



Guida per l'utente

AWS IAM Identity Center



AWS IAM Identity Center: Guida per l'utente

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Cos'è il Centro identità IAM?	1
Perché usare IAM Identity Center?	1
Rinomina di IAM Identity Center	3
Nessuna modifica ai namespace legacy	3
Nozioni di base	4
Prerequisiti e considerazioni di IAM Identity Center	6
Scelta di un Regione AWS	7
Utilizzo di IAM Identity Center solo per applicazioni	14
Ruoli IAM creati da IAM Identity Center	14
IAM Identity Center e AWS Organizations	15
Istanze IAM Identity Center	16
Account AWS tipi che possono abilitare IAM Identity Center	17
Istanze organizzative di IAM Identity Center	18
Istanze account del Centro identità IAM	19
Elimina la tua istanza IAM Identity Center	24
Abilita IAM Identity Center	26
Per abilitare un'istanza di IAM Identity Center	27
Conferma le tue fonti di identità	30
Aggiorna firewall e gateway	32
Considerazioni sulla possibilità di inserire nella lista domini ed endpoint URL	34
Tutorial sulle fonti di identità	36
Active Directory	37
CyberArk	39
Prerequisiti	40
Considerazioni SCIM	41
Fase 1: abilitare il provisioning in IAM Identity Center	42
Fase 2: Configurare il provisioning in CyberArk	42
(Facoltativo) Fase 3: Configurazione degli attributi utente in ABAC (CyberArkfor access control) in IAM Identity Center	43
(Facoltativo) Passaggio di attributi per il controllo degli accessi	44
Google Workspace	45
Considerazioni	46
Passaggio 1Google Workspace: configurare l'applicazione SAML	47

Fase 2: IAM Identity Center eGoogle Workspace: Modifica dell'origine dell'identità IAM Identity Center e configurazione Google Workspace come provider di identità SAML	47
Passaggio 3Google Workspace: abilitare le app	49
Fase 4: IAM Identity Center: configurazione del provisioning automatico di IAM Identity Center	49
Fase 5Google Workspace: Configurazione del provisioning automatico	50
Passaggio di attributi per il controllo degli accessi - Facoltativo	52
Assegna l'accesso a Account AWS	53
Fasi successive	55
Risoluzione dei problemi	56
JumpCloud	56
Prerequisiti	57
Considerazioni SCIM	58
Fase 1: Abilitare il provisioning in IAM Identity Center	58
Fase 2: Configurare il provisioning in JumpCloud	59
(Facoltativo) Fase 3: Configurazione degli attributi utente JumpCloud per il controllo degli accessi in IAM Identity Center	60
(Facoltativo) Passaggio di attributi per il controllo degli accessi	61
Microsoft Entra ID	61
Prerequisiti	62
Considerazioni	62
Fase 1: Preparare il tenant Microsoft	64
Passaggio 2: prepara il tuo AWS account	66
Passaggio 3: configura e verifica la connessione SAML	69
Fase 4: Configurare e testare la sincronizzazione SCIM	73
Fase 5: Configurazione di ABAC - Opzionale	77
Assegna l'accesso a Account AWS	79
Microsoft Entra IDconfigurazione per l'accesso a regioni aggiuntive	81
Risoluzione dei problemi	81
Okta	84
Considerazioni	85
Passaggio 1Okta: ottieni i metadati SAML dal tuo account Okta	86
Fase 2: IAM Identity Center: configura Okta come fonte di identità per IAM Identity Center	86
Fase 3: IAM Identity Center eOkta: Esegui il provisioning Okta degli utenti	88
Fase 4Okta: Sincronizzazione degli utenti Okta con IAM Identity Center	89
Passaggio di attributi per il controllo degli accessi - Facoltativo	91

Assegna l'accesso a Account AWS	91
Oktac configurazione per l'accesso a regioni aggiuntive	94
Fasi successive	94
Risoluzione dei problemi	95
OneLogin	97
Prerequisiti	98
Fase 1: abilitare il provisioning in IAM Identity Center	98
Passaggio 2: configurare il provisioning in OneLogin	99
(Facoltativo) Passaggio 3: configura gli attributi utente OneLogin per il controllo degli accessi in IAM Identity Center	101
(Facoltativo) Passaggio di attributi per il controllo degli accessi	101
Risoluzione dei problemi	102
Identità Ping	103
PingFederate	103
PingOne	111
Directory del Centro identità	117
Tutorial video	123
Configurare la forza lavoro	124
Utenti, gruppi e provisioning	124
Unicità del nome utente e dell'indirizzo e-mail	124
Gruppi	125
Assegnazione di ruoli a utenti e gruppi	125
Deprovisioning di utenti e gruppi	125
Manage your identity source	126
Considerazioni sulla modifica dell'origine dell'identità	126
Cambia la fonte della tua identità	132
Attributi di utenti e gruppi in IAM Identity Center	134
Provider di identità esterni	135
Microsoft ADelenco	153
Gestione degli utenti nella directory Identity Center	174
Esecuzione del provisioning quando gli utenti si trovano in IAM Identity Center	175
Modifica della fonte dell'identità	175
Aggiungere utenti	175
Aggiungi gruppi	178
Aggiungere utenti ai gruppi	179
Elimina gruppi	180

Eliminare gli utenti	181
Rimuovi utenti dai gruppi	183
Modifica le proprietà dell'utente	184
Accesso alla forza lavoro	186
Comprendere le sessioni di autenticazione	186
Tipi di sessioni di autenticazione	187
Modi per terminare le sessioni utente	188
Cosa succede all'accesso degli utenti quando si termina una sessione	189
Disconnessione singola	193
Le migliori pratiche per la gestione delle sessioni	193
Configura la durata della sessione	193
Sessioni interattive per utenti	194
Sessioni in background degli utenti	195
Sessioni estese per Kiro	196
Termina le sessioni attive per gli utenti della forza lavoro	197
Considerazioni per le fonti di identità, la AWS CLI e AWS SDKs	199
Disabilita l'accesso degli utenti	202
Negare l'accesso degli utenti	203
Gestione dell'accesso per gli utenti nella directory Identity Center	205
Gestione delle password	205
MFA	205
Configurazione delle password degli utenti	206
Autenticazione a più fattori	209
Accesso alle applicazioni	223
AWS applicazioni gestite	224
Controllo dell'accesso alle applicazioni	224
Condivisione delle informazioni sull'identità	225
Limitazione dell'uso di applicazioni gestite AWS	226
Applicazioni che è possibile utilizzare con IAM Identity Center	227
Configurazione di IAM Identity Center per testare le applicazioni AWS gestite	231
Visualizzazione e modifica dei dettagli dell'applicazione	237
Disabilitazione di un'applicazione gestita AWS	238
Attivazione di sessioni di console con identità migliorata	239
Applicazioni gestite dal cliente	242
Applicazioni SAML 2.0 e 2.0 OAuth	243
Configurazione dell'applicazione SAML 2.0	248

Propagazione attendibile delle identità	252
Vantaggi della propagazione affidabile delle identità	252
Abilitare la propagazione affidabile delle identità	252
Come funziona la propagazione delle identità attendibili	253
Prerequisiti e considerazioni	254
Casi d'uso	256
Servizi di autorizzazione	282
Configurazione della propria applicazione OAuth 2.0	292
Configura applicazioni gestite dal cliente	293
Specificare applicazioni attendibili	297
Emittente di token affidabile	298
Ruota i certificati	313
Considerazioni prima della rotazione di un certificato	314
Ruota un certificato IAM Identity Center	314
Indicatori dello stato di scadenza del certificato	317
Comprendi le proprietà dell'applicazione	317
URL di avvio dell'applicazione	317
Stato del relè	318
Durata della sessione	319
Assegna l'accesso degli utenti alle applicazioni	319
Rimuovi l'accesso degli utenti alle applicazioni	320
Attributi della mappa	321
Account AWS accesso	322
Account AWS tipi	322
Assegnazione dell'accesso Account AWS	324
Esperienza dell'utente finale	325
Far rispettare e limitare l'accesso	326
Delegare e far rispettare l'accesso	326
Limitazione dell'accesso all'archivio di identità dagli account dei membri	326
Amministrazione delegata	327
Best practice	328
Prerequisiti	333
Registra un account membro	333
Annullamento della registrazione di un account membro	334
Visualizza gli account degli amministratori delegati	335
Accesso sopraelevato temporaneo	336

Accesso Single Sign-On a Account AWS	337
Assegna l'accesso a utenti o gruppi a Account AWS	337
Rimuovere l'accesso di utenti e gruppi a un Account AWS	340
Revoca una sessione attiva del set di autorizzazioni	341
Delega chi può assegnare l'accesso Single Sign-On	343
Set di autorizzazioni	345
Creare un set di autorizzazioni che applichi le autorizzazioni con privilegi minimi	345
Autorizzazioni predefinite	347
Autorizzazioni personalizzate	348
Creare, gestire ed eliminare set di autorizzazioni	351
Configura le proprietà del set di autorizzazioni	364
Riferimento ai set di autorizzazioni	370
Consigli per evitare interruzioni dell'accesso	373
Esempio di politica di fiducia personalizzata	373
Controllo dell'accesso basato sugli attributi	375
Vantaggi	375
Elenco di controllo: configurazione di ABAC utilizzando IAM Identity Center AWS	376
Attributi per il controllo degli accessi	379
Ruoli collegati ai servizi	386
AWS portale di accesso	388
Guida introduttiva al portale di AWS accesso	388
Configura il portale di AWS accesso	389
Cosa puoi configurare	389
Attivazione del portale di accesso AWS	389
Personalizzazione dell'URL del portale di AWS accesso	390
Conferma che gli utenti possano accedere al portale di AWS accesso	391
Utilizza il portale di accesso AWS	392
Come utilizzare il portale di accesso AWS	393
Accedere al portale di AWS accesso	393
Reimpostazione della password utente	396
AWS CLI e accesso AWS SDK	397
Creazione di collegamenti rapidi	402
Registrazione del dispositivo per l'MFA	405
Fine della sessione attiva	408
Utilizzo di IAM Identity Center su più Regioni AWS	409
Vantaggi del supporto multiregionale	409

Prerequisiti e considerazioni	409
Scelta di una regione aggiuntiva	410
Replica IAM Identity Center in un'altra regione	411
Fase 1: Creare una chiave di replica	411
Fase 2: Aggiungere la regione	411
Fase 3: Aggiornare la configurazione dell'IdP esterno	413
Fase 4: Conferma gli elenchi di indirizzi consentiti per firewall e gateway	413
Fase 5: Fornisci informazioni ai tuoi utenti	413
Modifiche alla regione oltre all'aggiunta della prima regione	414
Quali dati vengono replicati?	414
Accesso alla forza lavoro tramite una regione aggiuntiva	415
Sessioni utente su più sessioni Regioni AWS	415
AWS accedere agli endpoint del portale primari e aggiuntivi Regioni AWS	416
Endpoint ACS primari e aggiuntivi Regioni AWS	417
Utilizzo di applicazioni AWS gestite senza più ACS URLs	419
Failover verso un'altra regione per l'accesso Account AWS	420
Account AWS resilienza di accesso senza più ACS URLs	420
Distribuzione e gestione di applicazioni su più Regioni AWS	421
Distribuzione e gestione di applicazioni AWS gestite su più piattaforme Regioni AWS	421
Implementazione e gestione di applicazioni gestite dai clienti in più regioni AWS	423
Rimuovi una regione da IAM Identity Center	424
Fase 1: Aggiornamento della configurazione IdP esterna	424
Passaggio 2: rimuovere la regione	424
Fase 3: Eliminare la chiave di replica	425
Servizio APIs supportato in aggiunta Regioni AWS	426
CloudTrail eventi nelle regioni primarie e aggiuntive	426
Casi d'uso di IAM Identity Center nelle regioni primarie e aggiuntive	427
Progettazione della resilienza e comportamento regionale	430
Progettato per la disponibilità	431
Configurare l'accesso di emergenza al Console di gestione AWS	431
Riepilogo della configurazione dell'accesso di emergenza	432
Come progettare i ruoli operativi critici	433
Come pianificare il tuo modello di accesso	434
Come progettare una mappatura di emergenza di ruoli, account e gruppi	435
Come creare la configurazione di accesso di emergenza	436
Attività di preparazione alle emergenze	437

