che contiene un valore che l'emittente affidabile del token associa all'applicazione AWS gestita ricevente. Se sono presenti altre attestazioni, non vengono utilizzate da IAM Identity Center.
4. L'applicazione richiedente, o il AWS driver che utilizza, passa il token a IAM Identity Center e richiede che il token venga scambiato con un token generato da IAM Identity Center. Se si utilizza un AWS driver, potrebbe essere necessario configurarlo per questo caso d'uso. Per ulteriori informazioni, consulta la documentazione dell'applicazione AWS gestita pertinente.

5. IAM Identity Center utilizza l'endpoint OIDC Discovery per ottenere la chiave pubblica che può utilizzare per verificare l'autenticità del token. IAM Identity Center esegue quindi le seguenti operazioni:
   - Verifica il token.
   - Cerca nella directory di Identity Center. A tale scopo, IAM Identity Center utilizza l'attributo mappato specificato nel token.
   - Verifica che l'utente sia autorizzato ad accedere all'applicazione ricevente. Se l'applicazione AWS gestita è configurata per richiedere assegnazioni a utenti e gruppi, l'utente deve disporre di un'assegnazione diretta o basata sul gruppo all'applicazione; in caso contrario la richiesta viene rifiutata. Se l'applicazione AWS gestita è configurata per non richiedere assegnazioni a utenti e gruppi, l'elaborazione continua.

     > **Note**
     >
     > AWS i servizi hanno una configurazione di impostazione predefinita che determina se sono necessarie assegnazioni per utenti e gruppi. Si consiglia di non modificare l'impostazione Richiedi assegnazioni per queste applicazioni se si prevede di utilizzarle con una propagazione affidabile delle identità. Anche se sono state configurate autorizzazioni granulari che consentono l'accesso degli utenti a risorse applicative specifiche, la modifica dell'impostazione Richiedi assegnazioni potrebbe causare comportamenti imprevisti, tra cui l'interruzione dell'accesso degli utenti a tali risorse.

   - Verifica che l'applicazione richiedente sia configurata per utilizzare ambiti validi per l'applicazione gestita ricevente. AWS
6. Se i passaggi di verifica precedenti hanno esito positivo, IAM Identity Center crea un nuovo token. Il nuovo token è un token opaco (crittografato) che include l'identità dell'utente corrispondente in IAM Identity Center, il pubblico (Aud) dell'applicazione AWS gestita ricevente e gli ambiti che l'applicazione richiedente può utilizzare per effettuare richieste all'applicazione gestita AWS ricevente.
7. L'applicazione richiedente, o il driver che utilizza, avvia una richiesta di risorse all'applicazione ricevente e passa il token generato da IAM Identity Center all'applicazione ricevente.
8. L'applicazione ricevente effettua chiamate a IAM Identity Center per ottenere l'identità dell'utente e gli ambiti codificati nel token. Potrebbe anche effettuare richieste per ottenere gli attributi utente o l'appartenenza ai gruppi dell'utente dalla directory di Identity Center.
9. L'applicazione ricevente utilizza la propria configurazione di autorizzazione per determinare se l'utente è autorizzato ad accedere alla risorsa dell'applicazione richiesta.

10. Se l'utente è autorizzato ad accedere alla risorsa dell'applicazione richiesta, l'applicazione ricevente risponde alla richiesta.
11. L'identità dell'utente, le azioni eseguite per suo conto e altri eventi registrati nei registri e CloudTrail negli eventi dell'applicazione ricevente. Il modo specifico in cui queste informazioni vengono registrate varia in base all'applicazione.

Gestisci i certificati IAM Identity Center

IAM Identity Center utilizza i certificati per configurare una relazione di fiducia SAML tra IAM Identity Center e il fornitore di servizi dell'applicazione. Quando aggiungi un'applicazione in IAM Identity Center, viene creato automaticamente un certificato IAM Identity Center da utilizzare con quell'applicazione durante il processo di configurazione. Per impostazione predefinita, questo certificato IAM Identity Center generato automaticamente è valido per un periodo di cinque anni.

In qualità di amministratore di IAM Identity Center, a volte dovrai sostituire i vecchi certificati con quelli più recenti per una determinata applicazione. Ad esempio, potrebbe essere necessario sostituire un certificato quando si avvicina la data di scadenza del certificato. Il processo di sostituzione di un certificato precedente con uno più recente viene definito rotazione dei certificati.

Argomenti

Considerazioni prima della rotazione di un certificato

Prima di iniziare il processo di rotazione di un certificato in IAM Identity Center, considera quanto segue:

- Il processo di rotazione della certificazione richiede il ripristino della fiducia tra IAM Identity Center e il fornitore di servizi. Per ristabilire la fiducia, utilizza le procedure fornite in. Ruota un certificato IAM Identity Center
- L'aggiornamento del certificato con il fornitore di servizi può causare un'interruzione temporanea del servizio per gli utenti fino a quando la fiducia non viene ristabilita con successo. Pianifica attentamente questa operazione durante le ore non di punta, se possibile.

Ruota un certificato IAM Identity Center

La rotazione di un certificato IAM Identity Center è un processo in più fasi che prevede quanto segue:

- Generazione di un nuovo certificato
- Aggiungere il nuovo certificato al sito Web del fornitore di servizi
- Impostazione del nuovo certificato su attivo
- Eliminazione del certificato inattivo

Utilizza tutte le seguenti procedure nell'ordine seguente per completare il processo di rotazione dei certificati per una determinata applicazione.

Fase 1: Generare un nuovo certificato.

I nuovi certificati IAM Identity Center generati possono essere configurati per utilizzare le seguenti proprietà:

- Periodo di validità: specifica il tempo assegnato (in mesi) prima della scadenza di un nuovo certificato IAM Identity Center.
- Dimensione della chiave: determina il numero di bit che una chiave deve utilizzare con il relativo algoritmo crittografico. È possibile impostare questo valore su RSA a 1024 bit o RSA a 2048 bit. Per informazioni generali sul funzionamento delle dimensioni delle chiavi nella crittografia, consulta Dimensione delle chiavi.
- Algoritmo: specifica l'algoritmo utilizzato da IAM Identity Center per firmare l'asserzione/risposta SAML. È possibile impostare questo valore su SHA-1 o SHA-256. AWS consiglia di utilizzare SHA-256 quando possibile, a meno che il provider di servizi non richieda SHA-1. Per informazioni generali sul funzionamento degli algoritmi di crittografia, vedere Crittografia a chiave pubblica.

1. Apri la console IAM Identity Center.
2. Selezionare Applications (Applicazioni).
3. Nell'elenco delle applicazioni, scegli l'applicazione per cui desideri generare un nuovo certificato.
4. Nella pagina dei dettagli dell'applicazione, scegli la scheda Configurazione. Sotto i metadati di IAM Identity Center, scegli Gestisci certificato. Se non disponi di una scheda Configurazione o l'impostazione di configurazione non è disponibile, non è necessario ruotare il certificato per questa applicazione.

5. Nella pagina del certificato IAM Identity Center, scegli Genera nuovo certificato.
6. Nella finestra di dialogo Genera nuovo certificato IAM Identity Center, specifica i valori appropriati per Periodo di validità, Algoritmo e Dimensione della chiave. Quindi scegli Genera.

Passaggio 2: aggiorna il sito Web del fornitore di servizi.

Utilizzare la procedura seguente per ristabilire la fiducia con il fornitore di servizi dell'applicazione.

> **Important**
>
> Quando carichi il nuovo certificato sul fornitore di servizi, gli utenti potrebbero non essere in grado di autenticarsi. Per correggere questa situazione, imposta il nuovo certificato come attivo come descritto nel passaggio successivo.

1. Nella console IAM Identity Center, scegli l'applicazione per cui hai appena generato un nuovo certificato.
2. Nella pagina dei dettagli dell'applicazione, scegli Modifica configurazione.
3. Scegli Visualizza istruzioni, quindi segui le istruzioni per il sito Web del provider di servizi applicativi specifico per aggiungere il certificato appena generato.

Passaggio 3: imposta il nuovo certificato come attivo.

A un'applicazione possono essere assegnati fino a due certificati. IAM Identity Center utilizzerà la certificazione impostata come attiva per firmare tutte le asserzioni SAML.

1. Apri la console IAM Identity Center.
2. Selezionare Applications (Applicazioni).
3. Nell'elenco delle applicazioni, scegli la tua applicazione.
4. Nella pagina dei dettagli dell'applicazione, scegli la scheda Configurazione. Sotto i metadati di IAM Identity Center, scegli Gestisci certificato.
5. Nella pagina del certificato IAM Identity Center, seleziona il certificato che desideri impostare come attivo, scegli Azioni, quindi scegli Imposta come attivo.
6. Nella finestra di dialogo Imposta il certificato selezionato come attivo, conferma di aver compreso che per impostare un certificato come attivo potrebbe essere necessario ristabilire la fiducia, quindi scegli Rendi attivo.

Fase 4: Eliminare il vecchio certificato.

Utilizza la seguente procedura per completare il processo di rotazione dei certificati per la tua applicazione. È possibile eliminare solo un certificato che si trova in uno stato Inattivo.

1. Apri la console IAM Identity Center.
2. Selezionare Applications (Applicazioni).
3. Nell'elenco delle applicazioni, scegli la tua applicazione.
4. Nella pagina dei dettagli dell'applicazione, seleziona la scheda Configurazione. Sotto i metadati di IAM Identity Center, scegli Gestisci certificato.
5. Nella pagina del certificato IAM Identity Center, seleziona il certificato che desideri eliminare. Scegliere Actions (Operazioni), quindi selezionare Delete (Elimina VPC).
6. Nella finestra di dialogo Elimina certificato, scegli Elimina.

Indicatori dello stato di scadenza del certificato

Nella pagina Applicazioni, nelle proprietà di un'applicazione, è possibile notare delle icone colorate degli indicatori di stato. Queste icone vengono visualizzate nella colonna Scade il accanto a ciascun certificato nell'elenco. Di seguito vengono descritti i criteri utilizzati da IAM Identity Center per determinare quale icona viene visualizzata per ogni certificato.

- Rosso: indica che un certificato è attualmente scaduto.
- Giallo: indica che un certificato scadrà tra 90 giorni o meno.
- Verde: indica che un certificato è attualmente valido e rimarrà valido per almeno altri 90 giorni.

Per verificare lo stato attuale di un certificato

1. Apri la console IAM Identity Center.
2. Selezionare Applications (Applicazioni).
3. Nell'elenco delle applicazioni, controlla lo stato dei certificati nell'elenco, come indicato nella colonna Scade il.

Configura le proprietà dell'applicazione nella console IAM Identity Center

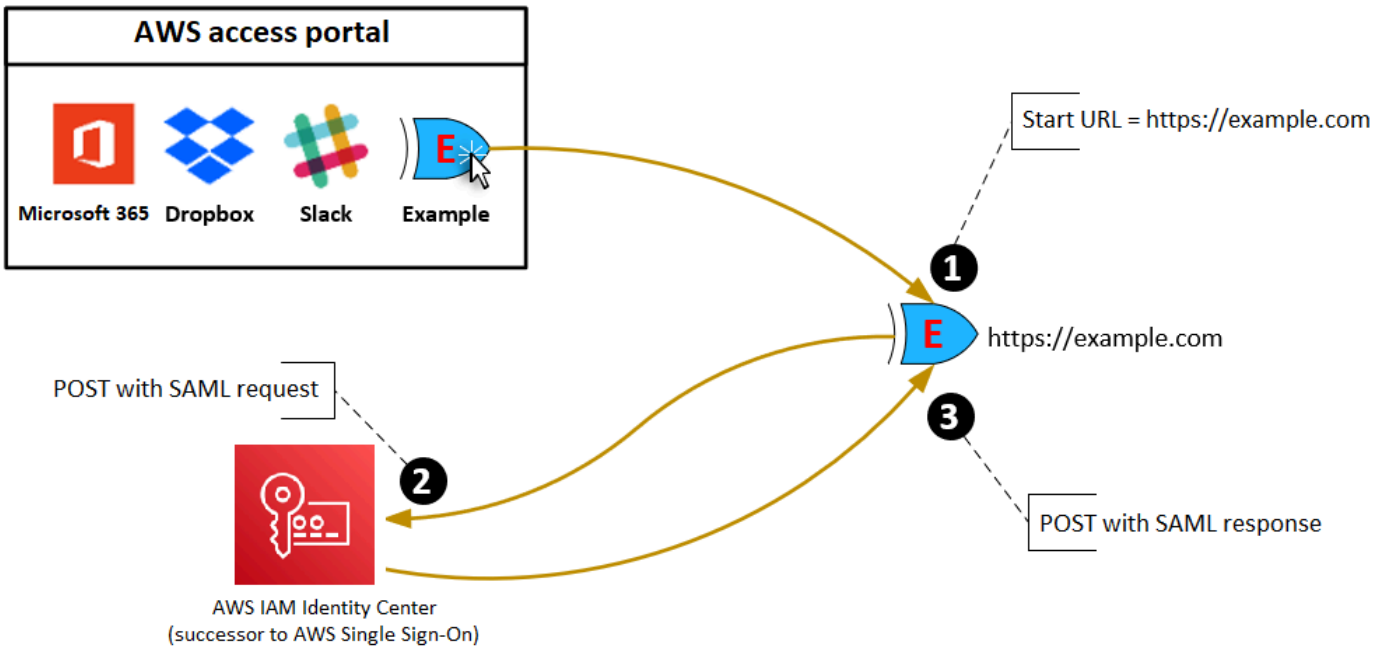
In IAM Identity Center puoi personalizzare l'esperienza utente configurando l'URL di avvio dell'applicazione, lo stato di inoltro e la durata della sessione.

URL di avvio dell'applicazione

È possibile utilizzare un URL di avvio dell'applicazione per iniziare il processo di federazione con la tua applicazione. L'uso tipico è per un'applicazione che supporta solo l'associazione avviata dal provider di servizi (SP).

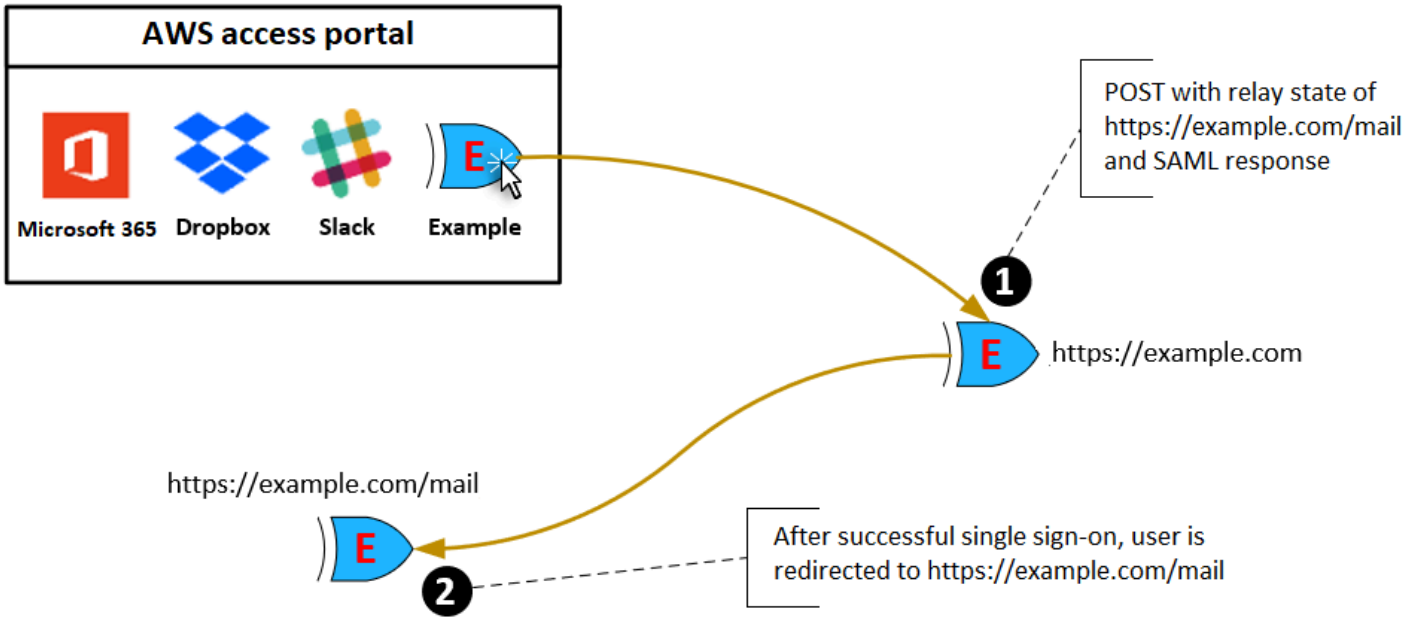
I passaggi e il diagramma seguenti illustrano il flusso di lavoro di autenticazione URL di avvio dell'applicazione quando un utente sceglie un'applicazione nel portale di accesso: AWS

1. Il browser dell'utente reindirizza la richiesta di autenticazione utilizzando il valore dell'URL di avvio dell'applicazione (in questo caso https://example.com).
2. L'applicazione invia un `HTML POST` with a `SAMLRequest` a IAM Identity Center.
3. IAM Identity Center invia quindi un messaggio `HTML POST` con un `SAMLResponse` messaggio all'applicazione.



Stato del relè

Durante il processo di autenticazione della federazione, lo stato del relay reindirizza gli utenti all'interno dell'applicazione. Per SAML 2.0, questo valore viene passato, senza modifiche, all'applicazione. Dopo aver configurato le proprietà dell'applicazione, IAM Identity Center invia il valore dello stato di inoltro insieme a una risposta SAML all'applicazione.



Durata della sessione

La durata della sessione è il periodo di tempo per il quale una sessione utente dell'applicazione è valida. Per SAML 2.0, viene utilizzato per impostare la `SessionNotOnOrAfter` data dell'elemento dell'asserzione SAML. `saml2:AuthNStatement`

La durata della sessione può essere interpretata dalle applicazioni in uno dei seguenti modi:

- Le applicazioni possono utilizzarla per determinare il tempo massimo consentito per la sessione dell'utente. Le applicazioni potrebbero generare una sessione utente con una durata inferiore. Questo può accadere quando l'applicazione supporta solo le sessioni degli utenti con una durata che è inferiore alla durata configurata per la sessione.
- Le applicazioni possono utilizzarla come durata esatta e potrebbe non consentire agli amministratori di configurare il valore. Questo può accadere quando l'applicazione supporta solo una durata di sessione specifica.

Per ulteriori informazioni su come viene utilizzata la durata della sessione, consulta la documentazione dell'applicazione specifica.

Assegna l'accesso degli utenti alle applicazioni nella console IAM Identity Center

Puoi assegnare agli utenti l'accesso Single Sign-On alle applicazioni SAML 2.0 nel catalogo delle applicazioni o alle applicazioni SAML 2.0 personalizzate.

Considerazioni per le assegnazioni di gruppo:

- Assegna l'accesso direttamente ai gruppi. Per semplificare l'amministrazione delle autorizzazioni di accesso, si consiglia di assegnare l'accesso direttamente ai gruppi anziché ai singoli utenti. Con i gruppi puoi concedere o negare le autorizzazioni a gruppi di utenti, anziché applicare tali autorizzazioni a ogni singolo individuo. Se un utente passa a un'organizzazione diversa, è sufficiente spostarlo in un gruppo diverso. L'utente riceve quindi automaticamente le autorizzazioni necessarie per la nuova organizzazione.
- I gruppi annidati non sono supportati. Quando si assegna l'accesso degli utenti alle applicazioni, IAM Identity Center non supporta l'aggiunta di utenti ai gruppi nidificati. Se un utente viene aggiunto a un gruppo nidificato, potrebbe ricevere un messaggio «Non hai alcuna applicazione» durante l'accesso. Le assegnazioni devono essere effettuate nei confronti del gruppo immediato di cui l'utente è membro.

Per assegnare l'accesso di utenti o gruppi alle applicazioni

> **Important**
>
> Per le applicazioni AWS gestite, è necessario aggiungere utenti direttamente dalle console delle applicazioni pertinenti o tramite le API.

1. Apri la console IAM Identity Center.

> **Note**
>
> Se gestisci gli utenti in AWS Managed Microsoft AD, assicurati che la console IAM Identity Center utilizzi la AWS regione in cui si trova la tua AWS Managed Microsoft AD directory prima di procedere con il passaggio successivo.

2. Selezionare Applications (Applicazioni).
3. Nell'elenco delle applicazioni, scegli il nome dell'applicazione a cui desideri assegnare l'accesso.
4. Nella pagina dei dettagli dell'applicazione, nella sezione Utenti assegnati, scegli Assegna utenti.
5. Nella finestra di dialogo Assegna utenti, immettete un nome utente o di gruppo. Puoi anche cercare utenti e gruppi. Puoi specificare più utenti o gruppi selezionando gli account applicabili come vengono visualizzati nei risultati della ricerca.
6. Scegliere Assign users (Assegna utenti).

Rimuovi l'accesso degli utenti nella console IAM Identity Center

Utilizza questa procedura per rimuovere l'accesso degli utenti alle applicazioni SAML 2.0 nel catalogo delle applicazioni o alle applicazioni SAML 2.0 personalizzate.

Per rimuovere l'accesso degli utenti a un'applicazione

1. Apri la console IAM Identity Center.
2. Selezionare Applications (Applicazioni).
3. Nell'elenco delle applicazioni, scegli l'applicazione da cui desideri rimuovere l'accesso utente.
4. Nella pagina dei dettagli dell'applicazione, nella sezione Utenti assegnati, seleziona l'utente o il gruppo che desideri rimuovere, quindi scegli il pulsante Rimuovi accesso.
5. Nella finestra di dialogo Remove access (Rimuovi accesso), verifica il nome dell'utente o del gruppo, Scegli quindi Remove access (Rimuovi accesso).

Mappa gli attributi dell'applicazione agli attributi di IAM Identity Center

Alcuni provider di servizi richiedono asserzioni SAML personalizzate per trasferire dati aggiuntivi sugli accessi degli utenti. In tal caso, utilizza la seguente procedura per specificare in che modo gli attributi utente delle applicazioni devono mappare agli attributi corrispondenti in IAM Identity Center.