Processo di failover di emergenza	437
Ritorno alle normali operazioni	438
Configurazione una tantum di un'applicazione federativa IAM diretta in Okta	438
Configurazione una tantum di un'applicazione federativa IAM diretta con ADFS	442
Sicurezza	449
Gestione delle identità e degli accessi per IAM Identity Center	450
Autenticazione	450
Controllo accessi	450
Panoramica sulla gestione degli accessi	451
Esempi di policy basate su identità	455
Esempio di policy basata sulle risorse	463
AWS politiche gestite	466
Uso di ruoli collegati ai servizi	487
Console IAM Identity Center e autorizzazione API	495
Azioni API dopo novembre 2023	496
Azioni API successive a ottobre 2020	497
AWS STS chiavi di condizione per IAM Identity Center	499
UserId	500
IdentityStoreArn	500
ApplicationArn	501
CredentialId	501
InstanceArn	501
Registrazione di log e monitoraggio	502
Registrazione delle chiamate API IAM Identity Center con AWS CloudTrail	502
Registrazione di IAM Identity Center SCIM con AWS CloudTrail	542
Amazon EventBridge	549
Registrazione degli errori di sincronizzazione AD configurabili	549
Convalida della conformità	552
Standard di conformità supportati	552
Resilienza	554
Sicurezza dell'infrastruttura	555
Protezione dei dati	556
Crittografia dei dati in transito	556
Privacy dei dati	557
Conservazione dei dati	557
Crittografia dei dati a riposo	557

Contesto di crittografia IAM Identity Center	559
Utilizzo del contesto di crittografia per controllare l'accesso alla chiave gestita dal cliente	559
Monitoraggio delle chiavi di crittografia per IAM Identity Center	560
AWS archiviazione, crittografia ed eliminazione degli attributi di identità di IAM Identity Center da parte delle applicazioni gestite	560
Implementazione di chiavi KMS gestite dal cliente	561
Dichiarazioni sulla chiave KMS di base e sulle politiche IAM	571
Dichiarazioni politiche chiave di Advanced KMS	593
Applicazione di tag alle risorse	602
Limitazioni applicate ai tag	603
Gestisci i tag con la console	603
AWS CLI esempi	604
Assegnazione di tag	604
Visualizzazione dei tag	605
Rimozione dei tag	605
Applicazione di tag quando si crea un set di autorizzazioni	605
Operazioni dell'API	606
Integrazione della AWS CLI con IAM Identity Center	607
Come integrare la AWS CLI con IAM Identity Center	607
Considerazioni per l'accesso privato	608
Quote	609
Quote delle applicazioni	609
Account AWS quote	610
Quote Active Directory	611
Quote degli archivi di identità di IAM Identity Center	611
Limiti di limitazione di IAM Identity Center	612
Quote di richieste di servizio OIDC	613
Quote aggiuntive	614
Risoluzione dei problemi	616
Problemi di creazione di un'istanza di account di IAM Identity Center	616
Ricevi un errore quando tenti di visualizzare l'elenco delle applicazioni cloud preconfigurate per funzionare con IAM Identity Center	616
Problemi relativi al contenuto delle asserzioni SAML create da IAM Identity Center	618
Alcuni utenti non riescono a sincronizzarsi in IAM Identity Center da un provider SCIM esterno	618

Errore duplicato di utenti o gruppi durante il provisioning di utenti o gruppi con un provider di identità esterno	620
Gli utenti non possono accedere se il loro nome utente è in formato UPN	621
Ricevo l'errore «Impossibile eseguire l'operazione sul ruolo protetto» durante la modifica di un ruolo IAM	621
Gli utenti della Directory non possono reimpostare la propria password	622
Il mio utente è referenziato in un set di autorizzazioni ma non può accedere agli account o alle applicazioni assegnati	622
Non riesco a configurare correttamente la mia applicazione dal catalogo delle applicazioni	623
Errore «Si è verificato un errore imprevisto» quando un utente tenta di accedere utilizzando un provider di identità esterno	623
Errore «Impossibile abilitare gli attributi per il controllo degli accessi»	624
Ricevo il messaggio «Browser non supportato» quando tento di registrare un dispositivo per l'MFA	625
Il gruppo «Domain Users» di Active Directory non si sincronizza correttamente con IAM Identity Center	625
Errore di credenziali MFA non valide	625
Ricevo il messaggio «Si è verificato un errore imprevisto» quando tento di registrarmi o accedere utilizzando un'app di autenticazione	625
Quando tento di accedere a IAM Identity Center ricevo il messaggio di errore «Non sei tu, siamo noi»	626
I miei utenti non ricevono e-mail da IAM Identity Center	626
Errore: non è possibile delete/modify/remove/assign accedere ai set di autorizzazioni forniti nell'account di gestione	627
Errore: token di sessione non trovato o non valido	627
I membri del gruppo provenienti da domini affidabili non si sincronizzano con IAM Identity Center	627
Risolvi i problemi relativi alle chiavi gestite dal cliente in AWS IAM Identity Center	628
Accesso negato: problema di autorizzazione KMS Decrypt	628
AWS ha gestito gli errori di accesso alle applicazioni con una chiave KMS gestita dal cliente abilitata in IAM Identity Center	628
AWS errori di assegnazione and/or degli utenti nell'installazione di applicazioni gestite con una chiave KMS gestita dal cliente abilitata in IAM Identity Center	629
Problema relativo alle autorizzazioni KMS: configurazione della chiave gestita dal cliente con AWS IAM Identity Center	629

AWS accedere agli errori di accesso al portale con una chiave KMS gestita dal cliente abilitata in IAM Identity Center	630
Risolvi i problemi di configurazione multiregionale in AWS IAM Identity Center	630
La regione in cui voglio replicare la mia istanza IAM Identity Center non è disponibile nella console IAM Identity Center	630
AWS errori di accesso alle applicazioni gestiti in una regione aggiuntiva	630
Cronologia dei documenti	631
AWS Glossario	642
.....	dcxliii

Cos'è il Centro identità IAM?

AWS IAM Identity Center è la AWS soluzione per connettere gli utenti della forza lavoro ad applicazioni AWS gestite come Kiro e Amazon Quick e ad altre AWS risorse. Puoi connettere il tuo provider di identità esistente e sincronizzare utenti e gruppi dalla tua directory, oppure creare e gestire i tuoi utenti direttamente in IAM Identity Center. Puoi quindi utilizzare IAM Identity Center per una o entrambe le seguenti operazioni:

- Accesso degli utenti alle applicazioni
- Accesso utente a Account AWS

Usi già IAM per l'accesso a Account AWS?

Non è necessario apportare modifiche ai Account AWS flussi di lavoro correnti per utilizzare IAM Identity Center per accedere alle applicazioni AWS gestite. Se utilizzi la [federazione con IAM](#) per Account AWS l'accesso, i tuoi utenti possono continuare ad accedere Account AWS nello stesso modo in cui hanno sempre fatto e tu puoi continuare a utilizzare i flussi di lavoro esistenti per gestire tale accesso.

Perché usare IAM Identity Center?

IAM Identity Center semplifica e semplifica l'accesso degli utenti della forza lavoro alle applicazioni o Account AWS, o a entrambe, attraverso le seguenti funzionalità chiave.

Integrazione con applicazioni gestite AWS

[AWS applicazioni gestite](#) come Kiro e Amazon Redshift integrazione con IAM Identity Center. IAM Identity Center fornisce applicazioni AWS gestite con una visione comune di utenti e gruppi.

Propagazione affidabile dell'identità tra le applicazioni

Grazie alla propagazione affidabile delle identità, le applicazioni AWS gestite come Amazon Quick possono condividere in modo sicuro l'identità di un utente con altre applicazioni AWS gestite, ad esempio Amazon Redshift e autorizzare l'accesso alle AWS risorse in base all'identità dell'utente. È possibile controllare più facilmente l'attività degli utenti perché CloudTrail gli eventi vengono registrati in base all'utente e alle azioni avviate dall'utente. In questo modo è più facile capire chi ha effettuato l'accesso a cosa. Per informazioni sui casi d'uso supportati, incluse le linee guida end-to-end alla configurazione, consulta [Casi d'uso affidabili per la propagazione delle identità](#).

Un unico posto per assegnare le autorizzazioni a più persone Account AWS

Con le autorizzazioni per più account, IAM Identity Center offre un'unica posizione in cui assegnare le autorizzazioni a gruppi di utenti in più gruppi. Account AWS 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 controllarne l'accesso a determinati utenti. Account AWS

Questa funzionalità opzionale è disponibile solo per le [istanze organizzative](#) di IAM Identity Center.

Un punto di federazione per semplificare l'accesso degli utenti AWS

Fornendo un punto di federazione, IAM Identity Center riduce lo sforzo amministrativo richiesto per utilizzare più applicazioni AWS gestite e Account AWS. Con IAM Identity Center, esegui la federazione una sola volta e hai un solo certificato da gestire quando utilizzi un provider di [SAML 2.0](#) identità. IAM Identity Center fornisce applicazioni AWS gestite con una visione comune di utenti e gruppi per casi d'uso affidabili di propagazione delle identità o quando gli utenti condividono l'accesso alle AWS risorse con altre persone.

Per informazioni su come configurare i provider di identità di uso comune per l'utilizzo con IAM Identity Center, consulta [Tutorial sulle fonti di identità di IAM Identity Center](#). Se non disponi di un provider di identità esistente, puoi [creare e gestire gli utenti direttamente in IAM Identity Center](#).

Due tipi di istanze

IAM Identity Center supporta due tipi di istanze: istanze organizzative 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 di produzione delle applicazioni. Un'istanza dell'organizzazione viene distribuita nell'account di AWS Organizations gestione e offre un unico punto da cui gestire l'accesso degli utenti. AWS

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 [Istanze di organizzazione e account di IAM Identity Center](#).

Accesso intuitivo al portale web per i tuoi utenti

Il portale di AWS accesso è un portale web intuitivo che fornisce agli utenti un accesso senza interruzioni a tutte le applicazioni assegnate o a entrambe Account AWS.

Accesso e applicazioni multiregionali Account AWS

Quando replichi l'istanza di IAM Identity Center in altre regioni, la forza lavoro può accedere alle applicazioni assegnate Account AWS e a quelle assegnate tramite tutte le regioni abilitate e può distribuire applicazioni AWS gestite in ciascuna regione abilitata.

Rinomina di IAM Identity Center

Il 26 luglio 2022, AWS Single Sign-On è stato rinominato in. AWS IAM Identity Center

Nessuna modifica ai namespace legacy

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](#)
- Risorse [CloudFormation](#) contenenti prefissi AWS::SSO
- Ruolo collegato al [servizio contenente](#) AWSServiceRoleForSSO
- Console contenente URLs e sso singlesignon
- Documentazione URLs contenente singlesignon

Nozioni di base sul Centro identità IAM

Di seguito viene descritto come iniziare a utilizzare IAM Identity Center.

1. Abilita IAM Identity Center

Quando [abiliti IAM Identity Center](#), scegli tra due tipi di istanze IAM Identity Center. Questi tipi sono: [istanze organizzative \(consigliate\)](#) e [istanze di account](#). Per ulteriori informazioni sulle diverse funzionalità di questi tipi di istanze, consulta le [istanze di organizzazione e account di IAM Identity Center](#).

Note

Dopo aver abilitato IAM Identity Center, puoi accedere e aprire la [console IAM Identity Center](#) effettuando una delle seguenti operazioni:

- Istanza dell'organizzazione: accedi AWS utilizzando credenziali con autorizzazioni amministrative nell'account di gestione.
- Istanza dell'account: accedi AWS utilizzando credenziali con autorizzazioni amministrative nell'area in Account AWS cui è abilitato IAM Identity Center.

2. Connect la tua fonte di identità a IAM Identity Center

Nella console IAM Identity Center, conferma la fonte di identità che desideri utilizzare. Vedi quanto segue per le fonti di identità:

- Provider di identità esterno: se disponi di un provider di identità esistente per gestire gli utenti della forza lavoro, puoi collegarlo a IAM Identity Center. Per ulteriori informazioni su come configurare i provider di identità di uso comune per l'utilizzo con IAM Identity Center, consulta [Tutorial sulle fonti di identità di IAM Identity Center](#).
- Active Directory: se utilizzi Active Directory per gestire gli utenti della forza lavoro, puoi collegarlo a IAM Identity Center. Per ulteriori informazioni, consulta [Utilizzo di Active Directory come origine di identità](#).
- IAM Identity Center - In alternativa, puoi [creare e gestire utenti e gruppi direttamente in IAM Identity Center](#).

 Note

Attualmente, è necessario utilizzare un provider di identità esterno come fonte di identità per sfruttare una configurazione multiregionale con IAM Identity Center. Per ulteriori informazioni sui vantaggi di questa configurazione, consulta [Utilizzo di IAM Identity Center su più Regioni AWS](#)

3. Configurare l'accesso utente a Account AWS (solo istanza dell'organizzazione)

Se utilizzi un'istanza organizzativa di IAM Identity Center, puoi [assegnare l'accesso a utenti o gruppi Account AWS](#), utilizzando [set di autorizzazioni](#) per concedere agli utenti l'accesso a Account AWS e risorse.