Per mappare gli attributi dell'applicazione agli attributi in IAM Identity Center

1. Apri la console IAM Identity Center.
2. Selezionare Applications (Applicazioni).
3. Nell'elenco delle applicazioni, scegli l'applicazione in cui desideri mappare gli attributi.
4. Nella pagina dei dettagli dell'applicazione, scegli Azioni, quindi scegli Modifica mappatura degli attributi.
5. Scegli Aggiungi nuova mappatura degli attributi.
6. Nella prima casella di testo, inserisci l'attributo dell'applicazione.
7. Nella seconda casella di testo, inserisci l'attributo in IAM Identity Center che desideri mappare all'attributo dell'applicazione. Ad esempio, potresti voler mappare l'attributo dell'applicazione **`Username`** all'attributo utente di IAM Identity Center**`email`**. Per visualizzare l'elenco degli attributi utente consentiti in IAM Identity Center, consulta la tabella inAWS Managed Microsoft AD Mappature degli attributi per le directory.
8. Nella terza colonna della tabella, scegli il formato appropriato per l'attributo dal menu.
9. Scegli Save changes (Salva modifiche).

Progettazione della resilienza e comportamento regionale

Il servizio IAM Identity Center è completamente gestito e utilizza AWS servizi durevoli e altamente disponibili, come Amazon S3 e Amazon EC2. Per garantire la disponibilità in caso di interruzione della zona di disponibilità, IAM Identity Center opera su più zone di disponibilità. Per informazioni sugli obiettivi di progettazione della disponibilità per IAM Identity Center, consulta l'Appendice A: Designed-For Availability for Select AWS Services nella Reliability Pillar Guide.

Abilita IAM Identity Center nel tuo account di gestione. AWS Organizations Ciò è necessario affinché IAM Identity Center possa effettuare il provisioning, il de-provisioning e l'aggiornamento dei ruoli per tutti i tuoiAccount AWS. Quando abiliti IAM Identity Center, questo viene distribuito su Regione AWS quello attualmente selezionato. Se desideri eseguire la distribuzione in uno specificoRegione AWS, modifica la selezione della regione prima di abilitare IAM Identity Center.

> **Note**
>
> IAM Identity Center controlla l'accesso ai suoi set di autorizzazioni e alle sue applicazioni solo dalla sua regione principale. Ti consigliamo di considerare i rischi associati al controllo degli accessi quando IAM Identity Center opera in una singola regione.

Sebbene IAM Identity Center determini l'accesso dalla regione in cui abiliti il servizio, Account AWS sono globali. Ciò significa che, dopo aver effettuato l'accesso a IAM Identity Center, gli utenti possono operare in qualsiasi regione quando accedono Account AWS tramite IAM Identity Center. La maggior parte delle applicazioni AWS gestite come Amazon SageMaker, tuttavia, deve essere installata nella stessa regione di IAM Identity Center per consentire agli utenti di autenticarsi e assegnare l'accesso a queste applicazioni. Per informazioni sui vincoli regionali quando si utilizza un'applicazione con IAM Identity Center, consulta la documentazione dell'applicazione.

Puoi anche utilizzare IAM Identity Center per autenticare e autorizzare l'accesso alle applicazioni basate su SAML raggiungibili tramite un URL pubblico, indipendentemente dalla piattaforma o dal cloud su cui è costruita l'applicazione.

Non è consigliabile utilizzarlo Istanze di account di IAM Identity Center come mezzo per implementare la resilienza in quanto crea un secondo punto di controllo isolato non collegato all'istanza dell'organizzazione.

Imposta l'accesso di emergenza a AWS Management Console

IAM Identity Center è costruito su un'AWSinfrastruttura ad alta disponibilità e utilizza un'architettura Availability Zone per eliminare i singoli punti di errore. Per un ulteriore livello di protezione nell'improbabile eventualità di un IAM Identity Center o di un'Regione AWSinterruzione, ti consigliamo di configurare una configurazione che possa essere utilizzata per fornire un accesso temporaneo a. AWS Management Console

Indice

Panoramica

AWS consente di:

- Connect il tuo IdP di terze parti a IAM Identity Center.
- Connect il tuo IdP di terze parti a un individuo Account AWS utilizzando la federazione basata su SAML 2.0.

Se utilizzi IAM Identity Center, puoi utilizzare queste funzionalità per creare la configurazione di accesso di emergenza descritta nelle sezioni seguenti. Questa configurazione consente di utilizzare IAM Identity Center come meccanismo di Account AWS accesso. Se IAM Identity Center viene interrotto, gli utenti delle operazioni di emergenza possono accedere alla AWS Management Console federazione diretta, utilizzando le stesse credenziali che utilizzano per accedere ai propri account.

Questa configurazione funziona quando IAM Identity Center non è disponibile, ma sono disponibili il piano dati IAM e il provider di identità esterno (IdP).

> **Important**
>
> Ti consigliamo di implementare questa configurazione prima che si verifichi un'interruzione, perché non puoi creare la configurazione se viene interrotto anche l'accesso per creare i ruoli IAM richiesti. Inoltre, verifica periodicamente questa configurazione per assicurarti che il tuo team capisca cosa fare in caso di interruzione di IAM Identity Center.

Riepilogo della configurazione dell'accesso di emergenza

Per configurare l'accesso di emergenza, è necessario completare le seguenti attività:

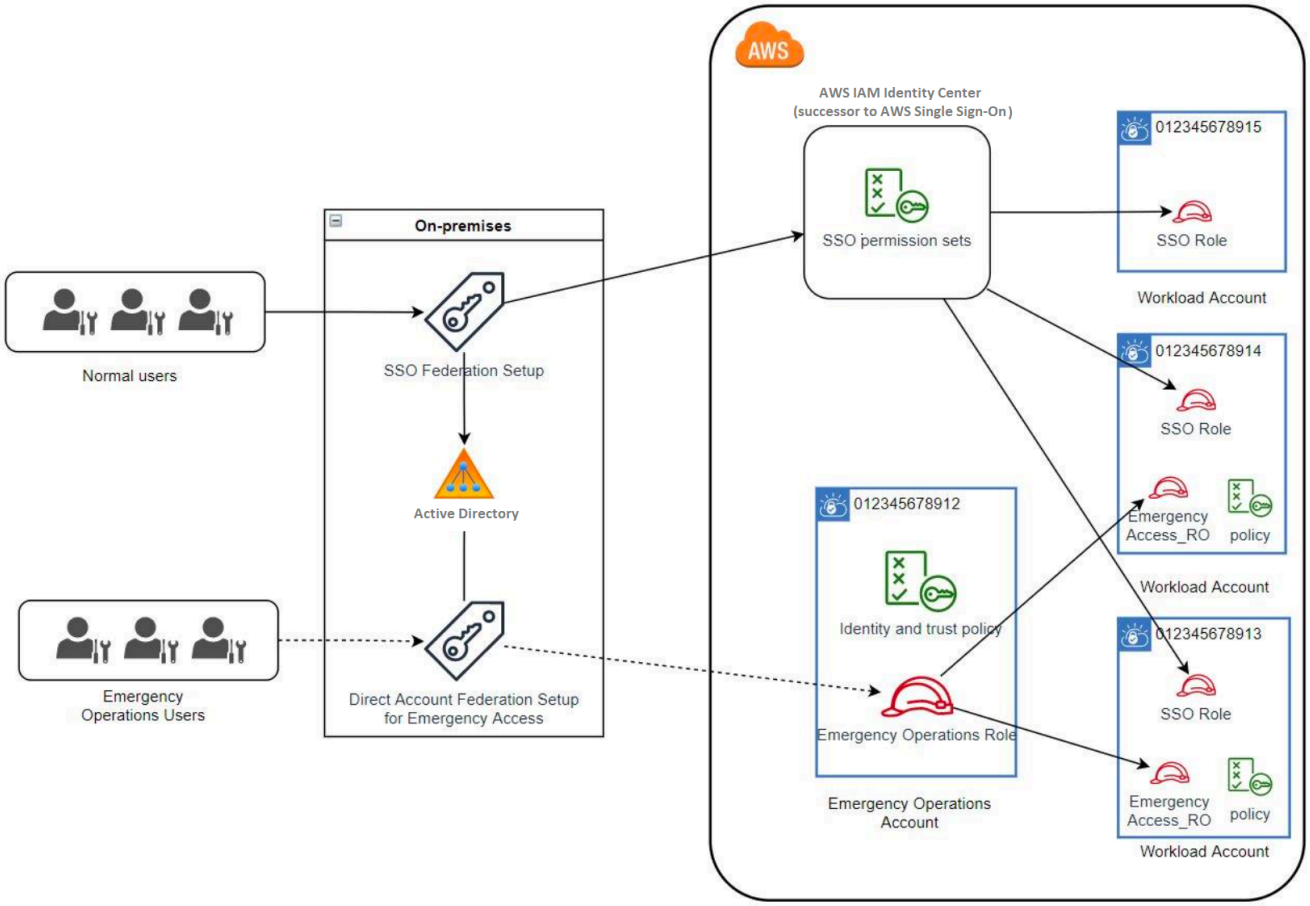
1. Crea un account per le operazioni di emergenza nella tua organizzazione in AWS Organizations.
2. Connect il tuo IdP all'account per le operazioni di emergenza utilizzando la federazione basata su SAML 2.0.
3. Nell'account per le operazioni di emergenza, crea un ruolo per la federazione di provider di identità di terze parti. Inoltre, crea un ruolo per le operazioni di emergenza in ciascuno dei tuoi account di carico di lavoro, con le autorizzazioni richieste.
4. Delega l'accesso ai tuoi account di carico di lavoro per il ruolo IAM che hai creato nell'account per le operazioni di emergenza. Per autorizzare l'accesso al tuo account per le operazioni di emergenza, crea un gruppo operativo di emergenza nel tuo IdP, senza membri.
5. Consenti al gruppo operativo di emergenza del tuo IdP di utilizzare il ruolo delle operazioni di emergenza creando una regola nel tuo IdP che abiliti l'accesso federato SAML 2.0 a. AWS Management Console

Durante le normali operazioni, nessuno ha accesso all'account per le operazioni di emergenza perché il gruppo operativo di emergenza del tuo IdP non ha membri. In caso di interruzione dell'IAM Identity Center, utilizza il tuo IdP per aggiungere utenti affidabili al gruppo operativo di emergenza del tuo IdP. Questi utenti possono quindi accedere al tuo IdP, accedere a e assumere il AWS Management Console ruolo delle operazioni di emergenza nell'account delle operazioni di emergenza. Da lì, questi utenti possono passare al ruolo di accesso di emergenza negli account dei carichi di lavoro in cui devono eseguire operazioni.

Come progettare i ruoli operativi critici

Con questo design, ne configuri uno Account AWS in cui federare tramite IAM, in modo che gli utenti possano assumere ruoli operativi critici. I ruoli operativi critici hanno una politica di fiducia che consente agli utenti di assumere un ruolo corrispondente negli account dei carichi di lavoro. I ruoli negli account del carico di lavoro forniscono le autorizzazioni necessarie agli utenti per eseguire il lavoro essenziale.

Il diagramma seguente fornisce una panoramica della progettazione.



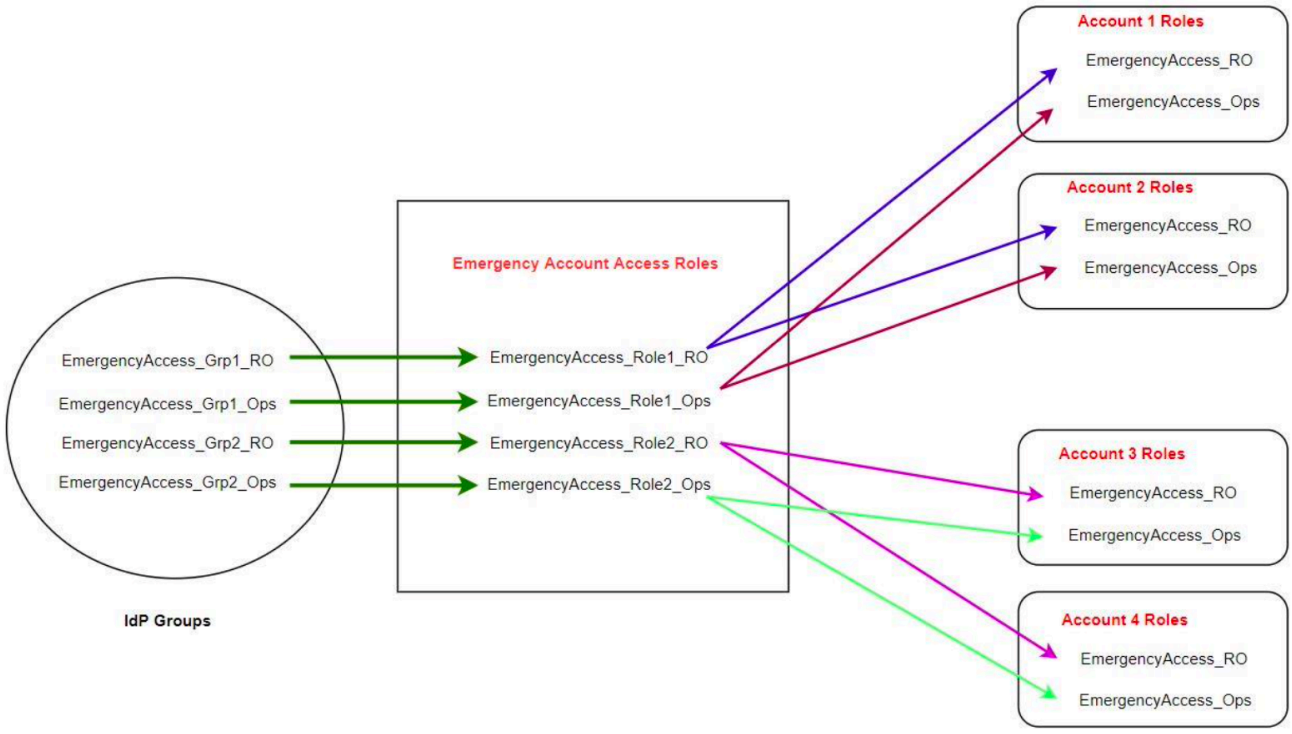
Come pianificare il modello di accesso

Prima di configurare l'accesso di emergenza, crea un piano per il funzionamento del modello di accesso. Utilizza la procedura seguente per creare questo piano.

1. Identifica i Account AWS punti in cui l'accesso di emergenza dell'operatore è essenziale durante un'interruzione di IAM Identity Center. Ad esempio, i tuoi account di produzione sono probabilmente essenziali, ma gli account di sviluppo e test potrebbero non esserlo.
2. Per quella raccolta di account, identifica i ruoli critici specifici di cui hai bisogno nei tuoi account. In tutti questi account, sii coerente nel definire cosa possono fare i ruoli. Ciò semplifica il lavoro nel tuo account con accesso di emergenza in cui crei ruoli tra account. Ti consigliamo di iniziare con due ruoli distinti in questi account: Read Only (RO) e Operations (Ops). Se necessario, puoi creare più ruoli e mappare questi ruoli a un gruppo più distinto di utenti con accesso di emergenza nella tua configurazione.
3. Identifica e crea gruppi di accesso di emergenza nel tuo IdP. I membri del gruppo sono gli utenti a cui deleghi l'accesso ai ruoli di accesso di emergenza.
4. Definisci quali ruoli possono assumere questi gruppi nell'account per l'accesso di emergenza. A tale scopo, definisci delle regole nel tuo IdP che generino attestazioni che elencino i ruoli a cui il gruppo può accedere. Questi gruppi possono quindi assumere i ruoli Read Only o Operations nell'account con accesso di emergenza. Da questi ruoli, possono assumere i ruoli corrispondenti nei tuoi account di carico di lavoro.

Come progettare una mappatura di emergenza di ruoli, account e gruppi

Il diagramma seguente mostra come mappare i gruppi di accesso di emergenza ai ruoli dell'account per l'accesso di emergenza. Il diagramma mostra anche le relazioni di fiducia tra i ruoli tra account che consentono ai ruoli degli account di accesso di emergenza di accedere ai ruoli corrispondenti negli account del carico di lavoro. Consigliamo che la progettazione del piano di emergenza utilizzi queste mappature come punto di partenza.



Come creare la configurazione di accesso di emergenza

Utilizza la seguente tabella di mappatura per creare la configurazione dell'accesso di emergenza. Questa tabella riflette un piano che include due ruoli negli account del carico di lavoro: Read Only (RO) e Operations (Ops), con le corrispondenti politiche di attendibilità e autorizzazioni. Le politiche di attendibilità consentono ai ruoli degli account con accesso di emergenza di accedere ai ruoli dei singoli account di carico di lavoro. I ruoli dei singoli account di carico di lavoro dispongono inoltre di politiche di autorizzazione relative a ciò che il ruolo può fare nell'account. Le politiche di autorizzazione possono essere politiche gestite o politiche AWS gestite dai clienti.

Account	Ruoli da creare	Policy di attendibilità	Policy delle autorizzazioni
Account 1	Emergency Access_RO	Emergency Access_Role1_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
Conto 1	Emergency Access_Ops	Emergency Access_Role1_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator

Account	Ruoli da creare	Policy di attendibilità	Policy delle autorizzazioni
Conto 2	Emergency Access_RO	Emergency Access_Role2_RO	arn:aws:iam: :aws:policy/ ReadOnlyAccess
Conto 2	Emergency Access_Ops	Emergency Access_Role2_Ops	arn:aws:iam::aws:policy/job-function/ SystemAdministrator
Account con accesso di emergenza	Emergency Access_Role1_RO Emergency Access_Role1_Ops Emergency Access_Role2_RO Emergency Access_Role2_Ops	IdP	AssumeRole per la risorsa relativa al ruolo nell'account

In questo piano di mappatura, l'account di accesso di emergenza contiene due ruoli di sola lettura e due ruoli operativi. Questi ruoli si affidano al tuo IdP per autenticare e autorizzare i gruppi selezionati ad accedere ai ruoli passando i nomi dei ruoli nelle asserzioni. Esistono ruoli operativi e di sola lettura corrispondenti nell'Account 1 e nell'Account 2 del carico di lavoro. Per l'Account 1 del carico di lavoro, il `EmergencyAccess_RO` ruolo si affida al `EmergencyAccess_Role1_RO` ruolo che risiede nell'account di accesso di emergenza. La tabella specifica modelli di fiducia simili tra l'account di carico di lavoro in sola lettura e i ruoli operativi e i ruoli di accesso di emergenza corrispondenti.

Attività di preparazione alle emergenze

Per preparare la configurazione dell'accesso di emergenza, si consiglia di eseguire le seguenti attività prima che si verifichi un'emergenza.

1. Configura un'applicazione di federazione IAM diretta nel tuo IdP. Per ulteriori informazioni, consulta Configurazione una tantum di un'applicazione federativa IAM diretta in Okta.

2. Crea una connessione IdP nell'account di accesso di emergenza a cui puoi accedere durante l'evento.
3. Crea ruoli di accesso di emergenza negli account di accesso di emergenza come descritto nella tabella di mappatura precedente.
4. Crea ruoli operativi temporanei con politiche di fiducia e autorizzazione in ciascuno degli account del carico di lavoro.
5. Crea gruppi operativi temporanei nel tuo IdP. I nomi dei gruppi dipenderanno dai nomi dei ruoli operativi temporanei.
6. Prova la federazione IAM diretta.
7. Disattiva l'applicazione di federazione IdP nel tuo IdP per impedirne l'uso regolare.

Processo di failover di emergenza

Quando un'istanza IAM Identity Center non è disponibile e si stabilisce che è necessario fornire l'accesso di emergenza alla console di AWS gestione, consigliamo la seguente procedura di failover.

1. L'amministratore IdP abilita l'applicazione di federazione IAM diretta nel tuo IdP.
2. Gli utenti richiedono l'accesso al gruppo operativo temporaneo tramite il meccanismo esistente, ad esempio una richiesta via e-mail, un canale Slack o un'altra forma di comunicazione.
3. Gli utenti che aggiungi ai tuoi gruppi di accesso di emergenza accedono all'IdP, selezionano l'account di accesso di emergenza e gli utenti scelgono un ruolo da utilizzare nell'account di accesso di emergenza. Da questi ruoli, possono assumere ruoli nei corrispondenti account di carico di lavoro che hanno una fiducia reciproca rispetto al ruolo dell'account di emergenza.

Ritorno alle normali operazioni

Controlla l'AWSHealth Dashboard per confermare quando viene ripristinata l'integrità del servizio IAM Identity Center. Per tornare alle normali operazioni, procedi nel seguente modo.

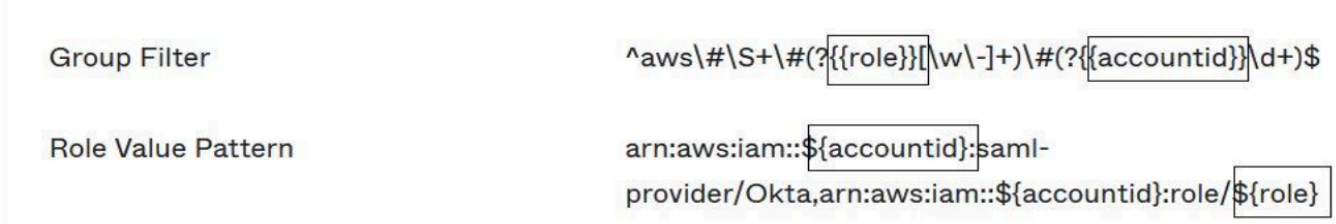
1. Dopo che l'icona di stato del servizio IAM Identity Center indica che il servizio è integro, accedi a IAM Identity Center.
2. Se riesci ad accedere correttamente a IAM Identity Center, comunica agli utenti con accesso di emergenza che IAM Identity Center è disponibile. Chiedi a questi utenti di disconnettersi e di utilizzare il portale di AWS accesso per accedere nuovamente a IAM Identity Center.

3. Dopo che tutti gli utenti con accesso di emergenza si sono disconnessi, nell'IdP, disabilita l'applicazione di federazione IdP. Ti consigliamo di eseguire questa operazione dopo l'orario di lavoro.
4. Rimuovi tutti gli utenti dal gruppo di accesso di emergenza nell'IdP.

L'infrastruttura dei ruoli di accesso di emergenza rimane valida come piano di accesso di backup, ma ora è disabilitata.

Configurazione una tantum di un'applicazione federativa IAM diretta in Okta

1. Accedi al tuo Okta account come utente con autorizzazioni amministrative.
2. In Okta Admin Console, in Applicazioni, scegli Applicazioni.
3. Scegli Sfoglia il catalogo delle app. Cerca e scegli AWSAccount Federation. Quindi scegli Aggiungi integrazione.
4. Configura la federazione IAM diretta AWS seguendo i passaggi in Come configurare SAML 2.0 per la federazione AWS degli account.
5. Nella scheda Opzioni di accesso, seleziona SAML 2.0 e inserisci le impostazioni Group Filter e Role Value Pattern. Il nome del gruppo per la directory utente dipende dal filtro configurato.