4. Configura l'accesso degli utenti alle applicazioni

Con IAM Identity Center, puoi concedere agli utenti l'accesso a due tipi di applicazioni:

a. [AWS applicazioni gestite](#)

- Puoi utilizzare IAM Identity Center con applicazioni AWS gestite come Amazon Q Business e Amazon Redshift. AWS CLI Per ulteriori informazioni, consultare [AWS applicazioni gestite e Integrazione della AWS CLI con IAM Identity Center](#).

b. [Applicazioni gestite dal cliente](#)

- Puoi integrare uno dei seguenti tipi di applicazioni gestite dai clienti con IAM Identity Center:
 - [Applicazioni elencate nel catalogo IAM Identity Center](#)
 - [Le tue applicazioni personalizzate](#)
- Dopo aver configurato l'applicazione, puoi [assegnare agli utenti l'accesso all'applicazione](#).

5. Fornisci agli utenti le istruzioni di accesso per il portale di accesso AWS

Il portale di AWS accesso è un portale web che fornisce agli utenti un accesso senza interruzioni a tutte le applicazioni loro assegnate o a Account AWS entrambe. I nuovi utenti in IAM Identity Center devono attivare le proprie credenziali utente prima di poter accedere al portale di AWS accesso.

Per informazioni su come accedere al portale di AWS accesso, consulta [Accedere al portale di AWS accesso nella Guida per l'Accedi ad AWS utente](#). Per ulteriori informazioni sulla procedura di accesso per il portale di AWS accesso, consulta [Accesso al portale di AWS accesso](#).

Prerequisiti e considerazioni di IAM Identity Center

Puoi utilizzare IAM Identity Center per accedere solo alle applicazioni AWS gestite, Account AWS solo o entrambe. Se utilizzi la federazione IAM per gestire l'accesso a Account AWS, puoi continuare a farlo utilizzando IAM Identity Center per l'accesso alle applicazioni.

Prima di abilitare IAM Identity Center, considera quanto segue:

- AWS Regione

Per prima cosa abilita IAM Identity Center in un'unica regione [supportata](#) per ogni istanza di IAM Identity Center. Se desideri utilizzare IAM Identity Center per l'accesso Single Sign-On agli AWS account, la regione deve essere accessibile a tutti gli utenti della tua organizzazione. Se prevedi di utilizzare IAM Identity Center per l'accesso alle applicazioni, tieni presente che alcune applicazioni AWS gestite, come Amazon SageMaker AI, possono funzionare solo nelle regioni che supportano. Inoltre, la maggior parte delle applicazioni AWS gestite richiede che IAM Identity Center sia disponibile nella stessa regione dell'applicazione. Ciò può essere ottenuto collocandole nella stessa regione o, se supportata, replicando l'istanza di IAM Identity Center nella regione di distribuzione desiderata di un' AWS applicazione gestita. Per ulteriori informazioni, consulta [Considerazioni per la scelta di un Regione AWS](#).

- Solo accesso alle applicazioni

Puoi utilizzare IAM Identity Center solo per l'accesso degli utenti ad applicazioni come Kiro, utilizzando il tuo provider di identità esistente. Per ulteriori informazioni, consulta [Utilizzo di IAM Identity Center solo per l'accesso degli utenti alle applicazioni](#).

 Note

L'accesso alle risorse dell'applicazione è gestito in modo indipendente dal proprietario dell'applicazione.

- Quota per i ruoli IAM

IAM Identity Center crea ruoli IAM per fornire agli utenti le autorizzazioni per accedere alle risorse dell'account. Per ulteriori informazioni, consulta [Ruoli IAM creati da IAM Identity Center](#).

- 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. Se hai già configurato AWS Organizations

e intendi aggiungere IAM Identity Center alla tua organizzazione, assicurati che tutte le AWS Organizations funzionalità siano abilitate. Per ulteriori informazioni, consulta [IAM Identity Center e AWS Organizations](#).

Le interfacce web di IAM Identity Center, tra cui il portale di accesso e la console IAM Identity Center, sono pensate per essere accessibili agli esseri umani tramite i browser Web supportati. I browser compatibili includono le ultime tre versioni di Microsoft Edge, Mozilla Firefox, Google Chrome e Apple Safari. L'accesso a questi endpoint utilizzando percorsi non basati su browser non è supportato. Per l'accesso programmatico ai servizi IAM Identity Center, consigliamo di utilizzare la documentazione APIs disponibile nelle guide di riferimento delle API IAM Identity Center e Identity Store.

Considerazioni per la scelta di un Regione AWS

Puoi abilitare IAM Identity Center in un'unica soluzione, supportata Regione AWS a tua scelta e disponibile per gli utenti di tutto il mondo. Questa disponibilità globale semplifica la configurazione dell'accesso degli utenti a più Account AWS applicazioni. Di seguito sono riportate le considerazioni chiave per la scelta di un Regione AWS.

- Posizione geografica dei tuoi utenti: 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 AI. SageMaker
- Regioni di attivazione (regioni disabilitate per impostazione predefinita): una regione opt-in è una Regione AWS regione disabilitata per impostazione predefinita. Per utilizzare una regione che richiede l'attivazione, è necessario abilitarla. Per ulteriori informazioni, consulta [Managing IAM Identity Center in una regione opt-in](#).
- Replica di IAM Identity Center in altre regioni: se prevedi di replicare IAM Identity Center in altre regioni Regioni AWS, devi scegliere una regione abilitata per impostazione predefinita. Per ulteriori informazioni, consulta [Utilizzo di IAM Identity Center su più Regioni AWS](#).
- Scelta delle regioni di distribuzione per le applicazioni AWS AWS gestite: le applicazioni gestite possono funzionare solo nelle aree Regioni AWS in cui sono disponibili. Molte applicazioni AWS gestite possono inoltre funzionare solo in una regione in cui è abilitato o replicato IAM Identity Center (regione principale o aggiuntiva). Per confermare se l'istanza di IAM Identity Center supporta la replica in regioni aggiuntive, consulta. [Utilizzo di IAM Identity Center su più Regioni AWS](#) Se la replica non è un'opzione, valuta la possibilità di abilitare IAM Identity Center nella regione in cui prevedi di utilizzare le applicazioni AWS gestite.

- Sovranità digitale: le normative sulla sovranità digitale o le politiche aziendali possono imporre l'uso di una particolare. Regione AWS Rivolgiti all'ufficio legale della tua azienda.
- Origine dell'identità: se utilizzi [AWS Managed Microsoft AD](#) la tua directory gestita automaticamente in Active [Directory \(AD\)](#) come origine dell'identità, la sua regione di origine deve corrispondere Regione AWS a quella in cui hai abilitato IAM Identity Center.
- Email interregionali con Amazon Simple Email Service: in alcune regioni, IAM Identity Center può chiamare [Amazon Simple Email Service \(Amazon SES\)](#) in un'altra regione per inviare e-mail. In queste chiamate interregionali, IAM Identity Center invia determinati attributi utente all'altra regione. Per ulteriori informazioni, consulta [Email interregionali con Amazon SES](#).
- AWS Control Tower— Se stai abilitando un'istanza organizzativa di IAM Identity Center da AWS Control Tower, l'istanza verrà creata nella stessa regione della AWS Control Tower landing zone.

Argomenti

- [Archiviazione e operazioni dei dati della regione IAM Identity Center](#)
- [Cambio Regioni AWS](#)
- [Disabilitazione di un Regione AWS punto in cui IAM Identity Center è abilitato](#)

Archiviazione e operazioni dei dati della regione IAM Identity Center

Scopri come IAM Identity Center gestisce l'archiviazione e le operazioni dei dati in tutto il mondo Regioni AWS.

Scopri come IAM Identity Center archivia i dati

Quando abiliti IAM Identity Center, tutti i dati che configuri in IAM Identity Center vengono archiviati nella regione in cui li hai abilitati. 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. Se replichi l'istanza di IAM Identity Center in regioni aggiuntive, IAM Identity Center replica automaticamente utenti, gruppi, set di autorizzazioni e relative assegnazioni e altri metadati e configurazioni in tali regioni.

Email interregionali con Amazon SES

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.

Codice regionale IAM Identity Center	Nome della regione IAM Identity Center	Codice regionale Amazon SES	Nome della regione Amazon SES
ap-east-1	Asia Pacifico (Hong Kong)	ap-northeast-2	Asia Pacifico (Seul)
ap-east-2	Asia Pacifico (Taipei)	ap-northeast-1	Asia Pacifico (Tokyo)
ap-south-2	Asia Pacifico (Hyderabad)	ap-south-1	Asia Pacifico (Mumbai)
ap-southeast-4	Asia Pacifico (Melbourne)	ap-southeast-2	Asia Pacifico (Sydney)
ap-southeast-5	Asia Pacifico (Malesia)	ap-southeast-1	Asia Pacifico (Singapore)
ap-southeast-6	Asia Pacifico (Nuova Zelanda)	ap-southeast-2	Asia Pacifico (Sydney)
ap-southeast-7	Asia Pacifico (Thailandia)	ap-northeast-3	Asia Pacifico (Osaka)
ca-west-1	Canada occidentale (Calgary)	ca-central-1	Canada (Centrale)
eu-south-2	Europa (Spagna)	eu-west-3	Europa (Parigi)
eu-central-2	Europa (Zurigo)	eu-central-1	Europa (Francoforte)

Codice regionale IAM Identity Center	Nome della regione IAM Identity Center	Codice regionale Amazon SES	Nome della regione Amazon SES
mx-central-1	Messico (centrale)	us-east-2	Stati Uniti orientali (Ohio)
me-central-1	Medio Oriente (Emirati Arabi Uniti)	eu-central-1	Europa (Francoforte)
us-gov-east-1	AWS GovCloud (Stati Uniti orientali)	us-gov-west-1	AWS GovCloud (Stati Uniti occidentali)

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, ma è necessario abilitare le seguenti [regioni opt-in](#) se si desidera utilizzare IAM Identity Center:

- Africa (Città del Capo)
- Asia Pacifico (Hong Kong)
- Asia Pacifico (Taipei)
- Asia Pacifico (Hyderabad)
- Asia Pacifico (Giacarta)

- Asia Pacifico (Melbourne)
- Asia Pacifico (Malesia)
- Asia Pacifico (Nuova Zelanda)
- Asia Pacifico (Thailandia)
- Canada occidentale (Calgary)
- Europa (Milano)
- Europa (Spagna)
- Europa (Zurigo)
- Israele (Tel Aviv)
- Messico (centrale)
- Medio Oriente (Bahrein)
- Medio Oriente (Emirati Arabi Uniti)

Se distribuisce IAM Identity Center in una regione opzionale, devi abilitare questa regione in tutti gli account per i quali desideri gestire l'accesso a IAM Identity Center. Tutti gli account necessitano di questa configurazione, indipendentemente dal fatto che tu crei o meno risorse in quella regione. Puoi abilitare una regione per gli account correnti della tua organizzazione e devi ripetere questa azione quando aggiungi nuovi account. 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](#).

Note

Il tuo account AWS membro deve essere inserito nella stessa regione della regione di attivazione in cui si trova l'istanza IAM Identity Center, in modo da poter accedere all'account del AWS membro dal portale di accesso. AWS

Metadati archiviati nelle regioni che accettano l'iscrizione

Quando abiliti IAM Identity Center per un account di gestione con 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 (ARNs) dei ruoli IAM creati da IAM Identity Center nell'account del membro

Regioni AWS che sono abilitati per impostazione predefinita

Le seguenti regioni sono abilitate per impostazione predefinita ed è possibile abilitare IAM Identity Center in queste regioni.

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

Cambio Regioni AWS

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. Per ulteriori informazioni, consulta [Considerazioni per la scelta di un Regione AWS](#).

Puoi cambiare la tua regione di IAM Identity Center solo [eliminando l'istanza corrente di IAM Identity Center](#) e creando un'istanza in un'altra regione. Se hai già abilitato un'applicazione AWS gestita con l'istanza IAM Identity Center esistente, disabilita l'applicazione prima di eliminare IAM Identity Center. Per istruzioni sulla disabilitazione delle applicazioni AWS gestite, consulta [Disabilitazione di un'applicazione gestita AWS](#)

Note

Se stai pensando di cambiare la tua regione di IAM Identity Center per consentire la distribuzione di un'applicazione AWS gestita in un'altra regione, prendi in considerazione la possibilità di replicare l'istanza di IAM Identity Center in quella regione. Per ulteriori informazioni, consulta [Utilizzo di IAM Identity Center su più Regioni AWS](#).

Considerazioni sulla configurazione nella nuova regione

È necessario ricreare utenti, gruppi, set di autorizzazioni, applicazioni e assegnazioni nella nuova istanza di IAM Identity Center. Puoi utilizzare l'account IAM Identity Center e l'assegnazione dell'applicazione [APIs](#) per ottenere un'istantanea della configurazione e quindi utilizzarla per ricostruire la configurazione in una nuova regione. Il passaggio a una regione diversa modifica anche l'URL del [portale di AWS accesso](#), che fornisce agli utenti l'accesso Single Sign-On alle proprie applicazioni. Account AWS Potrebbe inoltre essere necessario ricreare alcune configurazioni di IAM Identity Center tramite la console di gestione della nuova istanza.

Disabilitazione di un Regione AWS punto in cui IAM Identity Center è abilitato

Se si disabilita un sistema Regione AWS 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.

Per riattivare IAM Identity Center in [modalità opt-in Regioni AWS](#), devi riattivare la regione. Poiché IAM Identity Center deve rielaborare 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 per l'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.

Utilizzo di IAM Identity Center solo per l'accesso degli utenti alle applicazioni

Puoi utilizzare IAM Identity Center per l'accesso degli utenti ad applicazioni come Kiro o a Account AWS entrambe. Puoi connettere il tuo provider di identità esistente e sincronizzare utenti e gruppi dalla tua directory, oppure [creare e gestire gli utenti direttamente in IAM Identity Center](#). Per informazioni su come connettere il tuo provider di identità esistente a IAM Identity Center, consulta il [Tutorial sulle fonti di identità di IAM Identity Center](#).

Usi già IAM per l'accesso a Account AWS?

Non è necessario apportare modifiche ai Account AWS flussi di lavoro correnti per utilizzare IAM Identity Center per accedere alle applicazioni AWS gestite. Se utilizzi la [federazione con IAM](#) per Account AWS l'accesso, i tuoi utenti possono continuare ad accedere Account AWS nello stesso modo in cui hanno sempre fatto e tu puoi continuare a utilizzare i flussi di lavoro esistenti per gestire tale accesso.

Ruoli IAM creati da IAM Identity Center

Quando assegni un utente a un AWS account, IAM Identity Center crea ruoli IAM per fornire agli utenti le autorizzazioni per accedere alle risorse.

Quando assegni un set di autorizzazioni, IAM Identity Center crea i ruoli IAM corrispondenti controllati da IAM Identity Center in ciascun account e associa le policy 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 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. La replica dell'istanza IAM Identity Center in regioni aggiuntive non influisce sui ruoli IAM esistenti e non crea nuovi ruoli IAM.

Note

I set di autorizzazioni non vengono utilizzati per concedere autorizzazioni alle applicazioni.

Se hai già configurato i ruoli IAM nel tuo account 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. In caso contrario, 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, l'account Account AWS che configura 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 [Istanze organizzative 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 un'istanza organizzativa di IAM Identity Center, devi accedere a IAM Identity Center Console di gestione AWS accedendo al tuo account di AWS Organizations gestione come utente con credenziali amministrative o come utente root (opzione non consigliata a meno che non esistano altri utenti amministrativi). Per ulteriori informazioni, consulta [Creazione e gestione di un' AWS organizzazione](#) nella Guida per l'AWS Organizations utente.

Se accedi con credenziali amministrative da un account AWS Organizations membro, puoi abilitare un'istanza di account di IAM Identity Center. Le istanze di account hanno funzionalità limitate e sono associate a un singolo AWS account.

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.

- Istanza dell'organizzazione (consigliata)

Un'istanza di IAM Identity Center che abiliti nell'account di AWS Organizations gestione. Le istanze organizzative supportano tutte le funzionalità di IAM Identity Center. Ti consigliamo di implementare un'istanza organizzativa anziché istanze di account per ridurre al minimo il numero di punti di gestione.

- Istanza dell'account

Un'istanza di IAM Identity Center associata a una singola Account AWS istanza e visibile solo all'interno della AWS regione Account AWS e della regione in cui è abilitata. Utilizza un'istanza di account per scenari più semplici con account singolo. Puoi abilitare un'istanza di account da una delle seguenti opzioni:

- E Account AWS questo non è gestito da AWS Organizations
- Un account membro in AWS Organizations

Account AWS tipi che possono abilitare IAM Identity Center

Per abilitare IAM Identity Center, accedi a Console di gestione AWS 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 Organizations. È possibile associare solo un'istanza di IAM Identity Center a un'istanza standalone Account AWS e utilizzare tale istanza per le assegnazioni di applicazioni all'interno di tale istanza Account AWS.

Utilizza la tabella seguente per confrontare le funzionalità fornite dal tipo di istanza:

Funzionalità	Istanza nell'account AWS Organizations di gestione (consigliata)	Istanza in un account membro	Istanza in modalità autonoma Account AWS
Gestisci gli utenti	✔Sì	✔Sì	✔Sì
AWS portale di accesso per l'accesso Single Sign-On alle applicazioni gestite AWS	✔Sì	✔Sì	✔Sì
OAuth applicazioni gestite dai clienti 2.0 (OIDC)	✔Sì	✔Sì	✔Sì
Autorizzazioni per più account	✔Sì	✘No	✘No

Funzionalità	Istanza nell'account AWS Organizations di gestione (consigliata)	Istanza in un account membro	Istanza in modalità autonoma Account AWS
AWS portale di accesso per l'accesso Single Sign-On al Account AWS	✔Sì	✘No	✘No
applicazioni gestite dai clienti SAML 2.0	✔Sì	✘No	✘No
L'amministratore delegato può gestire l'istanza	✔Sì	✘No	✘No
Crittografia inattiva utilizzando una chiave KMS gestita dal cliente	✔Sì	✘No	✘No
Replica di IAM Identity Center in altre regioni	✔Sì	✘No	✘No

Per ulteriori informazioni sulle applicazioni AWS gestite e IAM Identity Center, consulta [AWS applicazioni gestite che è possibile utilizzare con IAM Identity Center](#).

Argomenti

- [Istanze organizzative di IAM Identity Center](#)
- [Istanze account del Centro identità IAM](#)
- [Elimina la tua istanza 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 organizzazione deve essere abilitata nel proprio account di gestione ed è

possibile gestire centralmente l'accesso di utenti e gruppi con un'unica istanza organizzativa. Puoi avere solo un'istanza organizzativa 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.

Per abilitare un'istanza organizzativa di IAM Identity Center, consulta [Per abilitare un'istanza di IAM Identity Center](#).

Quando utilizzare un'istanza organizzativa

Un'istanza organizzativa è il metodo principale per abilitare IAM Identity Center e di solito è consigliata un'istanza organizzativa. Le istanze organizzative offrono i seguenti vantaggi:

- Supporto per tutte le funzionalità di IAM Identity Center, inclusa la gestione delle autorizzazioni per più utenti dell'organizzazione, l'assegnazione dell'accesso alle applicazioni gestite dal cliente e la replica Account AWS in più regioni.
- 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.
- Controllo centralizzato della creazione di istanze di account: puoi controllare se le istanze di account possono essere create dagli account 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).

Per istruzioni su come abilitare un'istanza organizzativa di IAM Identity Center, consulta [Per abilitare un'istanza di IAM Identity Center](#).

Istanze account del Centro identità IAM

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 da una delle

seguenti opzioni: un account membro in AWS Organizations o un account autonomo Account AWS non gestito da AWS Organizations.

Per istruzioni su come abilitare un'istanza di account di IAM Identity Center, consulta [Per abilitare un'istanza di IAM Identity Center](#) e scegli la scheda Account.

Quando utilizzare un'istanza di account

Nella maggior parte dei casi, è consigliata un'[istanza organizzativa](#). Utilizza le istanze dell'account 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.
- Non hai il controllo dell' AWS organizzazione in cui operi. Ad esempio, una terza parte controlla l' AWS organizzazione che gestisce la tua Account AWS.

Important

Se prevedi di utilizzare IAM Identity Center per supportare applicazioni su più account, utilizza un'istanza dell'organizzazione. Le istanze di account non supportano questo caso d'uso.

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 che è possibile utilizzare con IAM Identity Center](#) Verifica la disponibilità della creazione di istanze di account con la tua applicazione AWS gestita.

Vincoli di disponibilità per gli account dei membri

Per distribuire le istanze di account di IAM Identity Center negli account dei AWS Organizations membri, deve essere soddisfatta una delle seguenti condizioni:

- Non esiste un'istanza organizzativa di IAM Identity Center nell'organizzazione.
- Nell'organizzazione è presente un'istanza organizzativa di IAM Identity Center e l'amministratore dell'istanza consente la creazione di istanze di account di IAM Identity Center (per le istanze dell'organizzazione create dopo il 15 novembre 2023).
- Nell'organizzazione è presente un'istanza organizzativa di IAM Identity Center e l'amministratore dell'istanza ha abilitato manualmente la creazione di istanze di account da parte degli account dei membri dell'organizzazione (per le istanze dell'organizzazione create prima del 15 novembre 2023). Per istruzioni, consulta [Consenti la creazione di istanze di account negli account dei membri](#).

Una volta soddisfatta una delle condizioni precedenti, devono essere soddisfatte tutte le seguenti condizioni:

- L'amministratore non ha creato una [politica di controllo dei servizi](#) che impedisca agli account dei membri di creare istanze di account.
- Non hai già un'istanza di IAM Identity Center nello stesso account, a prescindere da. Regione AWS
- Stai lavorando in un ambiente in Regione AWS cui è disponibile IAM Identity Center. Per informazioni sulle regioni, consulta [Archiviazione e operazioni dei dati della regione IAM Identity Center](#).

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 o unire un'istanza di account in un'istanza dell'organizzazione.
- Solo alcune [applicazioni AWS gestite supportano le](#) istanze di account.
- Utilizza istanze di account per utenti isolati che utilizzeranno le applicazioni in un solo 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.

Consenti la creazione di istanze di account negli account dei membri

Se hai abilitato IAM Identity Center prima del 15 novembre 2023, hai un'[istanza organizzativa](#) di IAM Identity Center con la possibilità per gli account membro di creare istanze di account disabilitata per impostazione predefinita. Puoi scegliere se i tuoi account membro possono creare istanze di account abilitando la funzionalità di istanza dell'account nella console IAM Identity Center.

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

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](#).

1. Apri la [console Centro identità IAM](#).
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.

Utilizza le politiche di controllo dei servizi per controllare la creazione delle istanze dell'account

La capacità degli account membri di creare istanze di account dipende da quando hai abilitato IAM Identity Center:

- Prima di novembre 2023: devi [consentire la creazione di istanze di account negli account dei membri](#), un'azione che non può essere annullata.
- Dopo il 15 novembre 2023: per impostazione predefinita, gli account dei membri possono creare istanze di account.

In entrambi i casi, puoi utilizzare Service Control Policies (SCPs) per:

- Impedire a tutti gli account dei membri di creare istanze di account.
- Consenti solo ad account membri specifici di creare istanze di account.

Impedisce le istanze dell'account

Utilizza la seguente procedura per generare un SCP che impedisca agli account dei membri di creare istanze di account di IAM Identity Center.

1. Apri la [console Centro identità IAM](#).
2. Nella Dashboard, nella sezione Gestione centrale, seleziona il pulsante Impedisce 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. SCPs sono una funzionalità di AWS Organizations. Per istruzioni su come allegare un SCP, consulta [Allegare e scollegare le politiche di controllo del servizio](#) nella Guida per l'utente AWS Organizations.

Limita le istanze dell'account

Invece di impedire la creazione di tutte le istanze di account, questa policy impedisce qualsiasi tentativo di creare un'istanza di account di IAM Identity Center per tutti Account AWS tranne quelli esplicitamente elencati nel segnaposto. **"<ALLOWED-ACCOUNT-ID>"**

Example: Nega la politica per limitare la creazione di istanze di account

JSON

```
{  
  
  "Version": "2012-10-17",  
  "Statement" : [  
    {  
      "Sid": "DenyMemberAccountInstances",  
      "Effect": "Deny",  
      "Action": "sso:CreateInstance",  
    }  
  ]  
}
```



```

    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalAccount": ["<ALLOWED-ACCOUNT-ID>"]
      }
    }
  }
]
}

```

- Sostituisci ["<ALLOWED-ACCOUNT-ID>"] con gli Account AWS ID effettivi a cui desideri consentire la creazione di un'istanza di account di IAM Identity Center.
- Puoi elencare più account consentiti IDs nel formato array: ["11122223333", "444455556666"].
- Allega questa policy all'SCP della tua organizzazione per imporre il controllo centralizzato sulla creazione di istanze di account IAM Identity Center.

Per istruzioni su come allegare un SCP, consulta [Allegare e scollegare le politiche di controllo del servizio nella Guida per l'utente](#).AWS Organizations

Elimina la tua istanza IAM Identity Center

Quando un'istanza IAM Identity Center viene eliminata, tutti i dati in quell'istanza vengono eliminati e non possono essere recuperati. La tabella seguente descrive quali dati vengono eliminati in base al tipo di directory configurata in IAM Identity Center.