   Nella figura precedente, la `role` variabile si riferisce al ruolo delle operazioni di emergenza nell'account per l'accesso di emergenza. Ad esempio, se si crea il `EmergencyAccess_Role1_R0` ruolo (come descritto nella tabella di mappatura) in Account AWS `123456789012` e se l'impostazione del filtro di gruppo è configurata come mostrato nella figura precedente, il nome del gruppo dovrebbe essere`aws#EmergencyAccess_Role1_R0#123456789012`.
6. Nella directory (ad esempio, la directory in Active Directory), create il gruppo per l'accesso di emergenza e specificate un nome per la directory (ad esempio,`aws#EmergencyAccess_Role1_R0#123456789012`). Assegna i tuoi utenti a questo gruppo utilizzando il meccanismo di provisioning esistente.

7. Nell'account di accesso di emergenza, configura una politica di fiducia personalizzata che fornisca le autorizzazioni necessarie per assumere il ruolo di accesso di emergenza durante un'interruzione. Di seguito è riportato un esempio di dichiarazione per una politica di fiducia personalizzata allegata al `EmergencyAccess_Role1_RO` ruolo. Per un'illustrazione, vedi l'account di emergenza nel diagramma seguente. Come progettare una mappatura di emergenza di ruoli, account e gruppi

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
         "Effect":"Allow",
         "Principal":{
            "Federated":"arn:aws:iam::123456789012:saml-provider/Okta"
         },
         "Action":[
            "sts:AssumeRoleWithSAML",
            "sts:SetSourceIdentity",
            "sts:TagSession"
         ],
         "Condition":{
            "StringEquals":{
               "SAML:aud":"https:~/~/signin.aws.amazon.com/saml"
            }
         }
      }
   ]
}
```

8. Di seguito è riportato un esempio di dichiarazione per una politica di autorizzazioni associata al ruolo. `EmergencyAccess_Role1_RO` Per un'illustrazione, vedi l'account di emergenza nel diagramma seguente. Come progettare una mappatura di emergenza di ruoli, account e gruppi

```
{
    "Version": "2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Action":"sts:AssumeRole",
         "Resource":[
            "arn:aws:iam::<account 1>:role/EmergencyAccess_RO",
            "arn:aws:iam::<account 2>:role/EmergencyAccess_RO"
```

```
            ]
        }
    ]
}
```

9. Negli account del carico di lavoro, configura una politica di attendibilità personalizzata. Di seguito è riportato un esempio di dichiarazione per una politica di fiducia allegata al `EmergencyAccess_R0` ruolo. In questo esempio, l'account `123456789012` è l'account di accesso di emergenza. Per un'illustrazione, vedi l'account del carico di lavoro nel diagramma seguente. Come progettare una mappatura di emergenza di ruoli, account e gruppi

```
{
    "Version": "2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:root"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

> **Note**
>
> La maggior parte IdPs consente di mantenere l'integrazione di un'applicazione disattivata fino a quando necessario. Ti consigliamo di mantenere disattivata l'applicazione di federazione IAM diretta nel tuo IdP fino a quando non viene richiesta per l'accesso di emergenza.

Sicurezza in AWS IAM Identity Center

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità applicabili AWS IAM Identity Center, consulta AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando utilizzi IAM Identity Center. I seguenti argomenti mostrano come configurare IAM Identity Center per soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le risorse dell'IAM Identity Center.

Argomenti

Gestione delle identità e degli accessi per IAM Identity Center

L'accesso a IAM Identity Center richiede credenziali che AWS possono essere utilizzate per autenticare le tue richieste. Tali credenziali devono disporre delle autorizzazioni per accedere alle AWS risorse, come un'applicazione gestita. AWS

L'autenticazione al portale di AWS accesso è controllata dalla directory che hai collegato a IAM Identity Center. Tuttavia, l'autorizzazione ai Account AWS dati disponibili per gli utenti dall'interno del portale di AWS accesso è determinata da due fattori:

1. A chi è stato assegnato l'accesso a coloro che Account AWS si trovano nella console IAM Identity Center. Per ulteriori informazioni, consulta Accesso Single Sign-On a Account AWS.
2. Quale livello di autorizzazioni sono state concesse agli utenti nella console IAM Identity Center per consentire loro l'accesso appropriato a tali Account AWS autorizzazioni. Per ulteriori informazioni, consulta Crea, gestisci ed elimina i set di autorizzazioni.

Le seguenti sezioni spiegano come un amministratore può controllare l'accesso alla console IAM Identity Center o delegare l'accesso amministrativo per day-to-day le attività dalla console IAM Identity Center.

- Autenticazione
- Controllo accessi

Autenticazione

Scopri come accedere AWS utilizzando le identità IAM.

Controllo accessi

Puoi disporre di credenziali valide per autenticare le tue richieste, ma a meno che tu non disponga delle autorizzazioni, non puoi creare o accedere alle risorse di IAM Identity Center. Ad esempio, è necessario disporre delle autorizzazioni per creare una directory connessa a IAM Identity Center.

Le seguenti sezioni descrivono come gestire le autorizzazioni per IAM Identity Center. Consigliamo di leggere prima la panoramica.

- Panoramica della gestione delle autorizzazioni di accesso alle risorse dell'IAM Identity Center

- Esempi di policy basate sull'identità per IAM Identity Center
- Utilizzo di ruoli collegati ai servizi per IAM Identity Center

Panoramica della gestione delle autorizzazioni di accesso alle risorse dell'IAM Identity Center

Ogni AWS risorsa è di proprietà di un Account AWS utente e le autorizzazioni per creare o accedere alle risorse sono regolate da politiche di autorizzazione. Per fornire l'accesso, un amministratore dell'account può aggiungere autorizzazioni alle identità IAM (ovvero utenti, gruppi e ruoli). Alcuni servizi (ad esempio AWS Lambda) supportano anche l'aggiunta di autorizzazioni alle risorse.

> **Note**
>
> Un amministratore account (o un utente amministratore) è un utente con privilegi di amministratore. Per ulteriori informazioni, consultare la sezione best practice IAM nella Guida per l'utente IAM.

Argomenti

- Risorse e operazioni di IAM Identity Center
- Informazioni sulla proprietà delle risorse
- Gestione dell'accesso alle risorse
- Specificazione degli elementi della policy: azioni, effetti, risorse e principi
- Specifica delle condizioni in una policy

Risorse e operazioni di IAM Identity Center

In IAM Identity Center, le risorse principali sono le istanze delle applicazioni, i profili e i set di autorizzazioni.

Informazioni sulla proprietà delle risorse

Il proprietario della risorsa è colui Account AWS che ha creato una risorsa. Cioè, il proprietario Account AWS della risorsa è l'entità principale (l'account, un utente o un ruolo IAM) che autentica la richiesta che crea la risorsa. Negli esempi seguenti viene illustrato il funzionamento:

- Se Utente root dell'account AWS crea una risorsa IAM Identity Center, ad esempio un'istanza dell'applicazione o un set di autorizzazioni, sei Account AWS il proprietario di quella risorsa.
- Se crei un utente nel tuo AWS account e concedi a quell'utente le autorizzazioni per creare risorse IAM Identity Center, l'utente può quindi creare risorse IAM Identity Center. Tuttavia, il tuo AWS account, a cui appartiene l'utente, possiede le risorse.
- Se crei un ruolo IAM nel tuo AWS account con le autorizzazioni per creare risorse IAM Identity Center, chiunque possa assumere il ruolo può creare risorse IAM Identity Center. Il tuo Account AWS, a cui appartiene il ruolo, possiede le risorse dell'IAM Identity Center.

Gestione dell'accesso alle risorse

La policy delle autorizzazioni descrive chi ha accesso a cosa. Nella sezione seguente vengono descritte le opzioni disponibili per la creazione di policy relative alle autorizzazioni.

> **Note**
>
> Questa sezione illustra l'utilizzo di IAM nel contesto di IAM Identity Center. Non vengono fornite informazioni dettagliate sul servizio IAM. Per la documentazione di IAM completa, consulta la pagina Che cos'è IAM? nella Guida per l'utente di IAM. Per informazioni sulla sintassi delle policy IAM e le rispettive descrizioni, consultare Riferimento alle policy IAM di AWS nella Guida per l'utente di IAM.

Le policy collegate a un'identità IAM sono denominate policy basate su identità (policy IAM). Le policy collegate a una risorsa sono denominate policy basate sulle risorse. IAM Identity Center supporta solo politiche basate sull'identità (politiche IAM).

Argomenti

- Policy basate su identità (policy IAM)
- Policy basate su risorse

Policy basate su identità (policy IAM)

Puoi aggiungere autorizzazioni alle identità IAM. Ad esempio, puoi eseguire le operazioni seguenti:

- Allega una politica di autorizzazioni a un utente o a un gruppo del tuo Account AWS: un amministratore dell'account può utilizzare una politica di autorizzazioni associata a un particolare

utente per concedere a quell'utente le autorizzazioni per aggiungere una risorsa IAM Identity Center, come una nuova applicazione.

- Collega una policy di autorizzazione a un ruolo (assegnazione di autorizzazioni tra account): per concedere autorizzazioni tra più account, è possibile collegare una policy di autorizzazione basata su identità a un ruolo IAM.

  Per ulteriori informazioni sull'uso di IAM per delegare le autorizzazioni, consultare Gestione degli accessi nella Guida per l'utente di IAM.

La seguente policy di autorizzazione concede a un utente le autorizzazioni per eseguire tutte le operazioni che iniziano con `List`. Queste azioni mostrano informazioni su una risorsa IAM Identity Center, come un'istanza dell'applicazione o un set di autorizzazioni. Nota che il carattere jolly (*) nell'`Resource`elemento indica che le azioni sono consentite per tutte le risorse IAM Identity Center di proprietà dell'account.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"sso:List*",
         "Resource":"*"
      }
   ]
}
```

Per ulteriori informazioni sull'utilizzo di policy basate sull'identità con IAM Identity Center, consulta. Esempi di policy basate sull'identità per IAM Identity Center Per ulteriori informazioni su utenti, gruppi, ruoli e autorizzazioni, consultare Identità (utenti, gruppi e ruoli) nella Guida per l'utente di IAM.

Policy basate su risorse

Anche altri servizi, ad esempio Amazon S3, supportano policy di autorizzazioni basate su risorse. Ad esempio, è possibile associare una policy a un bucket S3 per gestire le autorizzazioni di accesso a quel bucket. IAM Identity Center non supporta policy basate sulle risorse.

Specificazione degli elementi della policy: azioni, effetti, risorse e principi

Per ogni risorsa IAM Identity Center (vediRisorse e operazioni di IAM Identity Center), il servizio definisce un set di operazioni API. Per concedere le autorizzazioni per queste operazioni API, IAM

Identity Center definisce una serie di azioni che è possibile specificare in una policy. Si noti che l'esecuzione di un'operazione API può richiedere le autorizzazioni per più di un'azione.

Di seguito sono elencati gli elementi di base di una policy:

- Risorsa: in una policy si utilizza il nome della risorsa Amazon (ARN) per identificare la risorsa a cui si applica la policy stessa.
- Operazione: utilizzi le parole chiave per identificare le operazioni sulla risorsa da permettere o rifiutare. Ad esempio, l'`sso:DescribePermissionsPolicies`autorizzazione consente all'utente di eseguire l'operazione IAM Identity Center`DescribePermissionsPolicies`.
- Effetto: l'effetto prodotto quando l'utente richiede l'operazione specifica, ovvero un'autorizzazione o un rifiuto. USe non concedi esplicitamente (consenti) l'accesso a una risorsa, l'accesso viene implicitamente rifiutato. Puoi anche rifiutare esplicitamente l'accesso a una risorsa per garantire che un utente non possa accedervi, anche se l'accesso viene concesso da un'altra policy.
- Principale - Nelle policy basate su identità (policy IAM), l'utente a cui la policy è collegata è il principale implicito. Per policy basate su risorse, specifichi l'utente, l'account, il servizio o un'altra entità che desideri riceva le autorizzazioni (si applica solo alle policy basate su risorse). IAM Identity Center non supporta policy basate sulle risorse.

Per ulteriori informazioni sulla sintassi e le descrizioni delle policy IAM, consultare AWS Riferimento alle policy IAM nella Guida per l'utente di IAM.

Specifica delle condizioni in una policy

Quando concedi le autorizzazioni, puoi utilizzare la sintassi della/e policy di accesso per specificare le condizioni necessarie per l'applicazione di una policy. Ad esempio, potresti decidere che una policy venga applicata solo dopo una data specifica. Per ulteriori informazioni su come specificare le condizioni in un linguaggio di policy, consulta la sezione Condizione nella Guida per l'utente di IAM.

Per esprimere le condizioni è necessario utilizzare chiavi di condizione predefinite. Non esistono chiavi di condizione specifiche per IAM Identity Center. Tuttavia, esistono chiavi di AWS condizione che è possibile utilizzare in modo appropriato. Per un elenco completo delle AWS chiavi, consulta Available global condition keys nella IAM User Guide.

Esempi di policy basate sull'identità per IAM Identity Center

Questo argomento fornisce esempi di policy IAM che puoi creare per concedere a utenti e ruoli le autorizzazioni per amministrare IAM Identity Center.

> **Important**
>
> Ti consigliamo di esaminare innanzitutto gli argomenti introduttivi che spiegano i concetti e le opzioni di base disponibili per gestire l'accesso alle risorse dell'IAM Identity Center. Per ulteriori informazioni, consulta la pagina Panoramica della gestione delle autorizzazioni di accesso alle risorse dell'IAM Identity Center.

In questa sezione vengono trattati gli argomenti seguenti:

- Esempi di policy personalizzate
- Autorizzazioni necessarie per utilizzare la console IAM Identity Center

Esempi di policy personalizzate

Questa sezione fornisce esempi di casi d'uso comuni che richiedono una policy IAM personalizzata. Queste politiche di esempio sono politiche basate sull'identità, che non specificano l'elemento Principal. Questo perché con una politica basata sull'identità non si specifica il principale che ottiene l'autorizzazione. Invece, alleghi la politica al principale. Quando colleghi una politica di autorizzazione basata sull'identità a un ruolo IAM, il principale identificato nella politica di fiducia del ruolo ottiene le autorizzazioni. Puoi creare policy basate sull'identità in IAM e collegarle a utenti, gruppi e/o ruoli. Puoi anche applicare queste policy agli utenti di IAM Identity Center quando crei un set di autorizzazioni in IAM Identity Center.

> **Note**
>
> Usa questi esempi per creare policy per il tuo ambiente e assicurati di testare sia i casi di test positivi («accesso concesso») che quelli negativi («accesso negato») prima di implementare queste politiche nell'ambiente di produzione. Per ulteriori informazioni sul test delle policy IAM, consulta Testare le policy IAM con il simulatore di policy IAM nella IAM User Guide.

Argomenti

- Esempio 1: consenti a un utente di visualizzare IAM Identity Center
- Esempio 2: consenti a un utente di gestire le autorizzazioni di Account AWS IAM Identity Center
- Esempio 3: consentire a un utente di gestire le applicazioni in IAM Identity Center
- Esempio 4: consentire a un utente di gestire utenti e gruppi nella directory dell'Identity Center

Esempio 1: consenti a un utente di visualizzare IAM Identity Center

La seguente politica di autorizzazione concede autorizzazioni di sola lettura a un utente in modo che possa visualizzare tutte le impostazioni e le informazioni sulla directory configurate in IAM Identity Center.

> **Note**
>
> Questa policy viene fornita solo a scopo esemplificativo. In un ambiente di produzione, ti consigliamo di utilizzare la policy `ViewOnlyAccess` AWS gestita per IAM Identity Center.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ds:DescribeDirectories",
                "ds:DescribeTrusts",
                "iam:ListPolicies",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:ListAccountsForParent",
                "organizations:ListOrganizationalUnitsForParent",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListPermissionSets",
                "sso:DescribePermissionSet",
                "sso:GetInlinePolicyForPermissionSet",
                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Esempio 2: consenti a un utente di gestire le autorizzazioni di Account AWS IAM Identity Center

La seguente politica di autorizzazioni concede le autorizzazioni per consentire a un utente di creare, gestire e distribuire set di autorizzazioni per: Account AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AttachManagedPolicyToPermissionSet",
                "sso:CreateAccountAssignment",
                "sso:CreatePermissionSet",
                "sso:DeleteAccountAssignment",
                "sso:DeleteInlinePolicyFromPermissionSet",
                "sso:DeletePermissionSet",
                "sso:DetachManagedPolicyFromPermissionSet",
                "sso:ProvisionPermissionSet",
                "sso:PutInlinePolicyToPermissionSet",
                "sso:UpdatePermissionSet"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMListPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:ListPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AccessToSSOProvisionedRoles",
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
```

```
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetSAMLProvider"
            ],
            "Resource": "arn:aws:iam::*:saml-provider/AWSSSO_*_DO_NOT_DELETE"
        }
    ]
}
```

> **Note**
>
> Le autorizzazioni aggiuntive elencate `"Sid": "AccessToSSOProvisiondRoles"` nelle sezioni e sono necessarie solo per consentire all'utente di creare assegnazioni nell'account di gestione. `"Sid": "IAMListPermissions"` AWS Organizations In alcuni casi, potrebbe essere necessario aggiungere anche `iam:UpdateSAMLProvider` a queste sezioni.

Esempio 3: consentire a un utente di gestire le applicazioni in IAM Identity Center

La seguente politica di autorizzazioni concede le autorizzazioni per consentire a un utente di visualizzare e configurare le applicazioni in IAM Identity Center, incluse le applicazioni SaaS preintegrate dal catalogo IAM Identity Center.

> **Note**
>
> L'`sso:AssociateProfile`operazione utilizzata nel seguente esempio di policy è necessaria per la gestione delle assegnazioni di utenti e gruppi alle applicazioni. Consente inoltre a un utente di assegnare utenti e gruppi Account AWS utilizzando i set

di autorizzazioni esistenti. Se un utente deve gestire l' Account AWS accesso all'interno di IAM Identity Center e richiede le autorizzazioni necessarie per gestire i set di autorizzazioni, consulta. Esempio 2: consenti a un utente di gestire le autorizzazioni di Account AWS IAM Identity Center

A ottobre 2020, molte di queste operazioni sono disponibili solo tramite la AWS console. Questo criterio di esempio include azioni di «lettura» come list, get e search, che in questo caso sono rilevanti per il funzionamento senza errori della console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:ImportApplicationInstanceServiceProviderMetadata",
                "sso:DeleteApplicationInstance",
                "sso:DeleteProfile",
                "sso:DisassociateProfile",
                "sso:GetApplicationTemplate",
                "sso:UpdateApplicationInstanceServiceProviderConfiguration",
                "sso:UpdateApplicationInstanceDisplayData",
                "sso:DeleteManagedApplicationInstance",
                "sso:UpdateApplicationInstanceStatus",
                "sso:GetManagedApplicationInstance",
                "sso:UpdateManagedApplicationInstanceStatus",
                "sso:CreateManagedApplicationInstance",
                "sso:UpdateApplicationInstanceSecurityConfiguration",
                "sso:UpdateApplicationInstanceResponseConfiguration",
                "sso:GetApplicationInstance",
                "sso:CreateApplicationInstanceCertificate",
                "sso:UpdateApplicationInstanceResponseSchemaConfiguration",
                "sso:UpdateApplicationInstanceActiveCertificate",
                "sso:DeleteApplicationInstanceCertificate",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationTemplates",
                "sso:ListApplications",
                "sso:ListApplicationInstances",
                "sso:ListDirectoryAssociations",
```

```
                "sso:ListProfiles",
                "sso:ListProfileAssociations",
                "sso:ListInstances",
                "sso:GetProfile",
                "sso:GetSSOStatus",
                "sso:GetSsoConfiguration",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeUsers",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Esempio 4: consentire a un utente di gestire utenti e gruppi nella directory dell'Identity Center

La seguente politica di autorizzazione concede le autorizzazioni per consentire a un utente di creare, visualizzare, modificare ed eliminare utenti e gruppi in IAM Identity Center.