Quali dati vengono eliminati	Directory connessa - AWS Managed Microsoft AD, AD Connector o provider di identità esterno	Archivio di identità IAM Identity Center	
Tutti i set di autorizzazioni per cui hai configurato Account AWS	☑Sì	☑Sì	

Quali dati vengono eliminati	Directory connessa - AWS Managed Microsoft AD, AD Connector o provider di identità esterno	Archivio di identità IAM Identity Center	
Tutte le applicazioni che hai configurato in IAM Identity Center	☑Sì	☑Sì	
Tutte le assegnazioni utente Account AWS e le applicazioni che hai configurato	☑Sì	☑Sì	
Tutti gli utenti e i gruppi presenti nella directory o nell'archivio	N/D	☑Sì	

Se hai replicato l'istanza di IAM Identity Center in regioni aggiuntive, devi rimuovere tali regioni prima di eliminare l'istanza.

Utilizza la seguente procedura per eliminare l'istanza di IAM Identity Center.

Per eliminare la tua istanza IAM Identity Center

1. Apri la [console Centro identità IAM](#).
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 ogni casella di controllo per confermare di aver compreso che i tuoi dati verranno eliminati. Digita l'istanza di IAM Identity Center nella casella di testo, quindi scegli Conferma.

Abilita IAM Identity Center

Quando abiliti IAM Identity Center, scegli un tipo di AWS IAM Identity Center istanza da abilitare. Un'istanza di un servizio è una singola implementazione di un servizio all'interno del tuo AWS ambiente. Esistono due tipi di istanze disponibili per IAM Identity Center: istanze organizzative e istanze di account. I tipi di istanze disponibili da abilitare dipendono dal tipo di account a cui hai effettuato l'accesso.

L'elenco seguente identifica il tipo di istanze IAM Identity Center che puoi abilitare per ogni tipo di Account AWS

- 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. È possibile replicare questo tipo di istanza in regioni aggiuntive per una maggiore resilienza dell'accesso all'account e flessibilità nella scelta delle regioni di distribuzione delle applicazioni. AWS
- Il tuo account AWS Organizations membro: consente di 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 Organizations. È possibile associare solo un'istanza di IAM Identity Center a un'istanza standalone Account AWS e utilizzare tale istanza per le assegnazioni di applicazioni all'interno di tale istanza. Account AWS

Important

L'account di gestione dell'organizzazione può controllare se gli [account dei membri dell'organizzazione possono creare istanze di account di IAM Identity Center](#) utilizzando una Service Control Policy.

Se utilizzi un account di livello gratuito, la creazione di un' AWS organizzazione aggiorna automaticamente l'account a un piano a pagamento con pay-as-you-go prezzi. I crediti del livello gratuito scadono immediatamente. Per ulteriori informazioni, consulta [Piano gratuito AWS FAQs](#).

Per un confronto delle diverse funzionalità fornite dai diversi tipi di istanze, consulta [Istanze di organizzazione e account di IAM Identity Center](#).

Prima di abilitare IAM Identity Center, ti consigliamo di consultare il [Prerequisiti e considerazioni di IAM Identity Center](#).

Per abilitare un'istanza di IAM Identity Center

Scegli la scheda relativa al tipo di istanza IAM Identity Center che desideri abilitare, un'organizzazione o un'istanza di account:

Organization (recommended)

1. Effettua una delle seguenti operazioni per accedere a Console di gestione AWS.
 - 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 con una versione autonoma Account AWS (credenziali IAM): accedi utilizzando le tue credenziali IAM con autorizzazioni amministrative.
 - Già in uso AWS Organizations (credenziali IAM): accedi utilizzando le credenziali del tuo account di gestione.
2. Apri la [console Centro identità IAM](#).
3. (Facoltativo) Se desideri utilizzare una chiave KMS gestita dal cliente per la crittografia a riposo anziché la chiave AWS gestita predefinita, configura la chiave gestita dal cliente nella sezione Chiave per la crittografia dei dati di IAM Identity Center a riposo. Per ulteriori informazioni, vedi [Implementazione di chiavi KMS gestite dal cliente in AWS IAM Identity Center](#).

Important

Esegui questo passaggio solo se hai configurato le autorizzazioni necessarie per l'uso della chiave gestita dal cliente KMS. Senza le autorizzazioni appropriate, questo passaggio potrebbe fallire o interrompere l'amministrazione di IAM Identity Center e le applicazioni gestite. AWS

4. In Abilita il Centro identità IAM, scegli Abilita.

5. Nella AWS Organizations pagina Abilita IAM Identity Center con, esamina le informazioni e quindi seleziona Abilita per completare il processo.

 Note

AWS Organizations può avere IAM Identity Center abilitato solo in una singola AWS regione. Dopo aver abilitato IAM Identity Center, se è necessario modificare la regione in cui è abilitato IAM Identity Center, è necessario [eliminare](#) l'istanza corrente e creare un'istanza nell'altra regione.

Dopo aver abilitato l'istanza dell'organizzazione, ti consigliamo di eseguire i seguenti passaggi per completare la configurazione dell'ambiente:

- Conferma di utilizzare la fonte di identità di tua scelta. Se hai già un'origine di identità assegnata, puoi continuare a usarla. Per ulteriori informazioni, consulta [Conferma delle origini di identità nel Centro identità IAM](#).
- Registra un account membro come amministratore delegato. Per ulteriori informazioni, consulta [Amministrazione delegata](#).
- IAM Identity Center ti fornisce un portale di accesso alle AWS risorse. Se filtri l'accesso a AWS domini o endpoint URL specifici utilizzando una soluzione di filtraggio dei contenuti Web come firewall di nuova generazione (NGFW) o Secure Web Gateways (SWG), vedi. [Aggiorna firewall e gateway per consentire l'accesso a Portale di accesso AWS](#)

Account

1. Effettua una delle seguenti operazioni per accedere a. Console di gestione AWS
 - 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.
 - Già in uso AWS Organizations (credenziali IAM): accedi utilizzando le credenziali amministrative del tuo account membro.
2. Apri la [console Centro identità IAM](#).

3. Se sei nuovo AWS o ne hai uno standalone Account AWS, in Abilita IAM Identity Center, scegli Abilita.

Vedi la AWS Organizations pagina Abilita IAM Identity Center con. Consigliamo questa opzione, ma non è obbligatoria.

Seleziona il link abilita un'istanza di account di IAM Identity Center.

4. Se sei un amministratore di un account AWS Organizations membro, in Abilita un'istanza di account di IAM Identity Center, seleziona Abilita un'istanza di account.
5. Nella pagina Abilita un'istanza di account di IAM Identity Center, esamina le informazioni e, facoltativamente, aggiungi i tag che desideri associare a questa istanza di account. Quindi seleziona Abilita per completare il processo.

Note

Se il tuo AWS account è membro di un'organizzazione, potrebbero esserci delle restrizioni alla tua capacità di abilitare un'istanza di account di IAM Identity Center.

- Se la tua organizzazione ha abilitato IAM Identity Center prima del 15 novembre 2023, la possibilità per gli account membro di creare istanze di account è disabilitata per impostazione predefinita e deve essere abilitata dall'account di gestione dell'organizzazione.
- Se la tua organizzazione ha abilitato IAM Identity Center dopo il 15 novembre 2023, la possibilità per gli account membro di creare istanze di account è abilitata per impostazione predefinita. Tuttavia, le policy di controllo del servizio possono essere utilizzate per impedire la creazione di istanze di account di IAM Identity Center all'interno di un'organizzazione.

Per ulteriori informazioni, consultare [the section called “Consenti la creazione di istanze di account negli account dei membri”](#) e [the section called “SCPs per la creazione di istanze di account”](#).

Conferma delle origini di identità nel Centro identità IAM

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. Se hai già una fonte di identità assegnata, puoi continuare a usarla.

Se gestisci già utenti e gruppi in Active Directory un IdP esterno, 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](#).

Per confermare la fonte della tua identità

1. Apri la [console Centro identità IAM](#).
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, questo viene configurato automaticamente 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 e alle tue applicazioni. Per un tutorial sull'utilizzo di questa fonte di identità, consulta [Configura 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 Directory Service o utilizzando la directory autogestita in Active 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 [Microsoft ADelenco](#).

 Note

IAM Identity Center non supporta Simple AD SAMBA4 basato su sistema Simple AD come fonte di identità.

Provider di identità esterno

Per i provider di identità esterni (IdPs) come Okta o Microsoft 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 in modo che IAM Identity Center conosca 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, consulta [Tutorial sulle fonti di identità di IAM Identity Center](#).

 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 provider di identità esterni. Per ulteriori informazioni, consulta [Richiedi agli utenti l'MFA](#).

 Note

Se prevedi di replicare IAM Identity Center in altre regioni, dovrai configurare un provider di identità esterno. Per ulteriori dettagli, inclusi i prerequisiti, consulta. [Utilizzo di IAM Identity Center su più Regioni AWS](#)

Aggiorna firewall e gateway per consentire l'accesso a Portale di accesso AWS

Il portale di AWS accesso offre agli utenti l'accesso Single Sign-On a tutte le tue applicazioni cloud Account AWS e a quelle più 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.

 Note

AWS le applicazioni gestite si integrano con IAM Identity Center e lo utilizzano per l'autenticazione e i servizi di directory, ma potrebbero non utilizzare il portale di AWS accesso per l'accesso alle applicazioni.

Se filtri l'accesso a AWS domini o endpoint URL specifici utilizzando una soluzione di filtraggio dei contenuti Web come firewall di nuova generazione (NGFW) o Secure Web Gateways (SWG), devi consentire l'elenco dei domini e degli endpoint URL associati al portale di accesso. AWS

L'elenco seguente fornisce i domini dual-stack IPv4 e gli endpoint URL da aggiungere alle liste di autorizzazione della soluzione di filtraggio dei contenuti Web.

IPv4 elenco di consentiti

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

- `oidc.[Region].amazonaws.com`
- `*.sso.amazonaws.com`
- `*.sso.[Region].amazonaws.com`
- `*.sso-portal.[Region].amazonaws.com`
- `[Region].prod.pr.panorama.console.api.aws/panoramamaroute`
- `[Region].signin.aws`
- `[Region].signin.aws.amazon.com`
- `signin.aws.amazon.com`
- `*.cloudfront.net`
- `opfcaptcha-prod.s3.amazonaws.com`

Elenco di autorizzazioni dual-stack

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

Elenco combinato degli elementi consentiti (IPv4 + Dual-stack con compatibilità con le versioni precedenti)

- `[Directory ID or alias].awsapps.com`

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

Considerazioni sulla possibilità di inserire nella lista domini ed endpoint URL

Oltre ai requisiti per la lista consentita per il portale di AWS accesso, gli altri servizi e applicazioni utilizzati potrebbero richiedere l'inserimento di domini nell'elenco consentito.

- 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. Console di gestione AWS Per un elenco di domini, consulta la sezione [Risoluzione dei problemi](#) nella Guida Console di gestione AWS introduttiva. Console di gestione AWS

- 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.
- Se utilizzi software esterno, ad esempio esterno IdPs (ad esempio Okta eMicrosoft Entra ID), dovrai includere i relativi domini nelle tue liste di autorizzazione.

Tutorial sulle fonti di identità di IAM Identity Center

Puoi connettere la tua fonte di identità esistente nel tuo account di AWS Organizations gestione a [un'istanza organizzativa di IAM Identity Center](#). Se non disponi di un provider di identità esistente, puoi creare e gestire gli utenti direttamente nella directory predefinita di IAM Identity Center. Puoi avere una fonte di identità per organizzazione.

I tutorial di questa sezione descrivono come configurare un'istanza organizzativa di IAM Identity Center con una fonte di identità di uso comune, creare un utente amministrativo e, se si utilizza IAM Identity Center, per gestire l'accesso Account AWS, creare e configurare i set di autorizzazioni. Se utilizzi IAM Identity Center solo per l'accesso alle applicazioni, non è necessario utilizzare i set di autorizzazioni.

Questi tutorial non descrivono come configurare le istanze di account di IAM Identity Center. È possibile utilizzare le istanze di account per assegnare utenti e gruppi alle applicazioni, ma non è possibile utilizzare questo tipo di istanza per gestire l'accesso degli utenti a. Account AWS Per ulteriori informazioni, consulta [Istanze account del Centro identità IAM](#).

Note

Prima di iniziare uno di questi tutorial, abilita IAM Identity Center. Per ulteriori informazioni, consulta [Abilita IAM Identity Center](#).

Argomenti

- [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](#)
- [Tutorial video](#)

Utilizzo di Active Directory come origine di identità

Se gestisci gli utenti nella tua AWS Managed Microsoft AD directory utilizzando 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 utilizzi AWS Managed Microsoft AD, devi abilitare IAM Identity Center nello stesso Regione AWS punto 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, usa AWS Managed Microsoft AD. Per ulteriori informazioni, consulta:

- [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

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 [Microsoft ADelenco](#)
2. Segui 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 in [Microsoft ADelenco](#).
2. Segui 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 Centro identità IAM](#).
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 [Creare 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. Per ulteriori informazioni, consulta [Utilizzo della federazione delle identità SAML e SCIM con provider di identità esterni](#).

Note

CyberArk attualmente non supporta il servizio ACS (Multiple Assertion Consumer Service) SAML nell'applicazione. URL AWS IAM Identity Center Questa funzionalità SAML è necessaria per sfruttare appieno il [supporto multiregionale](#) in IAM Identity Center. Se prevedi di replicare IAM Identity Center in altre regioni, tieni presente che l'utilizzo di un singolo URL ACS può influire sull'esperienza utente in tali regioni aggiuntive. La tua regione principale continuerà a funzionare normalmente. Ti consigliamo di collaborare con il tuo fornitore IdP per abilitare questa funzionalità. Per ulteriori informazioni sull'esperienza utente in altre regioni con un singolo URL ACS, consulta e. [the section called “Utilizzo di applicazioni AWS gestite senza più ACS URLs”](#) [the section called “Account AWS resilienza di accesso senza più ACS URLs”](#)

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](#)
- [Considerazioni SCIM](#)
- [Fase 1: abilitare il provisioning in IAM Identity Center](#)
- [Fase 2: Configurare il provisioning in CyberArk](#)
- [\(Facoltativo\) Fase 3: Configurazione degli attributi utente in ABAC \(CyberArk for access control\) in IAM Identity Center](#)
- [\(Facoltativo\) Passaggio di attributi per il controllo degli accessi](#)

Prerequisiti

Prima di iniziare, avrai bisogno di quanto segue:

- CyberArk abbonamento 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 l'endpoint SCIM e il token di accesso. Dovrai incollarli in un secondo momento quando configuri il provisioning nel tuo IdP.
 - a. Endpoint SCIM: ad esempio, `https://scim.us-east-2.amazonaws.com/ /scim/v2111111111-2222-3333-4444-555555555555`
 - b. Token di accesso: scegli Mostra token per copiare il valore.

Warning

Questa è l'unica volta in cui puoi ottenere l'endpoint SCIM e il token di accesso. Assicurati di copiare questi valori prima di andare avanti. Inserirai questi valori per configurare il provisioning automatico nel tuo IdP più avanti in questo tutorial.

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 [Prerequisiti](#) provisioning SCIM.

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.
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 funzioni CyberArk. 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 di CyberArk.
 - b. Il valore dell'attributo è il nome dell'attributo inviato nell'asserzione SAML a IAM Identity Center.
4. Scegli Save (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'Nameattributo `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 Google Workspace IAM Identity Center

Se la tua organizzazione lo utilizza, Google Workspace puoi integrare i tuoi utenti 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 a Google Workspace.

Note

Google Workspace attualmente non supporta il servizio ACS (Multiple Assertion Consumer Service) SAML URLs nell'applicazione. AWS IAM Identity Center Questa funzionalità SAML è necessaria per sfruttare appieno il [supporto multiregionale](#) in IAM Identity Center. Se prevedi di replicare IAM Identity Center in altre regioni, tieni presente che l'utilizzo di un singolo URL ACS può influire sull'esperienza utente in tali regioni aggiuntive. La tua regione principale continuerà a funzionare normalmente. Ti consigliamo di collaborare con il tuo fornitore IdP per abilitare questa funzionalità. Per ulteriori informazioni sull'esperienza utente in altre regioni con un singolo URL ACS, consulta e. [the section called “Utilizzo di applicazioni AWS gestite senza più ACS URLs”](#) [the section called “Account AWS resilienza di accesso senza più ACS URLs”](#)

Le informazioni utente di Google Workspace vengono sincronizzate in IAM Identity Center utilizzando il protocollo [System for Cross-domain Identity Management \(SCIM\)](#) 2.0. Per ulteriori informazioni, consulta [Utilizzo della federazione delle identità SAML e SCIM con provider di identità esterni](#).

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 e connetterti al tuo 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 Workspace utilizzo 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 in questo tutorial. 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, consulta [Abilita IAM Identity Center](#).

Considerazioni

- Prima di configurare il provisioning SCIM tra IAM Identity Center 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 attualmente supportato. 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 1 Google 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 e Google 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 [Abilita 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 IAM Identity Assertion Consumer Service (ACS) e l'URL dell'emittente di IAM Identity Center. Dovrai fornirli URLs nella Console di Google amministrazione nel passaggio successivo.
 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 ACS URL e Entity ID. 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.
 9. Nella pagina dei dettagli del fornitore di servizi, completa i campi sotto Name 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 Directory attributo. 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 3 Google 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
 - a. ENDPOINT SCIM - Ad esempio,
 - IPv4 `https://scim.Region.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
 - Dual-stack `https://scim.Region.api.aws/1111111111-2222-3333-4444-555555555555/scim/v2`
 - b. Token di accesso: scegli Mostra token per copiare il valore.

 Warning

Questa è l'unica volta in cui puoi 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 5 Google 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 Endpoint URL e scegli Continua.

3. Verifica che tutti gli attributi obbligatori di IAM Identity Center (quelli contrassegnati con *) siano mappati agli Google Cloud Directory attributi. 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 configurato 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.

Passaggio di attributi per il controllo degli accessi - Facoltativo

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 `tagCostCenter = 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.

Assegna l'accesso a Account AWS

I seguenti passaggi sono necessari solo per concedere l'accesso a Account AWS . Questi passaggi non sono necessari per concedere l'accesso alle AWS applicazioni.

Note

Per completare questo passaggio, avrai bisogno di un'istanza organizzativa di IAM Identity Center. Per ulteriori informazioni, consulta [Istanze di organizzazione e account di IAM Identity Center](#).

Fase 1: IAM Identity Center: concedere Google Workspace agli utenti l'accesso agli account

1. Torna alla console IAM Identity Center. Nel riquadro di navigazione di IAM Identity Center, in Autorizzazioni multiaccount, scegli. Account AWS
2. Nella Account AWS pagina, 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
 - Scegli Next (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 Create (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 che la tua pagina 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. 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 attualmente supportato. Non è possibile creare gruppi per gli Google Workspace utenti utilizzando. Console di gestione AWS 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 2 Google Workspace: conferma dell'accesso Google Workspace degli utenti alle risorse AWS

1. Accedi Google utilizzando un account utente di prova. Per informazioni su come aggiungere utenti a Google 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. Viene visualizzata l'app Amazon Web Services.
4. Seleziona l'app Amazon Web Services. Hai effettuato l' AWS accesso al portale di accesso 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.
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. Console di gestione AWS
7. L'utente ha effettuato l'accesso alla console.

Fasi successive

Ora che hai configurato Google Workspace come provider di identità e hai effettuato il provisioning degli utenti in IAM Identity Center, puoi:

- Utilizza il comando [create-group](#) di AWS CLI Identity Store o l'API IAM [CreateGroup](#) per creare gruppi per i tuoi utenti.

I gruppi sono utili per assegnare l'accesso a Account AWS applicazioni e applicazioni. Aniché 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

Risoluzione dei problemi

Per la risoluzione generale dei problemi relativi a SCIM e SAML con Google Workspace, consulta le seguenti sezioni:

- [Alcuni utenti non riescono a sincronizzarsi in IAM Identity Center da un provider SCIM esterno](#)
- [Problemi relativi al contenuto delle asserzioni SAML create da IAM Identity Center](#)
- [Errore duplicato di utenti o gruppi durante il provisioning di utenti o gruppi con un provider di identità esterno](#)
- [Per la Google Workspace risoluzione dei problemi, consulta la documentazione Google Workspace.](#)

Le seguenti risorse possono aiutarti a risolvere i problemi mentre lavori con: AWS

- [AWS re:Post](#)- Trova FAQs e collega altre risorse per aiutarti a risolvere i problemi.
- [Supporto AWS](#)- Richiedere supporto tecnico

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 [Security Assertion Markup Language \(SAML\) 2.0](#). Per ulteriori informazioni, consulta [Utilizzo della federazione delle identità SAML e SCIM con provider di identità esterni](#).

Questa connessione viene configurata JumpCloud utilizzando l'endpoint e il token di accesso SCIM IAM Identity Center. 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](#)
- [Considerazioni SCIM](#)
- [Fase 1: Abilitare il provisioning in IAM Identity Center](#)
- [Fase 2: Configurare il provisioning in JumpCloud](#)
- [\(Facoltativo\) Fase 3: Configurazione degli attributi utente JumpCloud per il controllo degli accessi in IAM Identity Center](#)
- [\(Facoltativo\) Passaggio di attributi per il controllo degli accessi](#)

Prerequisiti

Prima di iniziare, avrai bisogno di quanto segue:

- JumpCloud abbonamento 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 [JumpCloud documentazione per IAM Identity Center](#).
- Se hai replicato IAM Identity Center in altre regioni, devi aggiornare la configurazione del provider di identità per consentire l'accesso alle applicazioni AWS gestite e Account AWS da tali regioni. Per ulteriori dettagli, consultare [the section called “Fase 3: Aggiornare la configurazione dell'IdP esterno”](#). Consulta la JumpCloud documentazione per ulteriori dettagli.
- 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.

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 l'endpoint SCIM e il token di accesso. Dovrai incollarli in un secondo momento quando configuri il provisioning nel tuo IdP.
 - a. Endpoint SCIM: ad esempio, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
 - b. Token di accesso: scegli Mostra token per copiare il valore.

 Warning

Questa è l'unica volta in cui puoi ottenere l'endpoint SCIM e il token di accesso. Assicurati di copiare questi valori prima di andare avanti. Inserirai questi valori per configurare il provisioning automatico nel tuo IdP più avanti in questo tutorial.

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.
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. Scegli Save (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'Nameattributo `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 tagCostCenter = 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 Center supporta 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. Per ulteriori informazioni, consulta [Utilizzo della federazione delle identità SAML e SCIM con provider di identità esterni](#).

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 [Avvio rapido: configurazione di un tenant](#) nella documentazione. Microsoft
- Un account AWS IAM Identity Center abilitato. Per ulteriori informazioni, consulta [Enable IAM Identity Center](#) nella Guida per l'AWS IAM Identity Center utente.

Considerazioni

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.

Provisioning automatico

Prima di iniziare a distribuire SCIM, ti consigliamo di esaminarlo. [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 in Microsoft Entra ID, tale attributo non verrà rimosso dall'utente corrispondente in IAM Identity Center. Questa è una limitazione nota in Microsoft 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 in gruppi nidificati. Solo gli utenti che sono membri immediati di un gruppo assegnato in modo esplicito possono essere letti e assegnati. Microsoft Entra ID non decompone 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 In alternativa, puoi utilizzare la [sincronizzazione AD configurabile di IAM Identity Center](#) per integrare i Active Directory gruppi con IAM Identity Center.

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 documentazione.

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 in Microsoft Entra ID. Questa applicazione ti servirà in seguito per configurare la tua connessione SAML con AWS.

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 Center tra i risultati.
5. Scegli Create (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, immettete **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 Microsoft 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 riquadro 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 Center app 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 Center dall'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 Center app.

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 Center AWS

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. Console di gestione AWS 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 Centro identità IAM](#).
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. Scegli Next (Successivo).
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 Rivedi e crea, scegli 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 Centro identità IAM](#).
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 Microsoft Entra ID dell'utente. Ad esempio, NikkiWolf@***example.org***.
 - b. Conferma 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 Centro identità IAM](#).