In alcuni casi, le modifiche dirette a utenti e gruppi in IAM Identity Center sono limitate. Ad esempio, quando Active Directory o un provider di identità esterno con il provisioning automatico abilitato viene selezionato come origine dell'identità.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso-directory:ListGroupsForUser",
                "sso-directory:DisableUser",
                "sso-directory:EnableUser",
                "sso-directory:SearchGroups",
                "sso-directory:DeleteGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:DescribeDirectory",
                "sso-directory:UpdateUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
```

```
                "sso-directory:SearchUsers",
                "sso:ListDirectoryAssociations",
                "sso-directory:RemoveMemberFromGroup",
                "sso-directory:DeleteUser",
                "sso-directory:DescribeUsers",
                "sso-directory:UpdateGroup",
                "sso-directory:CreateGroup"
            ],
            "Resource": "*"
        }
    ]
}
```

Autorizzazioni necessarie per utilizzare la console IAM Identity Center

Affinché un utente possa lavorare con la console IAM Identity Center senza errori, sono necessarie autorizzazioni aggiuntive. Se è stata creata una policy IAM più restrittiva delle autorizzazioni minime richieste, la console non funzionerà come previsto per gli utenti con quella policy. L'esempio seguente elenca il set di autorizzazioni che potrebbero essere necessarie per garantire un funzionamento senza errori all'interno della console IAM Identity Center.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:DescribeAccountAssignmentCreationStatus",
                "sso:DescribeAccountAssignmentDeletionStatus",
                "sso:DescribePermissionSet",
                "sso:DescribePermissionSetProvisioningStatus",
                "sso:DescribePermissionsPolicies",
                "sso:DescribeRegisteredRegions",
                "sso:GetApplicationInstance",
                "sso:GetApplicationTemplate",
                "sso:GetInlinePolicyForPermissionSet",
                "sso:GetManagedApplicationInstance",
                "sso:GetMfaDeviceManagementForDirectory",
                "sso:GetPermissionSet",
                "sso:GetPermissionsPolicy",
                "sso:GetProfile",
                "sso:GetSharedSsoConfiguration",
                "sso:GetSsoConfiguration",
```

```
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:ListAccountAssignmentCreationStatus",
                "sso:ListAccountAssignmentDeletionStatus",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationInstances",
                "sso:ListApplications",
                "sso:ListApplicationTemplates",
                "sso:ListDirectoryAssociations",
                "sso:ListInstances",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetProvisioningStatus",
                "sso:ListPermissionSets",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListProfileAssociations",
                "sso:ListProfiles",
                "sso:ListTagsForResource",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeUsers",
                "sso-directory:ListGroupsForUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politiche gestite per IAM Identity Center

Creare policy gestite dai clienti IAM che forniscano al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo ed esperienza. Per iniziare rapidamente, puoi utilizzare le policy AWS gestite. Queste policy coprono i casi d'uso comuni e sono disponibili nel tuo Account AWS. Per ulteriori informazioni sulle policy gestite da AWS , consulta Policy gestite da AWS nella Guida per l'utente di IAM.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS per supportare nuove funzionalità. Questo tipo di aggiornamento

interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una policy gestita da AWS quando viene avviata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy ReadOnlyAccess AWS gestita fornisce l'accesso in sola lettura a tutti i AWS servizi e le risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consulta la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

Nel nuovo spazio dei nomi sono disponibili nuove azioni che consentono di elencare ed eliminare le sessioni utente. `identitystore-auth` Eventuali autorizzazioni aggiuntive per le azioni in questo namespace verranno aggiornate in questa pagina. Quando crei le tue policy IAM personalizzate, evita di usare * after `identitystore-auth` perché questo vale per tutte le azioni che esistono nel namespace oggi o in futuro.

AWS politica gestita: AWSSSOMasterAccountAdministrator

La `AWSSSOMasterAccountAdministrator` politica prevede le azioni amministrative necessarie ai committenti. La politica è destinata ai dirigenti che svolgono il ruolo di amministratore AWS IAM Identity Center . Nel tempo, l'elenco delle azioni fornite verrà aggiornato in base alle funzionalità esistenti di IAM Identity Center e alle azioni richieste come amministratore.

È possibile allegare la policy `AWSSSOMasterAccountAdministrator`alle identità IAM. Quando colleghi la `AWSSSOMasterAccountAdministrator` policy a un'identità, concedi AWS IAM Identity Center autorizzazioni amministrative. I responsabili con questa policy possono accedere a IAM Identity Center all'interno dell'account di AWS Organizations gestione e di tutti gli account dei membri. Questo responsabile può gestire completamente tutte le operazioni di IAM Identity Center, inclusa la possibilità di creare un'istanza IAM Identity Center, utenti, set di autorizzazioni e assegnazioni. Il responsabile può anche creare istanze di tali assegnazioni tra gli account dei membri dell' AWS organizzazione e stabilire connessioni tra le directory AWS Directory Service gestite e IAM Identity Center. Man mano che verranno rilasciate nuove funzionalità amministrative, all'amministratore dell'account verranno concesse automaticamente queste autorizzazioni.

Raggruppamenti di autorizzazioni

Questa policy è raggruppata in istruzioni in base al set di autorizzazioni fornite.

- `AWSSSOMasterAccountAdministrator`— Consente a IAM Identity Center di passare il ruolo di servizio denominato `AWSServiceRoleforSSO` a IAM Identity Center in modo che possa successivamente assumere il ruolo ed eseguire azioni per loro conto. Ciò è necessario quando la persona o l'applicazione tenta di abilitare IAM Identity Center. Per ulteriori informazioni, consulta Gestisci l'accesso a Account AWS.
- `AWSSSOMemberAccountAdministrator`— Consente a IAM Identity Center di eseguire azioni di amministratore dell'account in un AWS ambiente con più account. Per ulteriori informazioni, consulta AWS politica gestita: AWSSSOMemberAccountAdministrator.
- `AWSSSOManageDelegatedAdministrator`— Consente a IAM Identity Center di registrare e annullare la registrazione di un amministratore delegato dell'organizzazione.

Per visualizzare le autorizzazioni per questa policy, consulta Managed Policy Reference AWSSSOMasterAccountAdministrator.AWS

Informazioni aggiuntive su questa politica

Quando IAM Identity Center viene abilitato per la prima volta, il servizio IAM Identity Center crea un ruolo collegato al servizio nell'account di AWS Organizations gestione (precedentemente account principale) in modo che IAM Identity Center possa gestire le risorse del tuo account. Le azioni richieste sono `iam:CreateServiceLinkedRole` `eiam:PassRole`, mostrate nei seguenti frammenti.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "AWSSSOCreateSLR",
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName": "sso.amazonaws.com"
            }
         }
      },
      {
         "Sid":"AWSSSOMasterAccountAdministrator",
         "Effect":"Allow",
```

```
         "Action":"iam:PassRole",
         "Resource":"arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition":{
             "StringLike":{
               "iam:PassedToService":"sso.amazonaws.com"
             }
         }
      },
   ]
}
```

AWS politica gestita: AWSSSOMemberAccountAdministrator

La `AWSSSOMemberAccountAdministrator` politica prevede le azioni amministrative necessarie ai committenti. La policy è destinata ai responsabili che svolgono il ruolo di amministratore di IAM Identity Center. Nel tempo, l'elenco delle azioni fornite verrà aggiornato in base alle funzionalità esistenti di IAM Identity Center e alle azioni richieste come amministratore.

È possibile allegare la policy `AWSSSOMemberAccountAdministrator`alle identità IAM. Quando colleghi la `AWSSSOMemberAccountAdministrator` policy a un'identità, concedi AWS IAM Identity Center autorizzazioni amministrative. I responsabili con questa policy possono accedere a IAM Identity Center all'interno dell'account di AWS Organizations gestione e di tutti gli account dei membri. Questo responsabile può gestire completamente tutte le operazioni di IAM Identity Center, inclusa la possibilità di creare utenti, set di autorizzazioni e assegnazioni. Il responsabile può anche creare istanze di tali assegnazioni tra gli account dei membri dell' AWS organizzazione e stabilire connessioni tra le directory AWS Directory Service gestite e IAM Identity Center. Man mano che vengono rilasciate nuove funzionalità amministrative, all'amministratore dell'account vengono concesse automaticamente queste autorizzazioni.

Per visualizzare le autorizzazioni relative a questa politica, consulta AWS Managed Policy AWSSSOMemberAccountAdministratorReference.

Informazioni aggiuntive su questa politica

Gli amministratori di IAM Identity Center gestiscono utenti, gruppi e password nel loro archivio di directory di Identity Center (sso-directory). Il ruolo di amministratore dell'account include le autorizzazioni per le seguenti azioni:

- `"sso:*"`
- `"sso-directory:*"`

Gli amministratori di IAM Identity Center necessitano di autorizzazioni limitate per le seguenti AWS Directory Service azioni per eseguire le attività quotidiane.

- `"ds:DescribeTrusts"`
- `"ds:UnauthorizeApplication"`
- `"ds:DescribeDirectories"`
- `"ds:AuthorizeApplication"`
- `“ds:CreateAlias”`

Queste autorizzazioni consentono agli amministratori di IAM Identity Center di identificare le directory esistenti e gestire le applicazioni in modo che possano essere configurate per l'uso con IAM Identity Center. Per ulteriori informazioni su ciascuna di queste azioni, consulta Autorizzazioni AWS Directory Service API: riferimento alle azioni, alle risorse e alle condizioni.

IAM Identity Center utilizza le policy IAM per concedere le autorizzazioni agli utenti di IAM Identity Center. Gli amministratori di IAM Identity Center creano set di autorizzazioni e vi allegano delle policy. L'amministratore di IAM Identity Center deve disporre delle autorizzazioni per elencare le policy esistenti in modo da poter scegliere quali policy utilizzare con il set di autorizzazioni che sta creando o aggiornando. Per impostare autorizzazioni sicure e funzionali, l'amministratore di IAM Identity Center deve disporre delle autorizzazioni per eseguire la convalida delle policy di IAM Access Analyzer.

- `"iam:ListPolicies"`
- `"access-analyzer:ValidatePolicy"`

Gli amministratori di IAM Identity Center necessitano di un accesso limitato alle seguenti AWS Organizations azioni per eseguire le attività quotidiane:

- `"organizations:EnableAWSServiceAccess"`
- `"organizations:ListRoots"`
- `"organizations:ListAccounts"`
- `"organizations:ListOrganizationalUnitsForParent"`
- `"organizations:ListAccountsForParent"`
- `"organizations:DescribeOrganization"`
- `"organizations:ListChildren"`

- `"organizations:DescribeAccount"`
- `"organizations:ListParents"`
- `"organizations:ListDelegatedAdministrators"`
- `"organizations:RegisterDelegatedAdministrator"`
- `"organizations:DeregisterDelegatedAdministrator"`

Queste autorizzazioni consentono agli amministratori di IAM Identity Center di lavorare con le risorse dell'organizzazione (account) per attività amministrative di base di IAM Identity Center come le seguenti:

- Identificazione dell'account di gestione che appartiene all'organizzazione
- Identificazione degli account dei membri che appartengono all'organizzazione
- Abilitazione dell'accesso al AWS servizio per gli account
- Configurazione e gestione di un amministratore delegato

Per ulteriori informazioni sull'utilizzo di un amministratore delegato con IAM Identity Center, consulta. Amministrazione delegata Per ulteriori informazioni su come vengono utilizzate queste autorizzazioni AWS Organizations, consulta Utilizzo AWS Organizations con altri AWS servizi.

AWS politica gestita: AWSSSODirectoryAdministrator

È possibile allegare la policy `AWSSSODirectoryAdministrator`alle identità IAM.

Questa policy concede autorizzazioni amministrative per gli utenti e i gruppi di IAM Identity Center. I responsabili a cui è allegata questa policy possono apportare qualsiasi aggiornamento agli utenti e ai gruppi di IAM Identity Center.

Per visualizzare le autorizzazioni per questa policy, consulta AWS Managed Policy AWSSSODirectoryAdministratorReference.

AWS politica gestita: AWSSSOReadOnly

È possibile allegare la policy `AWSSSOReadOnly`alle identità IAM.

Questa policy concede autorizzazioni di sola lettura che consentono agli utenti di visualizzare le informazioni in IAM Identity Center. I responsabili a cui è associata questa policy non possono visualizzare direttamente gli utenti o i gruppi di IAM Identity Center. I responsabili a cui è associata

questa policy non possono effettuare aggiornamenti in IAM Identity Center. Ad esempio, i responsabili con queste autorizzazioni possono visualizzare le impostazioni di IAM Identity Center, ma non possono modificare nessuno dei valori delle impostazioni.

Per visualizzare le autorizzazioni per questa policy, consulta AWS Managed Policy AWSSSOReadOnlyReference.

AWS politica gestita: AWSSSODirectoryReadOnly

È possibile allegare la policy `AWSSSODirectoryReadOnly`alle identità IAM.

Questa policy concede autorizzazioni di sola lettura che consentono agli utenti di visualizzare utenti e gruppi in IAM Identity Center. I responsabili a cui è associata questa policy non possono visualizzare le assegnazioni, i set di autorizzazioni, le applicazioni o le impostazioni di IAM Identity Center. I responsabili a cui è allegata questa policy non possono effettuare aggiornamenti in IAM Identity Center. Ad esempio, i responsabili con queste autorizzazioni possono visualizzare gli utenti di IAM Identity Center, ma non possono modificare alcun attributo utente o assegnare dispositivi MFA.

Per visualizzare le autorizzazioni per questa policy, consulta AWSSSODirectoryReadOnlyManaged Policy Reference.AWS

AWS politica gestita: AWSIdentitySyncFullAccess

È possibile allegare la policy `AWSIdentitySyncFullAccess`alle identità IAM.

I principali a cui è allegato questo criterio dispongono delle autorizzazioni di accesso complete per creare ed eliminare profili di sincronizzazione, associare o aggiornare un profilo di sincronizzazione con una destinazione di sincronizzazione, creare, elencare ed eliminare filtri di sincronizzazione e avviare o interrompere la sincronizzazione.

Dettagli delle autorizzazioni

Per visualizzare le autorizzazioni relative a questa policy, consulta AWSIdentitySyncFullAccess AWSManaged Policy Reference.

AWS politica gestita: AWSIdentitySyncReadOnlyAccess

È possibile allegare la policy `AWSIdentitySyncReadOnlyAccess`alle identità IAM.

Questa politica concede autorizzazioni di sola lettura che consentono agli utenti di visualizzare informazioni sul profilo di sincronizzazione delle identità, sui filtri e sulle impostazioni di destinazione. I responsabili a cui è allegato questo criterio non possono apportare aggiornamenti alle impostazioni

di sincronizzazione. Ad esempio, i responsabili con queste autorizzazioni possono visualizzare le impostazioni di sincronizzazione delle identità, ma non possono modificare alcun valore del profilo o del filtro.

Per visualizzare le autorizzazioni per questa politica, consulta Managed Policy Reference AWSIdentitySyncReadOnlyAccess.AWS

AWS politica gestita: AWSSSOServiceRolePolicy

Non puoi collegare la `AWSSSOServiceRolePolicy` policy alle tue identità IAM.

Questa policy è associata a un ruolo collegato al servizio che consente a IAM Identity Center di delegare e stabilire quali utenti hanno accesso Single Sign-On a specifici in. Account AWS AWS Organizations Quando abiliti IAM, viene creato un ruolo collegato ai servizi in tutta l'organizzazione. Account AWS IAM Identity Center crea inoltre lo stesso ruolo collegato ai servizi in ogni account che viene successivamente aggiunto all'organizzazione. Questo ruolo consente a IAM Identity Center di accedere alle risorse di ciascun account per tuo conto. I ruoli collegati ai servizi che vengono creati in ciascuno di essi Account AWS sono denominati. `AWSServiceRoleForSSO` Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per IAM Identity Center.

AWS politica gestita: AWSIAMIdentityCenterAllowListForIdentityContext

Quando si assume un ruolo nel contesto di identità di IAM Identity Center, AWS Security Token Service (AWS STS) associa automaticamente la `AWSIAMIdentityCenterAllowListForIdentityContext` policy al ruolo.

Questa policy fornisce l'elenco delle azioni consentite quando si utilizza la propagazione affidabile delle identità con ruoli assunti con il contesto di identità IAM Identity Center. Tutte le altre azioni richiamate in questo contesto sono bloccate. Il contesto di identità viene passato come`ProvidedContext`.

Per visualizzare le autorizzazioni per questa politica, vedere AWSIAMIdentityCenterAllowListForIdentityContextin AWS Managed Policy Reference.

Aggiornamenti di IAM Identity Center alle policy AWS gestite

La tabella seguente descrive gli aggiornamenti alle policy AWS gestite per IAM Identity Center da quando questo servizio ha iniziato a tracciare queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei documenti di IAM Identity Center.

Modifica	Descrizione	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Questa policy ora includeelasticmapreduce:AddJobFlowSteps , elasticmapreduce:DescribeCluster elasticmapreduce:CancelSteps elasticmapreduce:DescribeStep , eelasticmapreduce:ListSteps azioni per supportare la propagazione affidabile delle identità in Amazon EMR.	17 maggio 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Questa politica ora includeqapps:CreateQApp ,,,qapps:PredictProblemStatementFromConversation ,qapps:PredictQAppFromProblemStatement ,qapps:CopyQApp ,,qapps:GetQApp ,qapps:ListQApps ,qapps:UpdateQApp ,qapps:DeleteQApp ,qapps:AssociateQAppWithUser ,qapps:DisassociateQAppFromUser ,qapps:ImportDocumentToQApp ,,qapps:Imp	30 aprile 2024

Modifica	Descrizione	Data
	`ortDocumentToQAppSession` ,`qapps:CreateLibraryItem` , `qapps:GetLibraryItem` `qapps:UpdateLibraryItem` `qapps:CreateLibraryItemReview` `qapps:ListLibraryItems` `qapps:CreateSubscriptionToken` `qapps:StartQAppSession` , e `qapps:StopQAppSession` azioni per supportare le sessioni di console con riconoscimento dell'identità per le applicazioni AWS gestite che supportano queste sessioni.	
AWSSSOMasterAccountAdministrator	Questa politica ora include `signin:ListTrustedIdentityPropagationApplicationsForConsole` le azioni `signin:CreateTrustedIdentityPropagationApplicationForConsole` e le azioni per supportare le sessioni di console con riconoscimento dell'identità per le applicazioni AWS gestite che supportano queste sessioni.	26 aprile 2024

Modifica	Descrizione	Data
AWSSSOMemberAccountAdministrator	Questa politica ora include `signin:ListTrustedIdentityPropagationApplicationsForConsole` le azioni `signin:CreateTrustedIdentityPropagationApplicationForConsole` e le azioni per supportare le sessioni di console con riconoscimento dell'identità per le applicazioni AWS gestite che supportano queste sessioni.	26 aprile 2024
AWSSSOReadOnly	Questa politica ora include l'`signin:ListTrustedIdentityPropagationApplicationsForConsole` azione per supportare sessioni di console con riconoscimento dell'identità per le applicazioni AWS gestite che supportano queste sessioni.	26 aprile 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Questa politica ora include l'`qbusiness:PutFeedback` azione per supportare sessioni di console con riconoscimento dell'identità per le applicazioni AWS gestite che supportano queste sessioni.	26 aprile 2024

Modifica	Descrizione	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Questa politica ora includeq:StartConversation ,,,, q:SendMessage q:ListConversations q:GetConversation q:StartTroubleshootingAnalysis q:GetTroubleshootingResults q:StartTroubleshootingResolutionExplanation ,e q:UpdateTroubleshootingCommandResult le azioni per supportare le sessioni di console con riconoscimento dell'identità per le applicazioni AWS gestite che supportano queste sessioni.	24 aprile 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Questa politica ora include l'sts:SetContext azione per supportare sessioni di console con riconoscimento dell'identità per le applicazioni AWS gestite che supportano queste sessioni.	19 aprile 2024

Modifica	Descrizione	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Questa politica ora includeqbusiness:Chat , qbusiness:ChatSync qbusiness:ListConversations qbusiness:ListMessages , e qbusiness:DeleteConversation le azioni per supportare le sessioni di console con riconoscimento dell'identità per le applicazioni AWS gestite che supportano queste sessioni.	11 aprile 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Questa politica ora include le s3:GetDataAccess azioni s3:GetAccessGrantsInstanceForPrefix e.	26 novembre 2023
AWSIAMIdentityCenterAllowListForIdentityContext	Questa policy fornisce l'elenco delle azioni consentite quando si utilizza la propagazione affidabile delle identità con ruoli assunti con il contesto di identità IAM Identity Center.	15 novembre 2023
AWSSSODirectoryReadOnly	Questa policy ora include il nuovo namespace identitystore-auth con nuove autorizzazioni per consentire agli utenti di elencare e ottenere sessioni.	21 febbraio 2023

Modifica	Descrizione	Data
AWSSSOServiceRolePolicy	Questa politica ora consente di eseguire l'`UpdateSAMLProvider` azione sull'account di gestione.	20 ottobre 2022
AWSSSOMasterAccountAdministrator	Questa politica ora include il nuovo namespace `identitystore-auth` con nuove autorizzazioni per consentire all'amministratore di elencare ed eliminare le sessioni per un utente.	20 ottobre 2022
AWSSSOMemberAccountAdministrator	Questa politica ora include il nuovo spazio dei nomi `identitystore-auth` con nuove autorizzazioni per consentire all'amministratore di elencare ed eliminare le sessioni per un utente.	20 ottobre 2022
AWSSSODirectoryAdministrator	Questa politica ora include il nuovo spazio dei nomi `identitystore-auth` con nuove autorizzazioni per consentire all'amministratore di elencare ed eliminare le sessioni per un utente.	20 ottobre 2022

Modifica	Descrizione	Data
AWSSSOMasterAccountAdministrator	Questa politica ora include nuove autorizzazioni per le chiamate. `ListDelegatedAdministrators` _ AWS Organizations Questa politica ora include anche un sottoinsieme di autorizzazioni `AWSSSOManageDelegatedAdministrator` che include le autorizzazioni per chiamare e. `RegisterDelegatedAdministrator` `DeregisterDelegatedAdministrator`	16 agosto 2022
AWSSSOMemberAccountAdministrator	Questa politica ora include nuove autorizzazioni per chiamare. `ListDelegatedAdministrators` _ AWS Organizations Questa politica ora include anche un sottoinsieme di autorizzazioni `AWSSSOManageDelegatedAdministrator` che include le autorizzazioni per chiamare e. `RegisterDelegatedAdministrator` `DeregisterDelegatedAdministrator`	16 agosto 2022

Modifica	Descrizione	Data
AWSSSOReadOnly	Questa politica ora include nuove autorizzazioni per chiamare `ListDelegatedAdministrators` AWS Organizations	11 agosto 2022
AWSSSOServiceRolePolicy	Questa politica ora include nuove autorizzazioni per chiamare `DeleteRolePermissionsBoundary` e. `PutRolePermisionsBoundary`	14 luglio 2022
AWSSSOServiceRolePolicy	Questa politica ora include nuove autorizzazioni che consentono di effettuare chiamate in `ListAWSServiceAccessForOrganization` and `ListDelegatedAdministrators` entrata. AWS Organizations	11 maggio 2022
AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator AWSSSOReadOnly	Aggiungi le autorizzazioni di IAM Access Analyzer che consentono a un principale di utilizzare i controlli delle policy per la convalida.	28 aprile 2022

Modifica	Descrizione	Data
AWSSSOMasterAccountAdministrator	Questa policy ora consente tutte le azioni del servizio IAM Identity Center Identity Store. Per informazioni sulle azioni disponibili nel servizio IAM Identity Center Identity Store, consulta il riferimento all'API IAM Identity Center Identity Store.	29 marzo 2022
AWSSSOMemberAccountAdministrator	Questa policy ora consente tutte le azioni del servizio IAM Identity Center Identity Store.	29 marzo 2022
AWSSSODirectoryAdministrator	Questa policy ora consente tutte le azioni del servizio IAM Identity Center Identity Store.	29 marzo 2022
AWSSSODirectoryReadOnly	Questa policy ora consente l'accesso alle azioni di lettura del servizio IAM Identity Center Identity Store. Questo accesso è necessario per recuperare le informazioni su utenti e gruppi dal servizio IAM Identity Center Identity Store.	29 marzo 2022
AWSIdentitySyncFullAccess	Questa policy consente l'accesso completo alle autorizzazioni di sincronizzazione delle identità.	3 marzo 2022

Modifica	Descrizione	Data
AWSIdentitySyncReadOnlyAccess	Questo criterio concede autorizzazioni di sola lettura che consentono a un principal e di visualizzare le impostazioni di sincronizzazione dell'identità.	3 marzo 2022
AWSSSOReadOnly	Questa policy concede autorizzazioni di sola lettura che consentono a un principal e di visualizzare le impostazioni di configurazione di IAM Identity Center.	4 agosto 2021
IAM Identity Center ha iniziato a tracciare le modifiche	IAM Identity Center ha iniziato a tracciare le modifiche per le policy AWS gestite.	4 agosto 2021

Utilizzo di ruoli collegati ai servizi per IAM Identity Center

AWS IAM Identity Center utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a IAM Identity Center. È predefinito da IAM Identity Center e include tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per tuo conto. Per ulteriori informazioni, consulta Ruoli collegati ai servizi.

Un ruolo collegato al servizio semplifica la configurazione di IAM Identity Center perché non è necessario aggiungere manualmente le autorizzazioni necessarie. IAM Identity Center definisce le autorizzazioni del suo ruolo collegato al servizio e, se non diversamente definito, solo IAM Identity Center può assumerne il ruolo. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate al servizio per IAM Identity Center

IAM Identity Center utilizza il ruolo collegato al servizio denominato AWSServiceRoleForSSOper concedere a IAM Identity Center le autorizzazioni per gestire le AWS risorse, inclusi i ruoli IAM, le policy e l'IdP SAML per tuo conto.

Il ruolo AWSServiceRoleForSSO collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `IAM Identity Center`

La politica di autorizzazione dei ruoli AWSServiceRoleForSSO collegati ai servizi consente a IAM Identity Center di completare quanto segue sui ruoli nel percorso «/aws-reserved/sso.amazonaws.com/» e con il prefisso «_»: AWSReservedSSO

- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam:DeleteRole`
- `iam:DeleteRolePermissionsBoundary`
- `iam:DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetRole`
- `iam:ListRolePolicies`
- `iam:PutRolePolicy`
- `iam:PutRolePermissionsBoundary`
- `iam:ListAttachedRolePolicies`

La politica di autorizzazione dei ruoli AWSServiceRoleForSSO collegati ai servizi consente a IAM Identity Center di completare quanto segue sui provider SAML con il prefisso «_»: AWSSSO

- `iam:CreateSAMLProvider`
- `iam:GetSAMLProvider`
- `iam:UpdateSAMLProvider`
- `iam:DeleteSAMLProvider`

La politica di autorizzazione dei ruoli AWSServiceRoleForSSO collegati ai servizi consente a IAM Identity Center di completare quanto segue per tutte le organizzazioni:

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

La policy AWSServiceRoleForSSO di autorizzazione dei ruoli collegati al servizio consente a IAM Identity Center di completare quanto segue su tutti i ruoli IAM (*):

- `iam:listRoles`

La policy di autorizzazione dei ruoli AWSServiceRoleForSSO collegati ai servizi consente a IAM Identity Center di completare quanto segue su «arn:aws:iam: :*:role/ /sso.amazonaws.com/»: aws-service-role AWSServiceRoleForSSO

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam:DeleteServiceLinkedRole`

La politica di autorizzazione dei ruoli consente a IAM Identity Center di completare le seguenti azioni sulle risorse.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"IAMRoleProvisioningActions",
         "Effect":"Allow",
         "Action":[
            "iam:AttachRolePolicy",
            "iam:CreateRole",
            "iam:DeleteRolePermissionsBoundary",
            "iam:PutRolePermissionsBoundary",
            "iam:PutRolePolicy",
            "iam:UpdateRole",
            "iam:UpdateRoleDescription",
```

```
            "iam:UpdateAssumeRolePolicy"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
         ],
         "Condition":{
            "StringNotEquals":{
               "aws:PrincipalOrgMasterAccountId":"${aws:PrincipalAccount}"
            }
         }
      },
      {
         "Sid":"IAMRoleReadActions",
         "Effect":"Allow",
         "Action":[
            "iam:GetRole",
            "iam:ListRoles"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"IAMRoleCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteRole",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:ListRolePolicies",
            "iam:ListAttachedRolePolicies"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
         ]
      },
      {
         "Sid":"IAMSLRCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus",
            "iam:DeleteRole",
            "iam:GetRole"
```

```
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO"
         ]
      },
      {
        "Sid": "IAMSAMLProviderCreationAction",
        "Effect": "Allow",
        "Action": [
          "iam:CreateSAMLProvider"
      ],
      "Resource": [
         "arn:aws:iam::*:saml-provider/AWSSSO_*"
       ],
      "Condition": {
         "StringNotEquals": {
           "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
          }
        }
      },
      {
        "Sid": "IAMSAMLProviderUpdateAction",
        "Effect": "Allow",
        "Action": [
          "iam:UpdateSAMLProvider"
        ],
        "Resource": [
           "arn:aws:iam::*:saml-provider/AWSSSO_*"
        ]
      },
      {
         "Sid":"IAMSAMLProviderCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteSAMLProvider",
            "iam:GetSAMLProvider"
         ],
         "Resource":[
            "arn:aws:iam::*:saml-provider/AWSSSO_*"
         ]
      },
      {
         "Effect":"Allow",
```

```
         "Action":[
            "organizations:DescribeAccount",
            "organizations:DescribeOrganization",
            "organizations:ListAccounts",
            "organizations:ListAWSServiceAccessForOrganization",
            "organizations:ListDelegatedAdministrators"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"AllowUnauthAppForDirectory",
         "Effect":"Allow",
         "Action":[
            "ds:UnauthorizeApplication"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"AllowDescribeForDirectory",
         "Effect":"Allow",
         "Action":[
            "ds:DescribeDirectories",
            "ds:DescribeTrusts"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"AllowDescribeAndListOperationsOnIdentitySource",
         "Effect":"Allow",
         "Action":[
            "identitystore:DescribeUser",
            "identitystore:DescribeGroup",
            "identitystore:ListGroups",
            "identitystore:ListUsers"
         ],
         "Resource":[
            "*"
         ]
```

```
        }
    ]
}
```

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per IAM Identity Center

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Una volta abilitato, IAM Identity Center crea un ruolo collegato ai servizi in tutti gli account all'interno dell'organizzazione in Organizations AWS . IAM Identity Center crea inoltre lo stesso ruolo collegato ai servizi in ogni account che viene successivamente aggiunto all'organizzazione. Questo ruolo consente a IAM Identity Center di accedere alle risorse di ciascun account per tuo conto.

> **Note**
>
> - Se hai effettuato l'accesso all'account di AWS Organizations gestione, questo utilizza il ruolo attualmente connesso e non il ruolo collegato al servizio. Ciò impedisce l'aumento dei privilegi.
> - Quando IAM Identity Center esegue qualsiasi operazione IAM nell'account di AWS Organizations gestione, tutte le operazioni avvengono utilizzando le credenziali del responsabile IAM. Ciò consente agli accessi di CloudTrail fornire la visibilità di chi ha apportato tutte le modifiche ai privilegi nell'account di gestione.

> **Important**
>
> Se utilizzavi il servizio IAM Identity Center prima del 7 dicembre 2017, quando ha iniziato a supportare i ruoli collegati al servizio, IAM Identity Center ha creato il AWSServiceRoleForSSO ruolo nel tuo account. Per ulteriori informazioni, consulta Un nuovo ruolo è apparso nel mio account IAM.

Se elimini questo ruolo collegato ai servizi e devi crearlo di nuovo, puoi utilizzare lo stesso processo per ricreare il ruolo nel tuo account.

Modifica di un ruolo collegato al servizio per IAM Identity Center

IAM Identity Center non consente di modificare il ruolo collegato al AWSServiceRoleForSSO servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per IAM Identity Center

Non è necessario eliminare manualmente il ruolo. AWSServiceRoleForSSO Quando un Account AWS utente viene rimosso da un' AWS organizzazione, IAM Identity Center ripulisce automaticamente le risorse ed elimina il ruolo collegato al servizio. Account AWS

Puoi anche utilizzare la console IAM, la CLI IAM o l'API IAM per eliminare manualmente il ruolo collegato al servizio. Per farlo, sarà necessario prima eseguire manualmente la pulizia delle risorse associate al ruolo collegato ai servizi e poi eliminarlo manualmente.

> **Note**
>
> Se il servizio IAM Identity Center utilizza il ruolo quando tenti di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse IAM Identity Center utilizzate da AWSServiceRoleForSSO

1. Rimuovi l'accesso a utenti e gruppiper tutti gli utenti e i gruppi che hanno accesso a Account AWS.
2. Eliminare i set di autorizzazioniche hai associato a Account AWS.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM, la CLI IAM o l'API IAM per eliminare il ruolo collegato al AWSServiceRoleForSSO servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Console IAM Identity Center e autorizzazione API

Le API della console IAM Identity Center esistenti supportano la doppia autorizzazione, che consente di mantenere l'uso delle operazioni API esistenti quando sono disponibili API più recenti. Se disponi di istanze esistenti di IAM Identity Center create prima del 15 novembre 2023 e del 15 ottobre 2020, puoi utilizzare le seguenti tabelle per determinare quali operazioni API ora vengono mappate a nuove operazioni API rilasciate dopo tali date.

Argomenti

Azioni API dopo novembre 2023

Le istanze di IAM Identity Center create prima del 15 novembre 2023 rispettano le azioni API vecchie e nuove, purché non venga negata esplicitamente alcuna delle azioni. Le istanze create dopo il 15 novembre 2023 utilizzano azioni API più recenti per l'autorizzazione nella console IAM Identity Center.

Nome operativo della console utilizzato prima del 15 novembre 2023	Azione API utilizzata dopo il 15 novembre 2023
AssociateProfile	CreateApplicationAssignment
CreateManagedApplicationInstance | CreateApplicationInstance	CreateApplication
CreateManagedApplicationInstance	PutApplicationAuthenticationMethod
DeleteApplicationInstance | DeleteManagedApplicationInstance	DeleteApplication
DeleteSSO	DeleteInstance
DisassociateProfile	DeleteApplicationAssignment
GetApplicationTemplate	DescribeApplicationProvider

Nome operativo della console utilizzato prima del 15 novembre 2023	Azione API utilizzata dopo il 15 novembre 2023
GetManagedApplicationInstance	DescribeApplication
GetSharedSsoConfiguration	DescribeInstance
ListApplicationInstances	ListApplications
ListApplicationTemplates	ListApplicationProviders
ListDirectoryAssociations	DescribeInstance
ListProfileAssociations	ListApplicationAssignments
UpdateApplicationInstanceDisplayData | UpdateApplicationInstanceStatus | UpdateManagedApplicationInstanceStatus	UpdateApplication

Azioni API successive a ottobre 2020

Le istanze di IAM Identity Center create prima del 15 ottobre 2020 rispettano le azioni API vecchie e nuove, purché non venga negata esplicitamente alcuna delle azioni. Le istanze create dopo il 15 ottobre 2020 utilizzano azioni API più recenti per l'autorizzazione nella console IAM Identity Center.

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
AssociateProfile	AssociateProfile	CreateAccountAssignment
AttachManagedPolicy	PutPermissionsPolicy	AttachManagedPolicyToPermissionSet
CreatePermissionSet	CreatePermissionSet	CreatePermissionSet
DeleteApplicationInstanceForAWsAccount	DeleteApplicationInstance | DeleteTrust	DeleteAccountAssignment

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
DeleteApplicationProfileForAwsAccount	DeleteProfile	DeleteAccountAssignment
DeletePermissionsPolicy	DeletePermissionsPolicy	DeleteInlinePolicyFromPermissionSet
DeletePermissionSet	DeletePermissionSet	DeletePermissionSet
DescribePermissionsPolicies	DescribePermissionsPolicies	ListManagedPoliciesInPermissionSet
DetachManagedPolicy	DeletePermissionsPolicy	DetachManagedPolicyFromPermissionSet
DisassociateProfile	DisassociateProfile	DeleteAccountAssignment
GetApplicationInstanceForAWSAccount	GetApplicationInstance	ListAccountAssignments
GetAWSAccountProfileStatus	GetProfile	ListPermissionSetsProvisionedToAccount
GetPermissionSet	GetPermissionSet	DescribePermissionSet
GetPermissionsPolicy	GetPermissionsPolicy	GetInlinePolicyForPermissionSet
ListAccountsWithProvisionedPermissionSet	ListApplicationInstances | GetApplicationInstance	ListAccountsForProvisionedPermissionSet
ListAWSAccountProfiles	ListProfiles | GetProfile	ListPermissionSetsProvisionedToAccount
ListPermissionSets	ListPermissionSets	ListPermissionSets
ListProfileAssociations	ListProfileAssociations	ListAccountAssignments

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance | CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile | CreateProfile | UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust | CreateTrust | UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet
UpdatePermissionSet	UpdatePermissionSet	UpdatePermissionSet

AWS STS chiavi contestuali di condizione per IAM Identity Center

Quando un principale effettua una richiesta a AWS, AWS raccoglie le informazioni sulla richiesta in un contesto di richiesta, che viene utilizzato per valutare e autorizzare la richiesta. È possibile utilizzare l'elemento `Condition` di una policy JSON per confrontare le chiavi della richiesta con i valori chiave specificati nella policy. Le informazioni sulla richiesta vengono fornite da diverse fonti, tra cui il responsabile della richiesta, la risorsa, la richiesta a fronte della quale viene effettuata e i metadati relativi alla richiesta stessa. Le chiavi di condizione specifiche del servizio sono definite per l'uso con un singolo servizio. AWS

IAM Identity Center include un provider di AWS STS contesto che consente alle applicazioni AWS gestite e alle applicazioni di terze parti di aggiungere valori per le chiavi di condizione definite da IAM Identity Center. Queste chiavi sono incluse nei ruoli IAM. I valori chiave vengono impostati quando un'applicazione passa un token a AWS STS. L'applicazione ottiene il token a cui passa AWS STS in uno dei seguenti modi:

- Durante l'autenticazione con IAM Identity Center.
- Dopo lo scambio di token con un emittente di token affidabile per la propagazione dell'identità affidabile. In questo caso, l'applicazione ottiene un token da un emittente di token affidabile e lo scambia con un token di IAM Identity Center.

Queste chiavi vengono in genere utilizzate da applicazioni che si integrano con la propagazione affidabile delle identità. In alcuni casi, quando sono presenti valori chiave, puoi utilizzare queste chiavi nelle policy IAM che crei per consentire o negare le autorizzazioni.

Ad esempio, potresti voler fornire un accesso condizionale a una risorsa in base al valore di. `UserId` Questo valore indica quale utente di IAM Identity Center utilizza il ruolo. L'esempio è simile all'utilizzo`SourceId`. A differenza`SourceId`, tuttavia, il valore per `UserId` rappresenta un utente specifico e verificato dell'archivio di identità. Questo valore è presente nel token che l'applicazione ottiene e a cui AWS STS passa. Non è una stringa generica che può contenere valori arbitrari.

Argomenti

- archivio di identità: UserId
- archivio di identità: IdentityStoreArn
- centro di identità: ApplicationArn
- centro di identità: CredentialId
- centro di identità: InstanceArn

archivio di identità: UserId

Questa chiave di contesto è l'utente `UserId` di IAM Identity Center che è l'oggetto dell'asserzione di contesto emessa da IAM Identity Center. L'asserzione di contesto viene passata a. AWS STS Puoi utilizzare questa chiave per confrontare l'utente `UserId` di IAM Identity Center per conto del quale viene effettuata la richiesta con l'identificatore dell'utente specificato nella policy.

- Disponibilità: questa chiave viene inclusa nel contesto della richiesta dopo l'impostazione di un'asserzione di contesto emessa da IAM Identity Center, quando si assume un ruolo utilizzando qualsiasi AWS STS `assume-role` comando nell'operazione AWS CLI o nell' AWS STS `AssumeRole`API.
- Tipo di dati: stringa
- Tipo di valore: valore singolo

archivio di identità: IdentityStoreArn

Questa chiave di contesto è l'ARN dell'archivio di identità collegato all'istanza di IAM Identity Center che ha emesso l'asserzione di contesto. È anche l'archivio di identità in cui è possibile cercare

gli attributi. `identitystore:UserID` È possibile utilizzare questa chiave nelle politiche per determinare se `identitystore:UserID` proviene dall'ARN di un archivio di identità previsto.

- Disponibilità: questa chiave viene inclusa nel contesto della richiesta dopo l'impostazione di un'asserzione di contesto emessa da IAM Identity Center, quando si assume un ruolo utilizzando qualsiasi AWS STS `assume-role` comando nell'operazione AWS CLI o AWS STS `AssumeRole` API.
- Tipo di dati: Arn, String
- Tipo di valore: valore singolo

centro di identità: ApplicationArn

Questa chiave di contesto è l'ARN dell'applicazione a cui IAM Identity Center ha emesso un'asserzione di contesto. È possibile utilizzare questa chiave nelle policy per determinare se `identitycenter:ApplicationArn` proviene da un'applicazione prevista. L'utilizzo di questa chiave può aiutare a impedire l'accesso a un ruolo IAM da parte di un'applicazione inaspettata.

- Disponibilità: questa chiave è inclusa nel contesto della richiesta di un'operazione AWS STS `AssumeRole` API. Il contesto della richiesta include un'asserzione di contesto emessa da IAM Identity Center.
- Tipo di dati: Arn, String
- Tipo di valore: valore singolo

centro di identità: CredentialId

Questa chiave di contesto è un ID casuale per la credenziale del ruolo con identità avanzata e viene utilizzata solo per la registrazione. Poiché questo valore chiave è imprevedibile, si consiglia di non utilizzarlo per asserzioni contestuali nelle politiche.

- Disponibilità: questa chiave è inclusa nel contesto della richiesta di un' AWS STS `AssumeRole`operazione API. Il contesto della richiesta include un'asserzione di contesto emessa da IAM Identity Center.
- Tipo di dati: stringa
- Tipo di valore: valore singolo

centro di identità: InstanceArn

Questa chiave di contesto è l'ARN dell'istanza di IAM Identity Center che ha emesso l'asserzione di contesto per. `identitystore:UserID` Puoi utilizzare questa chiave per determinare se l'asserzione `identitystore:UserID` and context proviene dall'ARN di un'istanza IAM Identity Center prevista.

- Disponibilità: questa chiave è inclusa nel contesto della richiesta di un'operazione AWS STS `AssumeRole` API. Il contesto della richiesta include un'asserzione di contesto emessa da IAM Identity Center.
- Tipo di dati: Arn, String
- Tipo di valore: valore singolo

Registrazione e monitoraggio in IAM Identity Center

Come best practice, dovresti monitorare la tua organizzazione per accertarti che le modifiche vengano registrate. Questo ti aiuta a garantire che eventuali modifiche impreviste possano essere esaminate e che le modifiche indesiderate possano essere annullate. AWS IAM Identity Center attualmente supporta due AWS servizi che consentono di monitorare l'organizzazione e le attività che si svolgono al suo interno.

Argomenti

- Registrazione delle chiamate API di IAM Identity Center con AWS CloudTrail
- Amazon EventBridge
- Registrazione degli errori di sincronizzazione AD e di sincronizzazione AD configurabili

Registrazione delle chiamate API di IAM Identity Center con AWS CloudTrail

AWS IAM Identity Center è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in IAM Identity Center. CloudTrail acquisisce le chiamate API per IAM Identity Center come eventi. Le chiamate acquisite includono chiamate dalla console IAM Identity Center e chiamate di codice alle operazioni dell'API IAM Identity Center. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per IAM Identity Center. Se non configuri un percorso, puoi comunque visualizzare gli eventi

più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata effettuata a IAM Identity Center, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Argomenti

Informazioni su IAM Identity Center in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività in IAM Identity Center, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi che si verificano nel tuo Account AWS, compresi gli eventi per IAM Identity Center, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le Regioni AWS . Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Quando CloudTrail la registrazione è abilitata in IAM Identity Center Account AWS, le chiamate API effettuate alle azioni di IAM Identity Center vengono tracciate nei file di registro. I record di IAM Identity Center vengono scritti insieme ad altri record AWS di servizio in un file di registro. CloudTrail

determina quando creare e scrivere su un nuovo file in base a un periodo di tempo e alle dimensioni del file.

Sono supportate le seguenti CloudTrail operazioni di IAM Identity Center:

Operazioni dell'API della console	Operazioni API pubbliche
AssociateDirectory	AttachManagedPolicyToPermissionSet
AssociateProfile	CreateAccountAssignment
BatchDeleteSession	CreateInstanceAccessControlAttributeConfiguration
BatchGetSession	CreatePermissionSet
CreateApplicationInstance	DeleteAccountAssignment
CreateApplicationInstanceCertificate	DeleteInlinePolicyFromPermissionSet
CreatePermissionSet	DeleteInstanceAccessControlAttributeConfiguration
CreateProfile	DeletePermissionSet
DeleteApplicationInstance	DescribeAccountAssignmentCreationStatus
DeleteApplicationInstanceCertificate	DescribeAccountAssignmentDeletionStatus
DeletePermissionsPolicy	DescribeInstanceAccessControlAttributeConfiguration
DeletePermissionSet	DescribePermissionSet
DeleteProfile	DescribePermissionSetProvisioningStatus

Operazioni dell'API della console	Operazioni API pubbliche
DescribePermissionsPolicies	DetachManagedPolicyFromPermissionSet
DisassociateDirectory	GetInlinePolicyForPermissionSet
DisassociateProfile	ListAccountAssignmentCreationStatus
GetApplicationInstance	ListAccountAssignmentDeletionStatus
GetApplicationTemplate	ListAccountAssignments
GetMfaDeviceManagementForDirectory	ListAccountsForProvisionedPermissionSet
GetPermissionSet	ListInstances
GetSSOStatus	ListManagedPoliciesInPermissionSet
ImportApplicationInstanceServiceProviderMetadata	ListPermissionSetProvisioningStatus
ListApplicationInstances	ListPermissionSets
ListApplicationInstanceCertificates	ListPermissionSetsProvisionedToAccount
ListApplicationTemplates	ListTagsForResource
ListDirectoryAssociations	ProvisionPermissionSet
ListPermissionSets	PutInlinePolicyToPermissionSet
ListProfileAssociations	TagResource
ListProfiles	UntagResource

Operazioni dell'API della console	Operazioni API pubbliche
ListSessions	UpdateInstanceAccessControlAttributeConfiguration
PutMfaDeviceManagementForDirectory	UpdatePermissionSet
PutPermissionsPolicy	
StartSSO	
UpdateApplicationInstanceActiveCertificate	
UpdateApplicationInstanceDisplayData	
UpdateApplicationInstanceServiceProviderConfiguration	
UpdateApplicationInstanceStatus	
UpdateApplicationInstanceResponseConfiguration	
UpdateApplicationInstanceResponseSchemaConfiguration	
UpdateApplicationInstanceSecurityConfiguration	
UpdateDirectoryAssociation	
UpdateProfile	

Per ulteriori informazioni sulle operazioni delle API pubbliche di IAM Identity Center, consulta la Guida di riferimento dell'API IAM Identity Center.

Sono supportate le seguenti CloudTrail operazioni di IAM Identity Center Identity Store:

- AddMemberToGroup
- CompleteVirtualMfaDeviceRegistration
- CompleteWebAuthnDeviceRegistration
- CreateAlias
- CreateExternalIdPConfigurationForDirectory
- CreateGroup
- CreateUser
- DeleteExternalIdPConfigurationForDirectory
- DeleteGroup
- DeleteMfaDeviceForUser
- DeleteUser
- DescribeDirectory
- DescribeGroups
- DescribeUsers
- DisableExternalIdPConfigurationForDirectory
- DisableUser
- EnableExternalIdPConfigurationForDirectory
- EnableUser
- GetAWSSPConfigurationForDirectory
- ListExternalIdPConfigurationsForDirectory
- ListGroupsForUser
- ListMembersInGroup
- ListMfaDevicesForUser
- PutMfaDeviceManagementForDirectory
- RemoveMemberFromGroup
- SearchGroups
- SearchUsers
- StartVirtualMfaDeviceRegistration
- StartWebAuthnDeviceRegistration

- `UpdateExternalIdPConfigurationForDirectory`
- `UpdateGroup`
- `UpdateMfaDeviceForUser`
- `UpdatePassword`
- `UpdateUser`
- `VerifyEmail`

Sono supportate le seguenti CloudTrail azioni OIDC di IAM Identity Center:

- `CreateToken`
- `RegisterClient`
- `StartDeviceAuthorization`

Sono supportate le seguenti CloudTrail azioni del portale IAM Identity Center:

- `Authenticate`
- `Federate`
- `ListApplications`
- `ListProfilesForApplication`
- `ListAccounts`
- `ListAccountRoles`
- `GetRoleCredentials`
- `Logout`

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o utente AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, vedete l'elemento CloudTrail userIdentity.

Comprensione delle voci dei file di registro di IAM Identity Center

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro per un amministratore (samadams@example.com) che ha avuto luogo nella console IAM Identity Center:


```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDAJAIENLMexample",
            "arn":"arn:aws:iam::08966example:user/samadams",
            "accountId":"08966example",
            "accessKeyId":"AKIAIIJM2K4example",
            "userName":"samadams"
         },
         "eventTime":"2017-11-29T22:39:43Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"DescribePermissionsPolicies",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":{
            "permissionSetId":"ps-79a0dde74b95ed05"
         },
         "responseElements":null,
         "requestID":"319ac6a1-d556-11e7-a34f-69a333106015",
         "eventID":"a93a952b-13dd-4ae5-a156-d3ad6220b071",
         "readOnly":true,
         "resources":[

         ],
```

```
         "eventType":"AwsApiCall",
         "recipientAccountId":"08966example"
      }
   ]
}
```

L'esempio seguente mostra una voce di CloudTrail registro per un'azione dell'utente finale (bobsmith@example.com) avvenuta nel portale di AWS accesso:

```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"Unknown",
            "principalId":"example.com//
S-1-5-21-1122334455-3652759393-4233131409-1126",
            "accountId":"08966example",
            "userName":"bobsmith@example.com"
         },
         "eventTime":"2017-11-29T18:48:28Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"ListApplications",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":null,
         "responseElements":null,
         "requestID":"de6c0435-ce4b-49c7-9bcc-bc5ed631ce04",
         "eventID":"e6e1f3df-9528-4c6d-a877-6b2b895d1f91",
         "eventType":"AwsApiCall",
         "recipientAccountId":"08966example"
      }
   ]
}
```

L'esempio seguente mostra una voce di CloudTrail registro per un'azione dell'utente finale (bobsmith@example.com) che ha avuto luogo in IAM Identity Center OIDC:

```
{
      "eventVersion": "1.05",
      "userIdentity": {
```

```
        "type": "Unknown",
        "principalId": "example.com//S-1-5-21-1122334455-3652759393-4233131409-1126",
        "accountId": "08966example",
        "userName": "bobsmith@example.com"
      },
      "eventTime": "2020-06-16T01:31:15Z",
      "eventSource": "sso.amazonaws.com",
      "eventName": "CreateToken",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "203.0.113.0",
      "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
      "requestParameters": {
        "clientId": "clientid1234example",
        "clientSecret": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "grantType": "urn:ietf:params:oauth:grant-type:device_code",
        "deviceCode": "devicecode1234example"
      },
      "responseElements": {
        "accessToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "tokenType": "Bearer",
        "expiresIn": 28800,
        "refreshToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "idToken": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "eventID": "09a6e1a9-50e5-45c0-9f08-e6ef5089b262",
      "readOnly": false,
      "resources": [
        {
          "accountId": "08966example",
          "type": "IdentityStoreId",
          "ARN": "d-1234example"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "08966example"
}
```

Comprensione degli eventi di accesso a IAM Identity Center

AWS CloudTrail registra gli eventi di accesso riusciti e quelli non riusciti per tutte le fonti di identità. AWS IAM Identity Center Le identità native di origine SSO e Active Directory (AD Connector e AWS Managed Microsoft AD) includeranno eventi di accesso aggiuntivi che vengono acquisiti ogni volta

che a un utente viene richiesto di risolvere un problema o un fattore specifico delle credenziali, nonché lo stato di quella particolare richiesta di verifica delle credenziali. Solo dopo aver completato tutte le richieste relative alle credenziali, l'utente potrà accedere, il che comporterà la registrazione di un evento. `UserAuthentication`

La tabella seguente riporta i nomi degli CloudTrail eventi di accesso a IAM Identity Center, il loro scopo e l'applicabilità a diverse fonti di identità.

Nome evento	Scopo dell'evento	Applicabilità della fonte di identità
`CredentialChallenge`	Utilizzato per notificare che IAM Identity Center ha richiesto all'utente di risolvere una specifica richiesta di credenziali e specifica `CredentialType` quella richiesta (ad esempio, PASSWORD o TOTP).	Utenti nativi di IAM Identity Center, AD Connector e AWS Managed Microsoft AD
`CredentialVerification`	Utilizzato per notificare che l'utente ha tentato di risolvere una `CredentialChallenge` richiesta specifica e specifica se la credenziale è riuscita o meno.	Utenti nativi di IAM Identity Center, AD Connector e AWS Managed Microsoft AD
`UserAuthentication`	Utilizzato per notificare che tutti i requisiti di autenticazione richiesti dall'utente sono stati completati con successo e che l'utente ha effettuato correttamente l'accesso. Gli utenti che non riusciranno a completare correttamente le sfide relative alle credenziali richieste non comporteranno la registraz	Tutte le fonti di identità

Nome evento	Scopo dell'evento	Applicabilità della fonte di identità
	ione di alcun *UserAuthentication* evento.	

La tabella seguente riporta ulteriori utili campi di dati sugli eventi contenuti all'interno di eventi di accesso CloudTrail specifici.

Nome evento	Scopo dell'evento	Applicabilità dell'evento di accesso	Valori di esempio
`AuthWorkflowID`	Utilizzato per correlare tutti gli eventi emessi in un'intera sequenza di accesso. Per ogni accesso utente, IAM Identity Center può emettere più eventi.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	"AuthWorkflowID»: «9de74b32-8362-4a01-a524-de21df59fd83"
`CredentialType`	Utilizzato per specificare la credenziale o il fattore che è stato contestato. `UserAuthentication` gli eventi includeranno tutti i `CredentialType` valori che sono stati verificati con successo nella sequenza di accesso dell'utente.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	CredentialType«: «PASSWORD» o "«: CredentialType «PASSWORD, TOTP» (i valori possibili includono: PASSWORD, TOTP, WEBAUTHN, EXTERNAL_IDP, RESYNC_TOTP)

Nome evento	Scopo dell'evento	Applicabilità dell'evento di accesso	Valori di esempio
`DeviceEnrollmentRequired`	Utilizzato per specificare che all'utente era richiesto di registrare un dispositivo MFA durante l'accesso e che l'utente ha completato con successo la richiesta.	`UserAuthentication`	"DeviceEnrollmentRequired«: «vero»
`LoginTo`	Utilizzato per specificare la posizione di reindirizzamento dopo una sequenza di accesso riuscita.	`UserAuthentication`	"LoginTo«:" https://mydirectory.awsapps.com/start/...»

Eventi di esempio per scenari di accesso a IAM Identity Center

Gli esempi seguenti mostrano la sequenza di CloudTrail eventi prevista per diversi scenari di accesso.

Argomenti

- Accesso riuscito durante l'autenticazione con una sola password
- Accesso riuscito durante l'autenticazione con un provider di identità esterno
- Accesso riuscito durante l'autenticazione con una password e un'app di autenticazione TOTP
- È necessario effettuare correttamente l'accesso durante l'autenticazione con una password e la registrazione MFA forzata
- Accesso non riuscito durante l'autenticazione con solo una password

Accesso riuscito durante l'autenticazione con una sola password

La seguente sequenza di eventi riporta un esempio di accesso riuscito con sola password.

CredentialChallenge (Password)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:33:58Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"5be44ffb-6946-4f47-acaf-1adebd4afead",
   "eventID":"27ea7725-c1fd-4355-bdba-d0e628e0e604",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


Operazione riuscita CredentialVerification (password)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
```

```
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"c49640f6-0c8a-43d3-a6e0-900e3bb188d4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```


Operazione completata UserAuthentication (solo password)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
```

```
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


Accesso riuscito durante l'autenticazione con un provider di identità esterno

La seguente sequenza di eventi riporta un esempio di accesso riuscito in caso di autenticazione tramite il protocollo SAML utilizzando un provider di identità esterno.

Operazione riuscita UserAuthentication (provider di identità esterno)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":""
   },
```

```
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"EXTERNAL_IDP"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


Accesso riuscito durante l'autenticazione con una password e un'app di autenticazione TOTP

La seguente sequenza di eventi illustra un esempio in cui era richiesta l'autenticazione a più fattori durante l'accesso e l'utente ha effettuato correttamente l'accesso utilizzando una password e un'app di autenticazione TOTP.

CredentialChallenge (Password)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
```

```
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:13Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"e454ea66-1027-4d00-9912-09c0589649e1",
   "eventID":"d89cc0b5-a23a-4b88-843a-89329aeaef2e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

Operazione riuscita CredentialVerification (password)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:20Z",
```

```
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"4533fd49-6669-4d0b-b272-a0b2139309a8",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

CredentialChallenge (TOTP)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
```

```
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"29202f08-f240-40cc-b789-c0cea8a27847",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


Riuscito CredentialVerification (TOTP)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
```

```
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"e889ff1d-fcaf-454f-805d-7132cf2362a4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```


Operazione riuscita UserAuthentication (Password + TOTP)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVLeFhWeDRmZFJmMmxHcWYwdzhZck5RQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11Fir1mCVJ-4Y5UY6RI10UCXvRePCHd6195xvYg1rwo1Pj7B-7UGIGlYUUVe31Nkzd7ihxKn6DMdnFfO01O8qc3RF
Sx-pjBXKG_jUcvBk_UILdGytV4o1u97h42B-
TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token
\u003dNMlui44guoVnxRd0qu2tYJIdyyFPX6SDRNTspIScfMM0AgFbho1nvvCaxPTghHbgHCRIXdffFtzH0sL1ow419Bobn
\u0026organization\u003dd-9067230c03\u0026region\u003dus-east-1",
```

```
      "CredentialType":"PASSWORD,TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"7a8c8725-db2f-488d-a43e-788dc6c73a4a",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```

È necessario effettuare correttamente l'accesso durante l'autenticazione con una password e la registrazione MFA forzata

La seguente sequenza di eventi riporta un esempio di accesso riuscito con password, ma l'utente era obbligato e ha completato con successo la registrazione di un dispositivo MFA prima di completare l'accesso.

CredentialChallenge (Password)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:02Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
```

```
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"321f4b13-42b5-4005-a0f7-826cad26d159",
   "eventID":"8c707b0f-e45a-4a9c-bee2-ff68638d2f1b",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

Operazione riuscita CredentialVerification (password)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"12b57efa-0a92-4479-91a3-5b6641817c21",
   "eventID":"783b0c89-7142-4942-8b84-6ee0de1b992e",
   "readOnly":false,
```

```
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```


Operazione completata UserAuthentication (è richiesta la password e la registrazione MFA)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:14Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVGQ3VqdHF5aW9CUDdrNXRTVTJUaWNnQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11eZ80S_maUsZ7ABETjeQhyWfvIHYz52rgR28sYAKN1oEk2G07czrwzXvE9HLlN2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY EgU3fhOL3QWvWiquYnDPMyPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrgrgbxXat2M646UZGp93krw7WYQdHIgi5OYI9QSc
\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD",
      "DeviceEnrollmentRequired":"true"
   },
```

```
   "requestID":"74d24604-a365-4237-8c4a-350795494b92",
   "eventID":"a15bf257-7f37-46c0-b67c-fea5fa6166be",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```

Accesso non riuscito durante l'autenticazione con solo una password

La seguente sequenza di eventi riporta un esempio di accesso non riuscito con sola password.

CredentialChallenge (Password)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T18:56:15Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f54848ea-b1aa-402f-bf0d-a54561a2ffcc",
   "eventID":"d96f1d6c-dbd9-4a0b-9a45-6a2b66078c78",
   "readOnly":false,
```

```
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

Fallito CredentialVerification (password)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T18:56:21Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
   },
   "requestID":"04528c82-a678-4a1f-a56d-ea2c6445a72a",
   "eventID":"9160fe06-fc2a-474f-9b78-000ee067a09d",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Failure"
```

```
    }
}
```

Amazon EventBridge

IAM Identity Center può collaborare con Amazon EventBridge per generare eventi quando si verificano azioni specificate dall'amministratore in un'organizzazione. Ad esempio, data la sensibilità di tali operazioni, la maggior parte degli amministratori desidera essere avvisata ogni volta che un utente crea un nuovo account nell'organizzazione o quando un amministratore di un account membro tenta di lasciare l'organizzazione. Puoi configurare EventBridge regole che cercano queste azioni e quindi inviare gli eventi generati a destinazioni definite dall'amministratore. I target possono essere un argomento Amazon SNS che invia e-mail o messaggi di testo agli abbonati. È inoltre possibile creare una AWS Lambda funzione che registri i dettagli dell'azione per una revisione successiva.

Per ulteriori informazioni EventBridge, incluso come configurarlo e abilitarlo, consulta la Amazon EventBridge User Guide.

Registrazione degli errori di sincronizzazione AD e di sincronizzazione AD configurabili

È possibile abilitare la registrazione sulle configurazioni di sincronizzazione con Active Directory (AD) e configurabili di sincronizzazione AD per ricevere registri con informazioni sugli errori che possono verificarsi durante il processo di sincronizzazione. Con questi registri, puoi monitorare se c'è un problema con la sincronizzazione AD e la sincronizzazione AD configurabile e intervenire, se applicabile. Puoi inviare i log a un gruppo di log Amazon CloudWatch Logs, a un bucket Amazon Simple Storage Service (Amazon S3) o a un gruppo di log Amazon Data Firehose con la distribuzione tra account supportata per i bucket Amazon S3 e Firehose.

Per ulteriori informazioni su limitazioni, autorizzazioni e log venduti, consulta Abilitazione della registrazione da. Servizi AWS

> **Note**
>
> Ti viene addebitato un costo per la registrazione. Per ulteriori informazioni, consulta Vend Logs nella pagina CloudWatch dei prezzi di Amazon.

Per abilitare la sincronizzazione AD e i log di errore di sincronizzazione AD configurabili

1. Accedi alla console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, scegli Azioni, quindi scegli Gestisci registri.
4. Scegli Aggiungi consegna dei log e uno dei seguenti tipi di destinazione.
   a. Scegli To Amazon CloudWatch Logs. Quindi scegli o inserisci il gruppo di log di destinazione.
   b. Scegli Amazon S3. Quindi scegli o inserisci il bucket di destinazione.
   c. Scegli To Firehose. Quindi scegli o inserisci il flusso di consegna della destinazione.
5. Scegli Invia.

Per disabilitare la sincronizzazione AD e i log degli errori di sincronizzazione AD configurabili

1. Accedi alla console IAM Identity Center.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, scegli Azioni, quindi scegli Gestisci registri.
4. Scegli Rimuovi per la destinazione che desideri rimuovere.
5. Scegli Invia.

Campi del registro degli errori di sincronizzazione AD e di sincronizzazione AD configurabili

Consulta l'elenco seguente per i possibili campi del registro degli errori.

`sync_profile_name`

Il nome del profilo di sincronizzazione.

`error_code`

Il codice di errore che rappresenta il tipo di errore che si è verificato.

`error_message`

Un messaggio che contiene informazioni dettagliate sull'errore che si è verificato.

`sync_source`

La fonte di sincronizzazione è da dove vengono sincronizzate le entità. Per IAM Identity Center, si tratta di un Active Directory (AD) gestito da AWS Directory Service. La sorgente di sincronizzazione contiene il dominio e l'ARN della directory interessata.

`sync_target`

La destinazione di sincronizzazione è la destinazione in cui vengono salvate le entità. Per IAM Identity Center, si tratta di un Identity Store. La destinazione di sincronizzazione contiene l'ARN di Identity Store interessato.

`source_entity_id`

Un identificatore univoco per l'entità che causa l'errore. Per IAM Identity Center, questo è il SID dell'entità.

`source_entity_type`

Il tipo di entità che causa l'errore. Il valore può essere `USER` o `GROUP`.

`eventTimestamp`

Il timestamp in cui si è verificato l'errore.

Esempi di log degli errori di sincronizzazione AD e di sincronizzazione AD configurabili

Esempio 1: un registro degli errori per una password scaduta per una directory AD

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "InvalidDirectoryCredentials",
        "error_message": "The password for your AD directory has expired. Please reset
 the password to allow Identity Sync to access the directory."
```

```
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:123456789:directory/d-123456",
        "domain": "EXAMPLE.com"
    },
    "eventTimestamp": "1683355579981"
}
```

Esempio 2: un registro degli errori per un utente con un nome utente non univoco

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "ConflictError",
        "error_message": "The source entity has a username conflict with the sync
 target. Please verify that the source identity has a unique username in the target."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:111122223333:directory/d-123456",
        "domain": "EXAMPLE.com"
    },
    "sync_target": {
        "arn": "arn:aws:identitystore::111122223333:identitystore/d-123456"
    },
    "source_entity_id": "SID-1234",
    "source_entity_type": "USER",
    "eventTimestamp": "1683355579981"
}
```

Convalida della conformità per IAM Identity Center

I revisori esterni valutano la sicurezza e la conformità di Servizi AWS tali sistemi nell' AWS IAM Identity Center ambito di più programmi di AWS conformità.

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Ambito per programma di conformitàServizi AWS di conformità e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.

- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Standard di conformità supportati

IAM Identity Center è stato sottoposto a controlli per i seguenti standard ed è idoneo all'uso come parte di soluzioni per le quali è necessario ottenere la certificazione di conformità.

	AWS ha ampliato il suo programma di conformità all'Healt h Insurance Portability and Accountability Act (HIPAA) per includere IAM Identity Center come servizio idoneo all'HIPAA. AWS offre un white paper incentrato sull'HIPAA per i clienti che desiderano saperne di più su come elaborare e archiviare le informazioni sanitarie. Servizi AWS Per ulteriori informazioni, consulta Compliance HIPAA.
	L'Information Security Registered Assessors Program (IRAP) consente ai clienti del governo australiano di garantire che siano in atto controlli di conformità appropria ti e di determinare il modello di responsabilità appropria to per soddisfare i requisiti dell'Australian Government Information Security Manual (ISM) prodotto dall'Australian Cyber Security Centre (ACSC). Per ulteriori informazioni, vedere IRAP Resources.
	IAM Identity Center dispone di un attestato di conformit à allo standard di sicurezza dei dati (DSS) PCI (Payment Card Industry) versione 3.2 al livello 1 del Service Provider. I clienti che utilizzano AWS prodotti e servizi per archiviar e, elaborare o trasmettere i dati dei titolari di carte possono utilizzare le seguenti fonti di identità in IAM Identity Center per gestire la propria certificazione di conformità PCI DSS: • Active Directory

	• Provider di identità esterno La fonte di identità IAM Identity Center attualmente non è conforme allo standard PCI DSS. Per ulteriori informazioni su PCI DSS, incluso come richiedere una copia del PCI AWS Compliance Package, vedere PCI DSS livello 1.
	I report System & Organization Control (SOC) sono rapporti di esame indipendenti di terze parti che dimostran o come IAM Identity Center raggiunge i controlli e gli obiettivi di conformità chiave. Questi report aiutano te e i tuoi auditor a capire in che modo i controlli supportano le operazioni e la conformità. Esistono tre tipi di report SOC: • AWS Rapporto SOC 1 - Scarica con Artifact AWS • AWS SOC 2: Rapporto su sicurezza, disponibilità e riservatezza - Scarica con AWS Artifact • AWS SOC 3: Rapporto su sicurezza, disponibilità e riservatezza IAM Identity Center rientra nell'ambito dei AWS report SOC 1, SOC 2 e SOC 3. Per ulteriori informazioni, consulta la pagina Conformità SOC.

Resilienza in IAM Identity Center

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta infrastruttura globale.AWS

Per ulteriori informazioni sulla AWS IAM Identity Center resilienza, consultaProgettazione della resilienza e comportamento regionale.

Sicurezza dell'infrastruttura in IAM Identity Center

In quanto servizio gestito, AWS IAM Identity Center è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere a IAM Identity Center attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Tagging delle risorse AWS IAM Identity Center

Un tag è un'etichetta di attributi personalizzata aggiunta a una risorsa AWS per semplificare l'identificazione, l'organizzazione e la ricerca delle risorse. Ogni tag è costituito da due parti:

- Una chiave del tag (ad esempio, `CostCenter`, `Environment` o `Project`). Le chiavi dei tag fanno distinzione tra maiuscole e minuscole e possono contenere fino a 128 caratteri.
- Un valore di tag (ad esempio, `111122223333` oppure `Production`). I valori dei tag fanno distinzione tra maiuscole e minuscole e possono contenere fino a 256 caratteri. È possibile impostare il valore di un tag su una stringa vuota, ma non su null. Non specificare il valore del tag equivale a utilizzare una stringa vuota.

I tag aiutano a identificare e a organizzare le risorse AWS. Molti servizi AWS supportano l'assegnazione di tag, perciò è possibile assegnare lo stesso tag a risorse di diversi servizi per indicare che queste sono correlate. Ad esempio, puoi assegnare lo stesso tag a un set di autorizzazioni specifico nella tua istanza di IAM Identity Center. Per ulteriori informazioni sulle strategie di tagging, consulta Tagging AWS Resources nella Riferimenti generali di AWSGuida e Tagging Best Practices.

Oltre a identificare, organizzare e tracciare AWS le risorse con i tag, puoi utilizzare i tag nelle policy IAM per controllare chi può visualizzare e interagire con le tue risorse. Per saperne di più sull'utilizzo dei tag per controllare l'accesso, consulta Controlling access to AWS resources using tags nella IAM User Guide. Ad esempio, puoi consentire a un utente di aggiornare un set di autorizzazioni IAM Identity Center, ma solo se il set di autorizzazioni IAM Identity Center ha un `owner` tag con un valore del nome di quell'utente.