2. In Autorizzazioni per più account, 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.

5.
Example

<caption>On the Seleziona i set di autorizzazioni page, choose the RegionalAdmin permission set created in Step 2.1, and then choose Next.</caption>

6. Nella pagina Rivedi e invia, esamina le selezioni effettuate, quindi scegli Invia.

Passaggio 3: configura e verifica la 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 fornitore di servizi, scegli Default IPv4 o Dual-stack. Puoi scaricare il file di metadati del fornitore di servizi dopo aver completato la modifica dell'origine dell'identità.
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 in Microsoft 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 2. Configura Single Sign-on.
3. Nella pagina Configura Single Sign-On con SAML, scegli SAML. Quindi 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 di configurazione SAML di base, verifica che entrambi i valori Identifier e Reply URL (Assertion Consumer Service URL) puntino ora agli endpoint in. AWS
 - Identificatore: si tratta dell'URL dell'emittente di IAM Identity Center. Lo stesso valore si applica indipendentemente dal fatto che si utilizzino endpoint IPv4 -only o dual-stack.
 - URL di risposta (Assertion Consumer Service URL) - I valori qui includono sia gli endpoint IPv4 -only che quelli dual-stack provenienti da tutte le regioni abilitate del tuo IAM Identity Center. Puoi utilizzare l'URL ACS della regione principale come URL predefinito in modo che gli utenti vengano reindirizzati alla regione principale quando avviano l'applicazione Amazon Web Services da Microsoft Entra ID. Per ulteriori informazioni su ACS URLs, consulta [Endpoint ACS primari e aggiuntivi Regioni AWS](#).
 - (Facoltativo) Se hai replicato IAM Identity Center in altre regioni, puoi anche creare un'app Microsoft Entra ID per aggiungere segnalibri al portale di AWS accesso in ogni regione aggiuntiva. Ciò consente agli utenti di accedere al portale di AWS accesso in altre regioni da Microsoft Entra ID. Assicurati di concedere ai tuoi utenti le autorizzazioni per accedere alle app per i segnalibri in Microsoft Entra ID. Consulta [Microsoft Entra ID la documentazione](#) per maggiori dettagli. Se prevedi di replicare IAM Identity Center in altre regioni in un secondo momento, consulta [Microsoft Entra ID configurazione per l'accesso a](#)

[regioni aggiuntive](#) la pagina dedicata alle indicazioni su come abilitare l'accesso alle regioni aggiuntive dopo questa configurazione iniziale.

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 con AWS 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. Scegli Next (Successivo).
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 Center applicazione 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 riquadro 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 il display sia visualizzato. Account AWS

 Tip

Se la pagina è vuota e non viene Account AWS visualizzata, 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 la scheda Account per visualizzare l'elenco degli account. Vengono visualizzati i nomi degli account IDs, gli 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**). Ciò 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 Console di gestione AWS 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 AWS Regioni. 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) in Microsoft 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. Scegliete Proprietà, quindi fornite i seguenti valori:
 - Nome - Invio **Richard**
 - Cognome - Invio **Roe**
 - Job title - Enter **Marketing Lead**
 - Dipartimento - Entra **Sales**
 - ID dipendente: inserisci **12345**
7. Scegli Review + create, 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,
 - IPv4: `https://scim.aws-region.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
 - Doppio stack: `https://scim.aws-region.api.aws/1111111111-2222-3333-4444-555555555555/scim/v2`
 - b. Token di accesso: scegli Mostra token per copiare il valore.

 Warning

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

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 4.2** 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. Scegli Save (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.

Fase 5: Configurazione di ABAC - Opzionale

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.

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

Configure user attributes in ID Microsoft Entra for access control in IAM Identity Center

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 [Creare 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. In **Nome**, inserisci `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. Scegli **Save** (Salva).

Configure ABAC using IAM Identity Center

Configura ABAC utilizzando IAM Identity Center

Con questo metodo, utilizzi la [Attributi per il controllo degli accessi](#) funzionalità di IAM Identity Center per passare un `Attribute` elemento con l'`NameAttribute` `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 `Department=billing`, usa il seguente attributo:

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

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

Assegna l'accesso a Account AWS

I seguenti passaggi sono necessari solo per concedere l'accesso a Account AWS . Questi passaggi non sono necessari per concedere l'accesso alle AWS applicazioni.

Note

Per completare questo passaggio, avrai bisogno di un'istanza organizzativa di IAM Identity Center. Per ulteriori informazioni, consulta [Istanze di organizzazione e account di IAM Identity Center](#).

Fase 1: IAM Identity Center: concedere Microsoft Entra ID agli utenti l'accesso agli account

1. Torna alla console IAM Identity Center. Nel riquadro di navigazione di IAM Identity Center, in Autorizzazioni multiaccount, scegli. Account AWS
2. Nella Account AWS pagina, 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
 - Scegli Next (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 Create (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

Fase 2 Microsoft Entra ID: Conferma l'accesso Microsoft Entra ID degli utenti alle AWS risorse

1. Torna alla Microsoft Entra ID console e accedi all'applicazione Sign-on basata su SAML di IAM Identity Center.
 2. Seleziona Utenti e gruppi e seleziona Aggiungi utenti o gruppi. Aggiungerai all'Microsoft Entra ID applicazione l'utente creato in questo tutorial nel passaggio 4. Aggiungendo l'utente, gli consentirai di accedere a AWS. Cerca l'utente che hai creato allo Step 4. Se seguissi questo passaggio, lo sarebbe **RichardRoe**.
- Per una demo, consulta [Federare l'istanza esistente di IAM Identity Center](#) con Microsoft Entra ID

Microsoft Entra ID configurazione per l'accesso a regioni aggiuntive di IAM Identity Center - Opzionale

Se hai replicato IAM Identity Center in altre regioni, devi aggiornare la configurazione del provider di identità per consentire l'accesso alle applicazioni AWS gestite e Account AWS tramite le regioni aggiuntive. I passaggi seguenti ti guidano attraverso la procedura. Per ulteriori dettagli su questo argomento, inclusi i prerequisiti, vedere [Utilizzo di IAM Identity Center su più Regioni AWS](#).

1. Recupera ACS URLs per le regioni aggiuntive dalla console IAM Identity Center come descritto in. [Endpoint ACS primari e aggiuntivi Regioni AWS](#)
2. Nella console dell'interfaccia di [amministrazione Microsoft Entra](#), accedi a Identità > Applicazioni > Applicazioni aziendali, quindi scegli AWS IAM Identity Center.
3. A sinistra, scegli 2. Configura Single Sign-on.
4. Nella pagina Configurazione SAML di base, nella sezione URL di risposta (Assertion Consumer Service URL), scegli Aggiungi URL di risposta per l'URL ACS di ogni regione aggiuntiva. Puoi mantenere gli URL ACS della regione principale come quelli predefiniti in modo che gli utenti continuino a essere reindirizzati alla regione principale quando avviano l'applicazione. AWS IAM Identity Center Microsoft Entra ID
5. Al termine dell'aggiunta dell'ACS URLs, salvate l'applicazione. AWS IAM Identity Center
6. Puoi creare un'app di segnalibri Microsoft Entra ID per il portale di AWS accesso in ogni regione aggiuntiva. Ciò consente agli utenti di accedere al portale di AWS accesso in altre regioni da Microsoft Entra ID. Assicurati di concedere ai tuoi utenti le autorizzazioni per accedere alle app per i segnalibri in. Microsoft Entra ID Consulta [Microsoft Entra ID la documentazione](#) per maggiori dettagli.
7. Verifica di poter accedere al portale di AWS accesso in ogni regione aggiuntiva. Vai al [portale di AWS accesso URLs](#) o avvia le app per aggiungere segnalibri da Microsoft Entra ID.

Risoluzione dei problemi

Per la risoluzione generale dei problemi relativi a SCIM e SAML con Microsoft Entra ID, consulta le seguenti sezioni:

- [Problemi di sincronizzazione con IAM Identity Microsoft Entra ID Center](#)
- [Alcuni utenti non riescono a sincronizzarsi in IAM Identity Center da un provider SCIM esterno](#)
- [Problemi relativi al contenuto delle asserzioni SAML create da IAM Identity Center](#)

- [Errore duplicato di utenti o gruppi durante il provisioning di utenti o gruppi con un provider di identità esterno](#)
- [Risorse aggiuntive](#)

Problemi di sincronizzazione con IAM Identity Microsoft Entra ID Center

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 consiste nel rivedere gli attributi dell'utente in Microsoft 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'unico attributo principale phoneNumbers.

[Per suggerimenti generali sulla risoluzione dei problemi SCIM, consulta Risoluzione dei problemi.](#)

Microsoft Entra IDSincronizzazione dell'account ospite

Se desideri sincronizzare i tuoi utenti Microsoft Entra ID ospiti con IAM Identity Center, consulta la seguente procedura.

Microsoft Entra ID l'email degli utenti ospiti è diversa da quella Microsoft Entra ID degli utenti. Questa differenza causa problemi durante il tentativo di sincronizzare gli utenti Microsoft Entra ID guest con IAM Identity Center. Ad esempio, consulta il seguente indirizzo email per un utente ospite:

`exampleuser_domain.com#EXT#@domain.onmicrosoft.com.`

IAM Identity Center non prevede che l'indirizzo e-mail contenga il `#EXT#@domain` formato.

1. Accedi all'interfaccia di [amministrazione di Microsoft Entra](#) e vai a Identità > Applicazioni > Applicazioni aziendali, quindi scegli AWS IAM Identity Center
2. Vai alla scheda Single Sign On nel riquadro a sinistra.
3. Seleziona Modifica che appare accanto a Attributi utente e reclami.
4. Seleziona Identificatore utente univoco (ID nome) dopo i reclami obbligatori.
5. Creerai due condizioni di reclamo per i tuoi Microsoft Entra ID utenti e gli utenti ospiti:
 - a. Per Microsoft Entra ID gli utenti, crea un tipo di utente per i membri con l'attributo source impostato su `user.userprincipalname`.
 - b. Per gli utenti Microsoft Entra ID ospiti, crea un tipo di utente per ospiti esterni con l'attributo source impostato su `user.mail`.
 - c. Seleziona Salva e riprova ad accedere come utente Microsoft Entra ID ospite.

Risorse aggiuntive

- Per suggerimenti generali sulla risoluzione dei problemi SCIM, consulta [Risoluzione dei problemi relativi a IAM Identity Center](#)
- Per la Microsoft Entra ID risoluzione dei problemi, consultate la [Microsoft documentazione](#).
- Per ulteriori informazioni sulla federazione tra più utenti Account AWS, consulta [Proteggere Account AWS con Azure Active Directory Federation](#).

Le seguenti risorse possono aiutarti a risolvere i problemi mentre lavori con: AWS

- [AWS re:Post](#)- Trova FAQs e collega altre risorse per aiutarti a risolvere i problemi.
- [Supporto AWS](#)- Richiedi supporto tecnico

Configura SAML e SCIM con Okta IAM Identity Center

Puoi fornire o sincronizzare automaticamente le informazioni su utenti e gruppi da Okta IAM Identity Center utilizzando il protocollo [System for Cross-domain Identity Management \(SCIM\)](#) 2.0. Per ulteriori informazioni, consulta [Utilizzo della federazione delle identità SAML e SCIM con provider di identità esterni](#).

Per configurare questa connessione Okta, 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 account Okta.

Okta supporta 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.

- Importa utenti: gli utenti possono essere importati da IAM Identity Center a Okta.

Obiettivo

In questo tutorial, illustrerai come configurare una connessione SAML con Okta IAM Identity Center. Successivamente, sincronizzerai gli utenti da Okta, 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.

Le seguenti funzionalità sono supportate durante la connessione Okta a IAM Identity Center tramite SAML:

- Accesso SAML avviato da IdP: gli utenti accedono tramite il Okta portale e ottengono l'accesso a IAM Identity Center.
- Accesso SAML avviato da SP: gli utenti accedono al portale di accesso, che li reindirizza all' AWS accesso tramite il portale. Okta

Note

[Puoi registrare un Okta account \(prova gratuita\) su cui è installata l'applicazione IAM Identity Center. Okta's](#) 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.

Se non hai ancora abilitato IAM Identity Center, consulta [Abilita IAM Identity Center](#).

Considerazioni

- Prima di configurare il provisioning SCIM tra Okta e IAM Identity Center, ti consigliamo di effettuare una prima revisione. [Considerazioni sull'utilizzo del provisioning automatico](#)
- Per ogni Okta utente deve essere specificato il valore 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.
- Quando viene utilizzato Okta con IAM Identity Center, IAM Identity Center è generalmente configurato come applicazione inOkta. Ciò consente di configurare più istanze di IAM Identity Center come più applicazioni, supportando l'accesso a più AWS Organizations, all'interno di una singola istanza di Okta

- 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.
- Se hai replicato IAM Identity Center in altre regioni, devi aggiornare la configurazione del provider di identità per consentire l'accesso alle applicazioni AWS gestite e Account AWS tramite regioni aggiuntive. Per ulteriori dettagli, inclusi i prerequisiti, consulta. [Utilizzo di IAM Identity Center su più Regioni AWS](#) I passaggi specifici di Okta sono descritti in [Oktaconfigurazione per l'accesso a regioni aggiuntive](#)

Passaggio 1Okta: 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 comemetadata.xml.

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

Fase 2: IAM Identity Center: 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, copia i seguenti elementi in un file di testo per accedervi facilmente:
 - URL IAM Identity Center Assertion Consumer Service (ACS): puoi scegliere tra ACS IPv4-only e dual-stack. URLs Inoltre, se l'istanza IAM Identity Center è abilitata in più regioni, ogni regione aggiuntiva ha il proprio ACS dual-stack e unico. IPv4 URLs Per ulteriori informazioni su ACS, consulta. URLs [Endpoint ACS primari e aggiuntivi Regioni AWS](#)
 - URL dell'emittente di IAM Identity Center

Questi valori ti serviranno più avanti in questo tutorial.