Attualmente, puoi applicare i tag solo ai set di autorizzazioni. Non puoi applicare tag ai ruoli corrispondenti in cui IAM Identity Center creaAccount AWS. Puoi utilizzare la console IAM Identity Center AWS CLI o le API IAM Identity Center per aggiungere, modificare o eliminare i tag per un set di autorizzazioni.

Le seguenti sezioni forniscono ulteriori informazioni sui tag per IAM Identity Center.

Limitazioni applicate ai tag

Le seguenti restrizioni di base si applicano ai tag sulle risorse IAM Identity Center:

- Il numero massimo di tag che puoi assegnare a una risorsa è 50.
- La lunghezza massima della chiave è di 128 caratteri Unicode.
- La lunghezza massima del valore è di 256 caratteri Unicode.
- I caratteri validi per la chiave e il valore di un tag sono:

  a-z, A-Z, 0-9, spazio e i seguenti caratteri: _.:/= + - e @
- Per chiavi e valori viene fatta distinzione tra maiuscole e minuscole.
- Non utilizzare `aws:` come prefisso per le chiavi; l'utilizzo di questo prefisso è esclusivo di AWS

Gestisci i tag utilizzando la console IAM Identity Center

Puoi utilizzare la console IAM Identity Center per aggiungere, modificare e rimuovere i tag associati all'istanza o ai set di autorizzazioni.

Per gestire i tag dei set di autorizzazioni per una console IAM Identity Center

1. Apri la console IAM Identity Center.
2. Scegli Set di autorizzazioni.
3. Scegli il nome del set di autorizzazioni contenente i tag che desideri gestire.
4. Nella scheda Autorizzazioni, in Tag, esegui una delle seguenti operazioni, quindi procedi con il passaggio successivo:

   a. Se i tag sono già assegnati per questo set di autorizzazioni, scegli Modifica tag.

   b. Se non è assegnato alcun tag a questo set di autorizzazioni, scegli Aggiungi tag.
5. Per ogni nuovo tag, digita i valori nelle colonne Chiave e Valore (opzionale). Al termine, scegliere Save changes (Salva le modifiche).

Per rimuovere un tag, scegli la X nella colonna Rimuovi accanto al tag che desideri rimuovere.

Per gestire i tag per un'istanza di IAM Identity Center

1. Apri la console IAM Identity Center.
2. Seleziona Impostazioni.
3. Seleziona la scheda Tags (Tag).

4. Per ogni tag, digita i valori nei campi Chiave e Valore (opzionale). Quando hai finito, scegli il pulsante Aggiungi nuovo tag.

Per rimuovere un tag, scegli il pulsante Rimuovi accanto al tag che desideri rimuovere.

Esempi di AWS CLI

AWS CLIFornisce comandi che puoi usare per gestire i tag che assegni al tuo set di autorizzazioni.

Assegnazione di tag

Utilizzate i seguenti comandi per assegnare tag al set di autorizzazioni.

Example **`tag-resource`**Comando per un set di autorizzazioni

Assegna tag a un set di autorizzazioni utilizzando `tag-resource`all'interno del `sso` set di comandi:

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test
```

Questo comando include i seguenti parametri:

- `instance-arn`— L'Amazon Resource Name (ARN) dell'istanza IAM Identity Center in base alla quale verrà eseguita l'operazione.
- `resource-arn`— L'ARN della risorsa con i tag da elencare.
- `tags`: le coppie chiave-valore dei tag.

Per assegnare più tag in una sola volta, specificali in un elenco separato da virgole:

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

Visualizzazione dei tag

Utilizzate i seguenti comandi per visualizzare i tag assegnati al set di autorizzazioni.

Example **`list-tags-for-resource`**Comando per un set di autorizzazioni

Visualizza i tag assegnati a un set di autorizzazioni utilizzando `list-tags-for-resource`all'interno del `sso` set di comandi:

```
$ aws sso-admin list-tags-for-resource --resource-arn sso-resource-arn
```

Rimozione dei tag

Utilizzate i seguenti comandi per rimuovere i tag da un set di autorizzazioni.

Example **`untag-resource`**Comando per un set di autorizzazioni

Rimuovi i tag da un set di autorizzazioni utilizzando `untag-resource`all'interno del `sso` set di comandi:

```
$ aws sso-admin untag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tag-keys Stage CostCenter Owner
```

Per il parametro `--tag-keys`, specificare una o più chiavi di tag e non includere i valori di tag.

Applicazione di tag quando si crea un set di autorizzazioni

Utilizzate i seguenti comandi per assegnare i tag nel momento in cui create un set di autorizzazioni.

Example Comando **`create-permission-set`** con tag

Quando si crea un set di autorizzazioni utilizzando il `create-permission-set`comando, è possibile specificare i tag con il `--tags` parametro:

```
$ aws sso-admin create-permission-set \
> --instance-arn sso-instance-arn \
> --name permission=set-name \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

Gestisci i tag utilizzando l'API IAM Identity Center

Puoi utilizzare le seguenti azioni nell'API IAM Identity Center per gestire i tag per il tuo set di autorizzazioni.

Azioni API per i tag delle istanze di IAM Identity Center

Utilizza le seguenti azioni API per assegnare, visualizzare e rimuovere i tag per un set di autorizzazioni o un'istanza di IAM Identity Center.

- TagResource
- ListTagsForResource
- UntagResource
- CreatePermissionSet
- CreateInstance

Integrazione diAWSCLI con IAM Identity Center

AWSL'integrazione della Command Line Interface (CLI) versione 2 con IAM Identity Center semplifica il processo di accesso. Gli sviluppatori possono accedere direttamente alAWS CLIutilizzando le stesse credenziali di Active Directory o IAM Identity Center utilizzate normalmente per accedere a IAM Identity Center e accedere agli account e ai ruoli assegnati. Ad esempio, dopo che un amministratore ha configurato IAM Identity Center per l'utilizzo di Active Directory per l'autenticazione, uno sviluppatore può accedere alAWS CLIutilizzando direttamente le proprie credenziali Active Directory.

AWSL'integrazione di CLI con IAM Identity Center offre i seguenti vantaggi:

- Le aziende possono consentire ai propri sviluppatori di accedere utilizzando le credenziali di IAM Identity Center o Active Directory connettendo IAM Identity Center ad Active Directory tramiteAWS Directory Service.
- Gli sviluppatori possono accedere dalla CLI per un accesso più rapido.
- Gli sviluppatori possono elencare e passare da un account all'altro e ruoli a cui hanno assegnato l'accesso.
- Gli sviluppatori possono generare e salvare automaticamente profili di ruolo denominati nella loro configurazione CLI e fare riferimento a essi nella CLI per eseguire comandi negli account e nei ruoli desiderati.
- La CLI gestisce automaticamente le credenziali a breve termine in modo che gli sviluppatori possano iniziare e rimanere nella CLI in modo sicuro senza interruzioni ed eseguire script a esecuzione prolungata.

Come effettuare l'integrazione diAWSCLI con IAM Identity Center

Per utilizzare il pluginAWSIntegrazione di CLI con IAM Identity Center, è necessario scaricare, installare e configurareAWS Command Line Interfaceversione 2. Per passaggi dettagliati su come scaricare e integrare ilAWS CLIcon IAM Identity Center, vedereConfigurazione dellaAWSCLI per utilizzare IAM Identity CenternellaAWS Command Line InterfaceGuida per l'utente di.

AWS IAM Identity Center Disponibilità regionale

IAM Identity Center è disponibile in diverse versioni di uso comune Regioni AWS. Questa disponibilità semplifica la configurazione dell'accesso degli utenti a più Account AWS applicazioni aziendali. Quando gli utenti AWS accedono al portale di accesso, possono selezionare ciò Account AWS per cui dispongono delle autorizzazioni e quindi accedere a. AWS Management Console Per un elenco completo degli endpoint e delle Regioni AWS quote di IAM Identity Center supportati da IAM Identity Center.

Dati della regione IAM Identity Center

Quando abiliti per la prima volta IAM Identity Center, tutti i dati che configuri in IAM Identity Center vengono archiviati nella regione in cui li hai configurati. Questi dati includono configurazioni di directory, set di autorizzazioni, istanze di applicazioni e assegnazioni di utenti alle applicazioni. Account AWS Se utilizzi l'archivio di identità IAM Identity Center, anche tutti gli utenti e i gruppi che crei in IAM Identity Center vengono archiviati nella stessa regione. Ti consigliamo di installare IAM Identity Center in una regione che intendi mantenere disponibile per gli utenti, non in una regione che potresti dover disabilitare.

AWS Organizations ne supporta solo uno Regione AWS alla volta. Per abilitare IAM Identity Center in un'altra regione, devi prima eliminare la configurazione corrente di IAM Identity Center. Il passaggio a una regione diversa modifica anche l'URL del portale di AWS accesso ed è necessario riconfigurare tutti i set di autorizzazioni e le assegnazioni.

Chiamate tra regioni

IAM Identity Center utilizza Amazon Simple Email Service (Amazon SES) per inviare e-mail agli utenti finali quando tentano di accedere con una password monouso (OTP) come secondo fattore di autenticazione. Queste e-mail vengono inviate anche per determinati eventi di gestione di identità e credenziali, ad esempio quando l'utente viene invitato a configurare una password iniziale, a verificare un indirizzo e-mail e a reimpostare la password. Amazon SES è disponibile in un sottoinsieme di Regioni AWS quelli supportati da IAM Identity Center.

IAM Identity Center chiama gli endpoint locali di Amazon SES quando Amazon SES è disponibile localmente in un Regione AWS. Quando Amazon SES non è disponibile localmente, IAM Identity Center chiama gli endpoint Amazon SES in un altro modo Regione AWS, come indicato nella tabella seguente.

I codici regionali Amazon SES sono elencati nella tabella seguente.

Codice regionale IAM Identity Center	Nome della regione IAM Identity Center	Codice regionale Amazon SES	Nome della regione Amazon SES
us-gov-east-1	AWS GovCloud (Stati Uniti orientali)	us-gov-west-1	AWS GovCloud (Stati Uniti occidentali)
ap-east-1	Asia Pacifico (Hong Kong)	ap-northeast-2	Asia Pacifico (Seul)
ap-southeast-4	Asia Pacifico (Melbourne)	ap-southeast-2	Asia Pacifico (Sydney)
ap-south-2	Asia Pacific (Hyderabad)	ap-south-1	Asia Pacifico (Mumbai)
eu-central-2	Europa (Zurigo)	eu-central-1	Europa (Francoforte)
eu-south-2	Europa (Spagna)	eu-west-3	Europa (Parigi)
me-central-1	Medio Oriente (Emirati Arabi Uniti)	eu-central-1	Europa (Francoforte)

In queste chiamate interregionali, IAM Identity Center potrebbe inviare i seguenti attributi utente:

- Indirizzo e-mail
- Nome
- Cognome
- Account in AWS Organizations
- AWS accedere all'URL del portale
- Username
- ID della directory
- ID utente

Gestione di IAM Identity Center in una regione opzionale (regione disabilitata per impostazione predefinita)

La Regioni AWS maggior parte è abilitata per le operazioni in tutti i AWS servizi per impostazione predefinita. Quelli Le regioni vengono attivate automaticamente per l'uso con IAM Identity Center. Le seguenti Regioni AWS sono regioni opzionali e devi abilitarle:

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

Quando abiliti IAM Identity Center per un account di gestione in un opt-in Regione AWS, i seguenti metadati IAM Identity Center per tutti gli account membro vengono archiviati nella regione.

- ID account
- Account name (Nome account)
- Email dell'account
- Amazon Resource Names (ARN) dei ruoli IAM creati da IAM Identity Center nell'account del membro

Se disabiliti una regione in cui è installato IAM Identity Center, viene disabilitato anche IAM Identity Center. Dopo che IAM Identity Center è stato disabilitato in una regione, gli utenti di quella regione non avranno accesso Single Sign-On Account AWS alle applicazioni. AWS conserva i dati nella configurazione di IAM Identity Center per almeno 10 giorni. Se riattivi IAM Identity Center entro questo lasso di tempo, i dati di configurazione di IAM Identity Center saranno ancora disponibili nella regione.

Per riattivare IAM Identity Center in modalità opt-in Regioni AWS, devi riattivare la regione. Poiché IAM Identity Center deve rielaborare nuovamente tutti gli eventi in pausa, la riattivazione di IAM Identity Center potrebbe richiedere del tempo.

> **Note**
>
> IAM Identity Center può gestire l'accesso solo a Account AWS quelli abilitati all'uso in un. Regione AWS Per gestire l'accesso a tutti gli account della tua organizzazione, abilita IAM Identity Center nell'account di gestione in un account Regione AWS che viene attivato automaticamente per l'uso con IAM Identity Center.

Per ulteriori informazioni sull'attivazione e la disabilitazione Regioni AWS, consulta Managing Regioni AWS nella Guida AWS generale.

Elimina la configurazione di IAM Identity Center

Quando una configurazione IAM Identity Center viene eliminata, tutti i dati in quella configurazione vengono eliminati e non possono essere recuperati. La tabella seguente descrive quali dati vengono eliminati in base al tipo di directory attualmente configurato in IAM Identity Center.

Quali dati vengono eliminati	Directory connessa (AWS Managed Microsoft AD o AD Connector)	Archivio di identità IAM Identity Center
Tutti i set di autorizzazioni per cui hai configurato Account AWS	✓	✓
Tutte le applicazioni che hai configurato in IAM Identity Center	✓	✓
Tutte le assegnazioni utente Account AWS e le applicazioni che hai configurato	✓	✓

Quali dati vengono eliminati	Directory connessa (AWS Managed Microsoft AD o AD Connector)	Archivio di identità IAM Identity Center
Tutti gli utenti e i gruppi presenti nella directory o nell'archivio	N/D	✓

Utilizza la seguente procedura quando devi eliminare la configurazione corrente di IAM Identity Center.

Per eliminare la configurazione di IAM Identity Center

1. Apri la console IAM Identity Center.
2. Nel riquadro di navigazione a sinistra scegliere Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Gestione.
4. Nella sezione Elimina la configurazione di IAM Identity Center, scegli Elimina.
5. Nella finestra di dialogo Elimina la configurazione di IAM Identity Center, seleziona ciascuna casella di controllo per confermare di aver compreso che i dati verranno eliminati. Digita la tua istanza IAM Identity Center nella casella di testo, quindi scegli Conferma.

AWS IAM Identity Center quote

Le tabelle seguenti descrivono le quote all'interno di IAM Identity Center. Le richieste di aumento delle quote devono provenire da un account di gestione o amministratore delegato. Per aumentare una quota, vedere Richiesta di aumento della quota.

> **Note**
>
> Ti consigliamo di utilizzare la AWS CLI e le API se hai più di 50.000 utenti, 10.000 gruppi o 500 set di autorizzazioni. Per ulteriori informazioni sulla CLI, vedere. Integrazione diAWSCLI con IAM Identity Center Per ulteriori informazioni sulle API, consulta Welcome to the IAM Identity Center API Reference.

Quote delle applicazioni

Risorsa	Quota predefinita	Può essere aumentata
La dimensione del file dei certificati SAML del provider di servizi (in formato PEM)	2 KB	No
Limite di asserzioni SAML	50.000 caratteri	No
Limite di dimensione del file del certificato IdP caricato su IAM Identity Center	2500 caratteri (UTF-8)	No
Ambiti di accesso per applicazione	25	No

Account AWS quote

Risorsa	Quota predefinita	Può essere aumentata
Numero dei set di autorizza zioni consentiti in IAM Identity Center	2000	Sì
Numero di set di autorizza zioni predisposti consentiti per Account AWS	250	Sì
Il numero di policy inline per set di autorizzazioni	1	No
Numero di politiche AWS gestite e gestite dai clienti per set di autorizzazioni	20 [1]	No
La dimensione massima della policy inline per un set di autorizzazioni	32.768 byte. La dimensione massima dei caratteri diversi dagli spazi bianchi nella policy in linea per set di autorizzazioni è di 10.240 byte.	No
Numero di ruoli IAM (set di autorizzazioni) che possono essere aggiornati contempor aneamente Account AWS	1	No

[1]AWS Identity and Access Management (IAM) stabilisce una quota di 10 policy gestite per ruolo. Per sfruttare questa quota, richiedi un aumento della quota IAM Managed policy allegate a un ruolo IAM nella console Service Quotas per ciascuna delle aree in Account AWS cui desideri distribuire il set di autorizzazioni.

> **Note**
>
> Set di autorizzazionivengono forniti Account AWS come ruoli IAM o utilizzano ruoli IAM esistenti in e quindi seguono le Account AWSquote IAM. Per ulteriori informazioni sulle quote associate ai ruoli IAM, consulta Quote IAM e STS.

Quote Active Directory

Risorsa	Quota predefinita	Può essere aumentata
Numero di directory connesse che è possibile avere in una volta	1	No

Quote di archiviazione delle identità di IAM Identity Center

Risorsa	Quota predefinita	Può essere aumentata
Numero di utenti supportati in IAM Identity Center	100000	Sì
Numero di gruppi supportati in IAM Identità Center	100000	No
Numero di gruppi univoci che possono essere utilizzati per valutare le autorizzazioni per un utente	1000	No

Limiti di limitazione di IAM Identity Center

Risorsa	Quota predefinita
API IAM Identity Center	Le API IAM Identity Center hanno un limite massimo di 20 transazioni al secondo (TPS). CreateAccountAssignmentHa una frequenza massima di 10 chiamate asincrone in sospeso. Queste quote non possono essere modificate.

Quote aggiuntive

Risorsa	Quota predefinita	Può essere aumentata
Numero totale di Account AWS o applicazioni che possono essere configurate*	3000	Sì
Numero totale di istanze di IAM Identity Center per account	1	No
Numero totale di emittenti di token affidabili	10	No

* Sono Account AWS supportate fino a 3000 applicazioni (totale combinato). Ad esempio, puoi configurare 2750 account e 250 applicazioni, per un totale di 3000 account e applicazioni.

Risoluzione dei problemi relativi a IAM Identity Center

Quanto segue può aiutarti a risolvere alcuni problemi comuni che potresti riscontrare durante la configurazione o l'utilizzo della console IAM Identity Center.

Problemi di creazione di un'istanza di account di IAM Identity Center

Potrebbero essere applicate diverse restrizioni durante la creazione di un'istanza di account di IAM Identity Center. Se non riesci a creare un'istanza di account tramite la console IAM Identity Center o l'esperienza di configurazione di un'applicazione AWS gestita supportata, verifica i seguenti casi d'uso:

- Regioni AWS Controllane altri Account AWS nell'istanza in cui stai tentando di creare l'account. Sei limitato a un'istanza di IAM Identity Center per. Account AWS Per abilitare l'applicazione, passa all'istanza Regione AWS con l'istanza di IAM Identity Center o passa a un account senza un'istanza di IAM Identity Center.
- Se la tua organizzazione ha abilitato IAM Identity Center prima del 14 settembre 2023, l'amministratore potrebbe dover attivare la creazione dell'istanza dell'account. Collabora con il tuo amministratore per abilitare la creazione dell'istanza dell'account dalla console IAM Identity Center nell'account di gestione.
- L'amministratore potrebbe aver creato una policy di controllo dei servizi per limitare la creazione di istanze di account di IAM Identity Center. Collabora con il tuo amministratore e aggiungi il tuo account all'elenco degli account consentiti.

Ricevi un errore quando tenti di visualizzare l'elenco delle applicazioni cloud preconfigurate per funzionare con IAM Identity Center

Il seguente errore si verifica quando si dispone di una policy che consente `sso:ListApplications` ma non altre API IAM Identity Center. Aggiorna la tua policy per risolvere questo errore.

L'`ListApplications`autorizzazione autorizza più API:

- L'`ListApplications`API.

- Un'API interna simile all'`ListApplicationProviders`API utilizzata nella console IAM Identity Center.

Per aiutare a risolvere la duplicazione, l'API interna ora autorizza anche l'uso dell'`ListApplicationProviders`azione. Per consentire l'`ListApplications`API pubblica ma negare l'API interna, la policy deve includere una dichiarazione che neghi l'azione: `ListApplicationProviders`

```
      "Statement": [
    {
         "Effect": "Deny",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "ListApplications",
        "Resource": "<instanceArn>" // (or "*" for all instances)
    }
]
```

Per consentire l'API interna ma negarla`ListApplications`, la policy deve solo consentire. `ListApplicationProviders` L'`ListApplications`API viene negata se non è esplicitamente consentita.

```
      "Statement": [
    {
         "Effect": "Allow",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    }
]
```

Una volta aggiornate le politiche, contattateci AWS Support per far rimuovere questa misura proattiva.

Problemi relativi al contenuto delle asserzioni SAML create da IAM Identity Center

IAM Identity Center offre un'esperienza di debug basata sul Web per le asserzioni SAML create e inviate da IAM Identity Center, inclusi gli attributi all'interno di queste asserzioni, durante l'accesso Account AWS e le applicazioni SAML dal portale di accesso. AWS Per visualizzare i dettagli di un'asserzione SAML generata da IAM Identity Center, utilizza i seguenti passaggi.

1. Accedi al portale di AWS accesso.
2. Mentre sei connesso al portale, tieni premuto il tasto Maiusc, scegli il riquadro dell'applicazione, quindi rilascia il tasto Shift.
3. Esamina le informazioni contenute nella pagina intitolata You are now in administrator mode (Si è ora in modalità amministratore). Per conservare queste informazioni per future consultazioni, scegliete Copia XML e incollate il contenuto altrove.
4. Scegliete Invia a <application>per continuare. Questa opzione invia l'asserzione al fornitore di servizi.

> **Note**
>
> Alcune configurazioni del browser e dei sistemi operativi potrebbero non supportare questa procedura. Questa procedura è stata testata su Windows 10 utilizzando i browser Firefox, Chrome ed Edge.

Alcuni utenti non riescono a sincronizzarsi in IAM Identity Center da un provider SCIM esterno

Se la sincronizzazione SCIM riesce per un sottoinsieme di utenti configurati nel tuo IdP per il provisioning in IAM Identity Center ma fallisce per altri, potresti visualizzare un errore simile a quello del tuo provider di identità. `'Request is unparsable, syntactically incorrect, or violates schema'` È inoltre possibile visualizzare messaggi dettagliati di errore di provisioning in. AWS CloudTrail

Questo problema spesso indica che l'utente del tuo IdP è configurato in un modo non supportato da IAM Identity Center. I dettagli completi dell'implementazione SCIM di IAM Identity Center, comprese

le specifiche dei parametri e delle operazioni obbligatori, opzionali e proibiti per gli oggetti utente, sono disponibili nella IAM Identity Center SCIM Implementation Developer Guide. La SCIM Developer Guide deve essere considerata autorevole per le informazioni sui requisiti SCIM. Tuttavia, le seguenti sono alcune delle cause più comuni di questo errore:

1. L'oggetto utente nell'IdP non ha un nome (dato), un cognome (di famiglia) e/o un nome visualizzato.

   - Soluzione: aggiungi un nome (dato), un cognome (famiglia) e un nome visualizzato per l'oggetto utente. Inoltre, assicurati che i mapping di provisioning SCIM per gli oggetti utente del tuo IdP siano configurati per inviare valori non vuoti per tutti questi attributi.

2. All'utente viene inviato più di un valore per un singolo attributo (noti anche come «attributi multivalore»). Ad esempio, l'utente può avere sia un numero di telefono aziendale che uno di casa specificato nell'IdP oppure più e-mail o indirizzi fisici e l'IdP è configurato per provare a sincronizzare più o tutti i valori per quell'attributo.

   - Opzioni di soluzione:

     i. Aggiorna le mappature di provisioning SCIM per gli oggetti utente presso il tuo IdP per inviare un solo valore per un determinato attributo. Ad esempio, configura una mappatura che invii solo il numero di telefono di lavoro per ogni utente.

     ii. Se gli attributi aggiuntivi possono essere rimossi in modo sicuro dall'oggetto utente nell'IdP, è possibile rimuovere i valori aggiuntivi, lasciando uno o zero valori impostati per quell'attributo per l'utente.

     iii. Se l'attributo non è necessario per alcuna azione in AWS, rimuovi la mappatura per quell'attributo dalle mappature di provisioning SCIM per gli oggetti utente del tuo IdP.

3. Il tuo IdP sta cercando di abbinare gli utenti nel target (IAM Identity Center, in questo caso) in base a più attributi. Poiché i nomi utente sono garantiti in modo univoco all'interno di una determinata istanza di IAM Identity Center, è sufficiente specificare `username` come attributo utilizzato per la corrispondenza.

   - Soluzione: assicurati che la configurazione SCIM nel tuo IdP utilizzi un solo attributo per la corrispondenza con gli utenti in IAM Identity Center. Ad esempio, la mappatura `username` o `userPrincipalName` nell'IdP all'attributo in SCIM per `userName` il provisioning a IAM Identity Center sarà corretta e sufficiente per la maggior parte delle implementazioni.

Gli utenti non possono accedere se il loro nome utente è in formato UPN

Gli utenti potrebbero non essere in grado di AWS accedere al portale di accesso in base al formato utilizzato per immettere il proprio nome utente nella pagina di accesso. Per la maggior parte, gli utenti possono accedere al portale utenti utilizzando il proprio nome utente semplice, il nome di accesso di livello inferiore (DOMAIN\UserName) o il nome di accesso UPN (). `UserName@Corp.Example.com` L'eccezione si verifica quando IAM Identity Center utilizza una directory connessa che è stata abilitata con MFA e la modalità di verifica è stata impostata su Context-aware o Always-on. In questo scenario, gli utenti devono accedere con il proprio nome di accesso di livello inferiore (DOMAIN\). UserName Per ulteriori informazioni, consulta Autenticazione a più fattori per gli utenti di Identity Center. Per informazioni generali sui formati dei nomi utente utilizzati per accedere ad Active Directory, vedere Formati dei nomi utente nel sito Web della documentazione Microsoft.

Ricevo l'errore «Impossibile eseguire l'operazione sul ruolo protetto» durante la modifica di un ruolo IAM

Quando esamini i ruoli IAM in un account, potresti notare che i nomi dei ruoli iniziano con '_'. AWSReservedSSO Questi sono i ruoli che il servizio IAM Identity Center ha creato nell'account e derivano dall'assegnazione di un set di autorizzazioni all'account. Il tentativo di modificare questi ruoli dall'interno della console IAM genererà il seguente errore:

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoleName_Here' -
 this role is only modifiable by AWS'
```

Questi ruoli possono essere modificati solo dalla console di amministrazione di IAM Identity Center, che si trova nell'account di gestione di AWS Organizations. Una volta modificato, puoi quindi trasferire le modifiche agli AWS account a cui è assegnato.

Gli utenti della Directory non possono reimpostare la propria password

Quando un utente della directory reimposta la propria password utilizzando la password dimenticata? opzione durante l'accesso al portale di AWS accesso, la nuova password deve rispettare la politica di password predefinita descritta in. Requisiti relativi alle password per la gestione delle identità in IAM Identity Center

Se un utente inserisce una password conforme alla politica e poi riceve l'errore`We couldn't update your password`, controlla se AWS CloudTrail ha registrato l'errore. Questo può essere fatto effettuando una ricerca nella console Event History o CloudTrail utilizzando il seguente filtro:

```
"UpdatePassword"
```

Se il messaggio indica quanto segue, potrebbe essere necessario contattare l'assistenza:

```
"errorCode": "InternalFailure",
      "errorMessage": "An unknown error occurred“
```

Un'altra possibile causa di questo problema è la convenzione di denominazione applicata al valore del nome utente. Le convenzioni di denominazione devono seguire schemi specifici come «cognome.givenname». Tuttavia, alcuni nomi utente possono essere piuttosto lunghi o contenere caratteri speciali e ciò può causare l'eliminazione di caratteri nella chiamata API, con conseguente errore. Potresti provare a reimpostare la password con un utente di prova nello stesso modo per verificare se questo è il caso.

Se il problema persiste, contatta il AWS Support Center.

Il mio utente è referenziato in un set di autorizzazioni ma non può accedere agli account o alle applicazioni assegnati

Questo problema può verificarsi se si utilizza System for Cross-domain Identity Management (SCIM) per il provisioning automatico con un provider di identità esterno. In particolare, quando un utente o il gruppo di cui l'utente era membro viene eliminato e poi ricreato utilizzando lo stesso nome utente (per gli utenti) o lo stesso nome (per i gruppi) nel provider di identità, viene creato un nuovo identificatore interno univoco per il nuovo utente o gruppo in IAM Identity Center. Tuttavia, IAM Identity Center ha ancora un riferimento al vecchio identificatore nel suo database delle autorizzazioni, in modo che il nome dell'utente o del gruppo appaia ancora nell'interfaccia utente, ma l'accesso fallisce. Questo perché l'ID utente o di gruppo sottostante a cui fa riferimento l'interfaccia utente non esiste più.

Per ripristinare Account AWS l'accesso in questo caso, puoi rimuovere l'accesso per il vecchio utente o gruppo dai luoghi in cui era stato originariamente assegnato e quindi riassegnare l'accesso all'utente o al gruppo. Account AWS Ciò aggiorna il set di autorizzazioni con l'identificatore corretto per il nuovo utente o gruppo. Analogamente, per ripristinare l'accesso all'applicazione, è possibile rimuovere l'accesso per l'utente o il gruppo dall'elenco degli utenti assegnati a quell'applicazione, quindi aggiungere nuovamente l'utente o il gruppo.

È inoltre possibile verificare se l'errore è AWS CloudTrail stato registrato cercando CloudTrail nei registri gli eventi di sincronizzazione SCIM che fanno riferimento al nome dell'utente o del gruppo in questione.

Non riesco a configurare correttamente la mia applicazione dal catalogo delle applicazioni

Se hai aggiunto un'applicazione dal catalogo delle applicazioni in IAM Identity Center, tieni presente che ogni fornitore di servizi fornisce la propria documentazione dettagliata. È possibile accedere a queste informazioni dalla scheda Configurazione dell'applicazione nella console IAM Identity Center.

Se il problema è legato alla configurazione della fiducia tra l'applicazione del provider di servizi e IAM Identity Center, assicurati di consultare il manuale di istruzioni per la risoluzione dei problemi.

Errore «Si è verificato un errore imprevisto» quando un utente tenta di accedere utilizzando un provider di identità esterno

Questo errore può verificarsi per diversi motivi, ma uno dei motivi più comuni è la mancata corrispondenza tra le informazioni sull'utente contenute nella richiesta SAML e le informazioni relative all'utente in IAM Identity Center.

Affinché un utente IAM Identity Center possa accedere correttamente quando utilizza un IdP esterno come origine dell'identità, deve essere vero quanto segue:

- Il formato SAML NameID (configurato presso il tuo provider di identità) deve essere 'email'
- Il valore NameID deve essere una stringa formattata correttamente (RFC2822) (user@domain.com)
- Il valore NameID deve corrispondere esattamente al nome utente di un utente esistente in IAM Identity Center (non importa se l'indirizzo e-mail in IAM Identity Center corrisponde o meno: la corrispondenza in entrata si basa sul nome utente)
- L'implementazione IAM Identity Center della federazione SAML 2.0 supporta solo 1 asserzione nella risposta SAML tra il provider di identità e IAM Identity Center. Non supporta asserzioni SAML crittografate.
- Le seguenti istruzioni si applicano se Attributi per il controllo degli accessi è abilitata nel tuo account IAM Identity Center:

- Il numero di attributi mappati nella richiesta SAML deve essere pari o inferiore a 50.
- La richiesta SAML non deve contenere attributi multivalore.
- La richiesta SAML non deve contenere più attributi con lo stesso nome.
- L'attributo non deve contenere XML strutturato come valore.
- Il formato del nome deve essere un formato specificato da SAML, non un formato generico.

> **Note**
>
> IAM Identity Center non esegue la creazione «just in time» di utenti o gruppi per nuovi utenti o gruppi tramite la federazione SAML. Ciò significa che l'utente deve essere pre-creato in IAM Identity Center, manualmente o tramite provisioning automatico, per poter accedere a IAM Identity Center.

Questo errore può verificarsi anche quando l'endpoint Assertion Consumer Service (ACS) configurato nel tuo provider di identità non corrisponde all'URL ACS fornito dall'istanza IAM Identity Center. Assicurati che questi due valori corrispondano esattamente.

Inoltre, puoi risolvere ulteriormente gli errori di accesso con provider di identità esterni accedendo AWS CloudTrail e filtrando il nome dell'evento P. ExternalId DirectoryLogin

Errore «Impossibile abilitare gli attributi per il controllo degli accessi»

Questo errore può verificarsi se l'utente che abilita ABAC non dispone delle `iam:UpdateAssumeRolePolicy` autorizzazioni necessarie per l'attivazione. Attributi per il controllo degli accessi

Ricevo il messaggio «Browser non supportato» quando tento di registrare un dispositivo per l'MFA

WebAuthn è attualmente supportato nei browser Web Google Chrome, Mozilla Firefox, Microsoft Edge e Apple Safari, nonché nelle piattaforme Windows 10 e Android. Alcuni componenti del WebAuthn supporto possono variare, ad esempio il supporto di Platform Authenticator nei browser

macOS e iOS. Se gli utenti tentano di registrare WebAuthn dispositivi su un browser o una piattaforma non supportati, vedranno alcune opzioni non supportate in grigio oppure riceveranno un messaggio di errore indicante che non tutti i metodi supportati sono supportati. In questi casi, fate riferimento a FIDO2: Web Authentication (WebAuthn) per ulteriori informazioni sul supporto del browser/piattaforma. Per ulteriori informazioni su IAM Identity Center WebAuthn , consulta. Autenticatori FIDO2

Il gruppo «Domain Users» di Active Directory non si sincronizza correttamente con IAM Identity Center

Il gruppo Active Directory Domain Users è il «gruppo primario» predefinito per gli oggetti utente AD. I gruppi primari di Active Directory e le relative appartenenze non possono essere letti da IAM Identity Center. Quando assegni l'accesso alle risorse o alle applicazioni IAM Identity Center, utilizza gruppi diversi dal gruppo Domain Users (o altri gruppi assegnati come gruppi primari) per far sì che l'appartenenza al gruppo rifletta correttamente nell'archivio di identità di IAM Identity Center.

Errore di credenziali MFA non valide

Questo errore può verificarsi quando un utente tenta di accedere a IAM Identity Center utilizzando un account di un provider di identità esterno (ad esempio, Okta oMicrosoft Entra ID) prima che il proprio account sia completamente fornito a IAM Identity Center utilizzando il protocollo SCIM. Dopo aver effettuato il provisioning dell'account utente su IAM Identity Center, questo problema dovrebbe essere risolto. Verifica che l'account sia stato fornito a IAM Identity Center. In caso contrario, controlla i registri di provisioning nel provider di identità esterno.

Ricevo il messaggio «Si è verificato un errore imprevisto» quando tento di registrarmi o accedere utilizzando un'app di autenticazione

I sistemi con password monouso (TOTP) basati sul tempo, come quelli utilizzati da IAM Identity Center in combinazione con app di autenticazione basate su codice, si basano 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 (https://www.time.gov/) o altri equivalenti locali/regionali.

Ricevo l'errore «Non sei tu, siamo noi» quando tento di accedere a 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 IAM Identity Center 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 impostare la data e l'ora in modo che vengano impostate automaticamente. Se ciò 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 IdP. Puoi controllare il certificato dalla console IAM Identity Center accedendo a Impostazioni. Nella scheda Identity Source scegli Azione, quindi scegli Gestisci autenticazione. Se i certificati IdP e IAM Identity Center non corrispondono, importa un nuovo certificato in IAM Identity Center.
- Assicurati che il formato NameID nel file di metadati del tuo provider di identità sia il seguente:
  - `urn:oasis:name:tc:SAML:1.1:nameid-format:emailAddress`
- Se utilizzi AD Connector AWS Directory Service come provider di identità, 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 AWS Directory Service.

I miei utenti non ricevono e-mail da IAM Identity Center

Tutte le e-mail inviate dal servizio IAM Identity Center proverranno dall'indirizzo `no-reply@signin.aws` o `no-reply@login.awsapps.com`. Il tuo sistema di posta deve essere configurato in modo da accettare le e-mail da questi indirizzi e-mail del mittente e non gestirle come posta indesiderata o spam.

Errore: non è possibile delete/modify/remove/assign l'accesso ai set di autorizzazioni forniti nell'account di gestione

Questo messaggio indica che la Amministrazione delegata funzionalità è stata abilitata e che l'operazione tentata in precedenza può essere eseguita correttamente solo da qualcuno che dispone delle autorizzazioni per l'account di gestione. AWS Organizations Per risolvere il problema, accedi

come utente con queste autorizzazioni e prova a eseguire nuovamente l'attività o assegnala a qualcuno che dispone delle autorizzazioni corrette. Per ulteriori informazioni, consulta Registra un account membro.

Errore: token di sessione non trovato o non valido

Questo errore può verificarsi quando un client, ad esempio un browser Web, o Kit di strumenti AWS AWS CLI, tenta di utilizzare una sessione revocata o invalidata sul lato server. Per risolvere il problema, torna all'applicazione client o al sito Web e riprova, effettuando nuovamente l'accesso, se richiesto. A volte ciò potrebbe richiedere l'annullamento anche delle richieste in sospeso, ad esempio un tentativo di connessione in sospeso dall'interno dell' Kit di strumenti AWS IDE.

Cronologia dei documenti

La tabella seguente descrive importanti aggiunte alla AWS IAM Identity Center documentazione. Inoltre, aggiorniamo frequentemente la documentazione tenendo conto dei feedback ricevuti.

- Ultimo aggiornamento importante della documentazione: 23 settembre 2022

Modifica	Descrizione	Data
Aggiornamenti per la politica AWS gestita	Autorizzazioni aggiornate per la politica `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gestita.	17 maggio 2024
Aggiornamenti per la politica AWS gestita	Autorizzazioni aggiornate per la politica `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gestita.	30 aprile 2024
Aggiornamenti per la politica AWS gestita	Autorizzazioni aggiornate per la politica `AWSSSOMasterAccountAdministrator` AWS gestita.	26 aprile 2024
Aggiornamenti per la politica AWS gestita	Autorizzazioni aggiornate per la politica `AWSSSOMemberAccountAdministrator` AWS gestita.	26 aprile 2024
Aggiornamenti per la politica AWS gestita	Autorizzazioni aggiornate per la politica `AWSSSOReadOnly` AWS gestita.	26 aprile 2024
Aggiornamenti per la politica AWS gestita	Autorizzazioni aggiornate per la politica `AWSIAMIde`	26 aprile 2024

	`ntityCenterAllowLi stForIdentityConte xt` AWS gestita.	
Aggiornamenti per la politica AWS gestita	Autorizzazioni aggiornate per la politica `AWSIAMIde ntityCenterAllowLi stForIdentityConte xt` AWS gestita.	24 aprile 2024
Aggiornamenti per la politica AWS gestita	Autorizzazioni aggiornate per la politica `AWSIAMIde ntityCenterAllowLi stForIdentityConte xt` AWS gestita.	19 aprile 2024
Aggiornamenti per la politica AWS gestita	Autorizzazioni aggiornate per la politica `AWSIAMIde ntityCenterAllowLi stForIdentityConte xt` AWS gestita.	11 aprile 2024
Aggiornamenti per la politica AWS gestita	Autorizzazioni aggiornate per la politica `AWSIAMIde ntityCenterAllowLi stForIdentityConte xt` AWS gestita.	26 novembre 2023
Nuovo argomento relativo alla politica AWS gestita	Sono stati aggiunti dettagli per la politica `AWSIAMIde ntityCenterAllowLi stForIdentityConte xt` AWS gestita.	15 novembre 2023
Linee guida avanzate per iniziare a usare IAM Identity Center	Sono stati aggiunti nuovi contenuti per iniziare a usare IAM Identity Center e creare un utente amministrativo	23 settembre 2022

Utenti e gruppi aggiornati nell'Identity Center API Reference	Questo aggiornamento include riferimenti alle nuove API di creazione, aggiornamento ed eliminazione nella Guida di riferimento dell'API Identity Center.	31 agosto 2022
AWS Single Sign-On (AWS SSO) rinominato in IAM Identity Center AWS	AWS introduce. AWS IAM Identity Center IAM Identity Center amplia le funzionalità di AWS Identity and Access Management (IAM) per aiutarti a gestire centralmente l'account e l'accesso alle applicazioni per gli utenti della tua forza lavoro. Le funzionalità di IAM Identity Center includono l'assegnazione delle applicazioni, le autorizzazioni per più account e un portale di accesso. AWS	26 luglio 2022
Support per i limiti delle autorizzazioni e le politiche gestite dai clienti nei set di autorizzazioni	Contenuti aggiunti per l'utilizzo di politiche AWS gestite e gestite dai clienti AWS Identity and Access Management (IAM) con set di autorizzazioni.	14 luglio 2022
Support per AWS regioni abilitate manualmente	Contenuti aggiunti per l'utilizzo di IAM Identity Center in regioni abilitate manualmente.	15 giugno 2022
Aggiornamenti per le politiche AWS gestite	Autorizzazioni aggiornate per la politica `AWSSSOServiceRolePolicy` AWS gestita.	11 maggio 2022

Support per l'amministrazione delegata	Contenuto aggiunto per la funzionalità di amministrazione delegata.	11 maggio 2022
Aggiornamenti per le politiche AWS gestite	Autorizzazioni aggiornate per e politiche `AWSSSOReadOnly` AWS gestite. `AWSSSOMasterAccountAdministrator` `AWSSSOMemberAccountAdministrator`	28 aprile 2022
Support per la sincronizzazione AD configurabile	Contenuto aggiunto per la funzionalità di sincronizzazione AD configurabile.	14 aprile 2022
Nuovo argomento relativo alla politica AWS gestita	Sono stati aggiunti dettagli per la politica `AWSSSOMasterAccountAdministrator` AWS gestita.	4 agosto 2021
Aggiornamenti per le quote	Adeguamenti alle tabelle delle quote.	21 dicembre 2020
Nuove politiche di esempio	Sono stati aggiunti nuovi esempi di policy gestite dai clienti e aggiornamenti alla sezione relativa alle autorizzazioni richieste.	21 dicembre 2020
Support per il controllo degli accessi basato sugli attributi (ABAC)	Contenuto aggiunto per la funzionalità ABAC.	24 novembre 2020
Support per l'iscrizione forzata alla MFA	Aggiornamenti per richiedere agli utenti di registrare un dispositivo MFA al momento dell'accesso.	23 novembre 2020

Support per WebAuthn	Contenuti aggiunti per nuove WebAuthn funzionalità.	20 novembre 2020
Support per Ping Identity	Contenuto aggiunto da integrare con Ping Identity i prodotti come provider di identità esterno supportato.	26 ottobre 2020
Support per OneLogin	Contenuto aggiunto da integrare OneLogin come provider di identità esterno supportato.	31 luglio 2020
Supporto perOkta	Contenuto aggiunto da integrare Okta come provider di identità esterno supportato.	28 maggio 2020
Support per provider di identità esterni	Riferimenti modificati dalla directory alla fonte di identità, contenuto aggiunto per supportare provider di identità esterni.	26 novembre 2019
Nuove impostazioni MFA	È stato rimosso l'argomento relativo alla verifica in due passaggi e al suo posto è stato aggiunto un nuovo argomento MFA.	24 ottobre 2019
Nuova impostazione per aggiungere la verifica in due passaggi	Sono stati aggiunti contenuti su come abilitare la verifica in due passaggi per gli utenti.	16 gennaio 2019
Support per la durata della sessione sugli AWS account	Aggiunti contenuti su come impostare la durata della sessione per un AWS account.	30 ottobre 2018

Nuova opzione per utilizzare la directory Identity Center	Contenuto aggiunto per la scelta della directory Identity Center o per la connessione a una directory esistente in Active Directory.	17 ottobre 2018
Support per lo stato di inoltro e la durata della sessione sulle applicazioni	Aggiunti contenuti sullo stato di inoltro e sulla durata della sessione per le applicazioni.	10 ottobre 2018
Supporto aggiuntivo per nuove applicazioni	Aggiunto 4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvaInSync, Egnyte, Engagedly, Expensify, Freshdesk, IdeaScale, Igloo, Jitbit, Kudos, LiquidFiles, Lucidchart, PurelyHR, Samanage, ScreenSteps, Sli.do, SmartSheet, Syncplicity, TalentLMS, Trello, UserVoice, Zoho, OpsGenie, DigiCert, WeekDone, ProdPad, e UserEcho al catalogo delle applicazioni.	3 agosto 2018
Support per l'accesso multiaccount agli account di gestione	Sono stati aggiunti contenuti su come delegare l'accesso a più account agli utenti in un account di gestione.	9 luglio 2018
Support per nuove applicazioni	Aggiunto DocuSign, Keeper Security, e aggiunto SugarCRM al catalogo delle applicazioni.	16 marzo 2018

Ottieni credenziali temporanee per l'accesso alla CLI	Sono state aggiunte informazioni su come ottenere credenziali temporanee per eseguire i comandi. AWS CLI	22 febbraio 2018
Nuova guida	Questa è la prima versione della IAM Identity Center User Guide.	7 dicembre 2017

Glossario AWS

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

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.