- b. In Metadati del provider di identità, in Metadati SAML IdP, seleziona Scegli file, quindi seleziona metadata.xml il file creato nel passaggio precedente.
 - c. Scegli Next (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 utilizzarla nel passaggio successivo.

8. Torna alla scheda Accedi dell' AWS IAM Identity Center app Okta admin dashboard e seleziona Modifica.
9. In Impostazioni di accesso avanzate inserisci quanto segue:
 - Per l'URL ACS, inserisci i valori che hai copiato per l'URL di IAM Identity Center Assertion Consumer Service (ACS). Puoi utilizzare l'URL ACS della regione principale come URL predefinito in modo che gli utenti vengano reindirizzati alla regione principale quando avviano l'applicazione Amazon Web Services da. Okta
 - (Facoltativo) Se hai replicato IAM Identity Center in altre regioni, puoi anche creare un'app Okta per aggiungere segnalibri al portale di AWS accesso in ogni regione aggiuntiva. Ciò consente agli utenti di accedere al portale di AWS accesso in altre regioni da. Okta Assicurati di concedere ai tuoi utenti le autorizzazioni per accedere alle app per i segnalibri in. Okta Consulta [Okta documentazione](#) per maggiori dettagli. Se prevedi di replicare IAM Identity Center in altre regioni in un secondo momento, consulta [Okta configurazione per l'accesso a regioni aggiuntive](#) la pagina dedicata alle indicazioni su come abilitare l'accesso alle regioni aggiuntive dopo questa configurazione iniziale.
 - Per l'URL dell'emittente, inserisci il valore che hai copiato per l'URL emittente di IAM Identity Center

- Per il formato del nome utente dell'applicazione, seleziona una delle opzioni dal menu.

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

10. Scegli Save (Salva).

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

Fase 3: IAM Identity Center eOkta: Esegui il provisioning Okta degli utenti

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:
 - a. Endpoint SCIM - Il formato dell'endpoint dipende dalla configurazione in uso:
 - IPv4: `https://scim.us-east-2.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
 - Doppio stack: `https://scim.us-east-2.api.aws/1111111111-2222-3333-4444-555555555555/scim/v2`
 - b. Token di accesso: scegli Mostra token per copiare il valore.

Warning

Questa è l'unica volta in cui puoi ottenere l'endpoint SCIM e il token di accesso. Assicurati di copiare questi valori prima di andare avanti. Inserirai questi valori per configurare il provisioning automatico Okta più avanti in questo tutorial.

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 automatico.
7. Configura Okta con i valori di provisioning SCIM copiati in precedenza in AWS IAM Identity Center questo passaggio:
 - a. Nel campo URL di base, inserisci il valore dell'endpoint SCIM.
 - 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. Scegli Save (Salva). Verrai spostato nella sezione 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. Scegli Save (Salva).

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

Fase 4Okta: 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. AWS 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 desideri sincronizzare con IAM Identity Center. Scegli Save (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. Per aggiungere singoli Okta utenti a IAM Identity Center, utilizza i seguenti passaggi:
 - a. Nella pagina Assegnazioni, scegli Assegna, quindi scegli Assegna a persone.
 - b. 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.

5. 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 di attributi per il controllo degli accessi - Facoltativo

Facoltativamente, puoi utilizzare la [Attributi per il controllo degli accessi](#) funzionalità di IAM Identity Center per passare un `Attribute` elemento con l'`NameAttribute` `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 `tagCostCenter = 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.

Assegna l'accesso a Account AWS

I seguenti passaggi sono necessari solo per concedere l'accesso a Account AWS . Questi passaggi non sono necessari per concedere l'accesso alle AWS applicazioni.

 Note

Per completare questo passaggio, avrai bisogno di un'istanza organizzativa di IAM Identity Center. Per ulteriori informazioni, consulta [Istanze di organizzazione e account di IAM Identity Center](#).

Fase 1: IAM Identity Center: 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 AWS pagina, 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. AdministratorAccessScegli Next (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 Create (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 dei set di autorizzazioni, scegli il pulsante Aggiorna. Il set di *AdministratorAccess* autorizzazioni creato viene visualizzato nell'elenco. Seleziona la casella di controllo per quel set di autorizzazioni, quindi scegli Avanti.

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

La pagina viene aggiornata con un messaggio che indica che la tua pagina 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. Quando l'utente accede, avrà la possibilità di scegliere il ruolo. *AdministratorAccess*

Fase 2Okta: Conferma dell'accesso Okta degli utenti alle risorse AWS

1. Accedi utilizzando un account di prova aOkta dashboard.
2. In Le mie app, seleziona l'AWS IAM Identity Center icona.
3. Dovresti 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 AdministratorAccess autorizzazioni.
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 l'accesso sia all'accesso programmatico che all' Console di gestione AWS accesso programmatico. Seleziona Console di gestione per aprire. Console di gestione AWS
6. L'utente ha effettuato l'accesso a Console di gestione AWS.

È inoltre possibile utilizzare il portale di AWS accesso. Questo reindirizza l'utente all'accesso tramite il Okta portale prima di accedere al portale di AWS accesso. Questo percorso segue il flusso di accesso SAML avviato da SP.

Oktaconfigurazione per l'accesso a regioni aggiuntive di IAM Identity Center - Facoltativa

Se hai replicato IAM Identity Center in altre regioni, devi aggiornare la configurazione del provider di identità per consentire l'accesso alle applicazioni AWS gestite e Account AWS tramite le regioni aggiuntive. I passaggi seguenti ti guidano attraverso la procedura. Per ulteriori dettagli su questo argomento, inclusi i prerequisiti, vedere [Utilizzo di IAM Identity Center su più Regioni AWS](#).

1. Recupera ACS URLs per le regioni aggiuntive dalla console IAM Identity Center come descritto in. [Endpoint ACS primari e aggiuntivi Regioni AWS](#)
2. Nel pannello di navigazione della dashboard di Okta amministrazione, scegli Applicazioni, quindi di nuovo Applicazioni nell'elenco espanso.
3. Scegliere l'applicazione AWS IAM Identity Center.
4. Scegli la scheda Sign On (Accedi).
5. In Impostazioni avanzate di accesso e altri SSO richiedibili URLs, scegli Aggiungi un altro URL ACS per ogni regione aggiuntiva e incolla l'URL ACS nel campo di testo.
6. Al termine dell'aggiunta dell'ACS, salva l'applicazione. URLs AWS IAM Identity Center
7. Puoi creare un'app di segnalibri Okta per il portale di AWS accesso in ogni regione aggiuntiva. Ciò consente agli utenti di accedere al portale di AWS accesso in altre regioni daOkta. Assicurati di concedere ai tuoi utenti le autorizzazioni per accedere alle app per i segnalibri in. Okta Consulta [Okta documentazione](#) per maggiori dettagli.
8. Verifica di poter accedere al portale di AWS accesso in ogni regione aggiuntiva. Vai al [portale di AWS accesso URLs](#) o avvia le app per aggiungere segnalibri daOkta.

Fasi successive

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

- Concedi l'accesso a Account AWS, vedi [Assegna l'accesso a utenti o gruppi a Account AWS](#).
- Concedi l'accesso alle applicazioni cloud, vedi [Assegna 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](#).

Risoluzione dei problemi

Per la risoluzione generale dei problemi relativi a SCIM e SAML con Okta, consulta le seguenti sezioni:

- [Riassegnazione del provisioning a utenti e gruppi eliminati da IAM Identity Center](#)
- [Errore di provisioning automatico in Okta](#)
- [Alcuni utenti non riescono a sincronizzarsi in IAM Identity Center da un provider SCIM esterno](#)
- [Problemi relativi al contenuto delle asserzioni SAML create da IAM Identity Center](#)
- [Errore duplicato di utenti o gruppi durante il provisioning di utenti o gruppi con un provider di identità esterno](#)
- [Risorse aggiuntive](#)

Riassegnazione del provisioning a utenti e gruppi eliminati da IAM Identity Center

- Potresti ricevere il seguente messaggio di errore nella Okta Console, se stai tentando di modificare un utente o un gruppo Okta che una volta era sincronizzato e poi eliminato da IAM Identity Center:
 - Invio automatico del profilo dall'utente *Jane Doe* all'app AWS IAM Identity Center non riuscito: errore durante il tentativo di inviare l'aggiornamento del profilo per *jane_doe@example.com*: Nessun utente restituito per l'utente *xxxxx-xxxxxx-xxxxx-xxxxxx*
 - Il gruppo collegato è mancante in AWS IAM Identity Center. Modifica il gruppo collegato per riprendere a richiedere l'iscrizione al gruppo.
- Potresti anche ricevere il seguente messaggio di errore nei registri Okta di sistema per utenti o gruppi di IAM Identity Center sincronizzati ed eliminati:
 - Errore Okta: Eventfailed application.provision.user.push_profile: nessun utente restituito per l'utente *xxxxx-xxxxxx-xxxxx-xxxxxx*
 - Errore Okta: application.provision.group_push.mapping.update.or.delete.failed.with.error: il gruppo collegato è mancante in AWS IAM Identity Center. Modifica il gruppo collegato per riprendere l'iscrizione al gruppo.

 Warning

Gli utenti e i gruppi devono essere eliminati da IAM Identity Center Okta anziché da IAM Identity Center se hai sincronizzato IAM Identity Center Okta utilizzando SCIM.

Risoluzione dei problemi relativi agli utenti IAM Identity Center eliminati

Per risolvere questo problema con gli utenti IAM Identity Center eliminati, è necessario eliminare gli utenti da Okta. Se necessario, anche questi utenti dovrebbero essere ricreati in Okta. Quando l'utente viene ricreato in Okta, verrà anche reinserito nell'IAM Identity Center tramite SCIM. [Per ulteriori informazioni sull'eliminazione di un utente, consulta la documentazione. Okta](#)

 Note

Se devi rimuovere l'accesso di un Okta utente a IAM Identity Center, devi prima rimuoverlo dal suo Group Push e poi dal suo Assignment Group in Okta. Ciò garantisce che l'utente venga rimosso dall'appartenenza al gruppo associato in IAM Identity Center. Per ulteriori informazioni sulla risoluzione dei problemi di Group Push, consulta [Okta la documentazione](#).

Risoluzione dei problemi relativi ai gruppi IAM Identity Center eliminati

Per risolvere questo problema con i gruppi IAM Identity Center eliminati, è necessario eliminare il gruppo da Okta. Se necessario, questi gruppi dovrebbero anche essere ricreati in Okta utilizzando Group Push. Quando l'utente viene ricreato in Okta, verrà anche reinserito nell'IAM Identity Center tramite SCIM. [Per ulteriori informazioni sull'eliminazione di un gruppo, consulta la documentazione di Okta.](#)

Errore di provisioning automatico in Okta

Se viene visualizzato il seguente messaggio di errore in Okta:

Impossibile eseguire il provisioning automatico dell'utente Jane Doe all'app: utente corrispondente AWS IAM Identity Center non trovato

Per ulteriori informazioni, [Okta consulta la documentazione](#).

Risorse aggiuntive

- Per suggerimenti generali sulla risoluzione dei problemi SCIM, vedere [Risoluzione dei problemi relativi a IAM Identity Center](#).

Le seguenti risorse possono aiutarti a risolvere i problemi mentre lavori con: AWS

- [AWS re:Post](#)- Trova FAQs e collega altre risorse per aiutarti a risolvere i problemi.
- [Supporto AWS](#)- Richiedere supporto tecnico

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. Per ulteriori informazioni, consulta [Utilizzo della federazione delle identità SAML e SCIM con provider di identità esterni](#).

Note

OneLogin attualmente non supporta il servizio ACS (Multiple Assertion Consumer Service) SAML nell'applicazione. URLs AWS IAM Identity Center Questa funzionalità SAML è necessaria per sfruttare appieno il [supporto multiregionale](#) in IAM Identity Center. Se prevedi di replicare IAM Identity Center in altre regioni, tieni presente che l'utilizzo di un singolo URL ACS può influire sull'esperienza utente in tali regioni aggiuntive. La tua regione principale continuerà a funzionare normalmente. Ti consigliamo di collaborare con il tuo fornitore IdP per abilitare questa funzionalità. Per ulteriori informazioni sull'esperienza utente in altre regioni con un singolo URL ACS, consulta e. [the section called “Utilizzo di applicazioni AWS gestite senza più ACS URLs”](#) [the section called “Account AWS resilienza di accesso senza più ACS URLs”](#)

Puoi configurare questa connessione in OneLogin, 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](#)
- [Fase 1: abilitare il provisioning in IAM Identity Center](#)
- [Passaggio 2: configurare il provisioning in OneLogin](#)
- [\(Facoltativo\) Passaggio 3: configura gli attributi utente OneLogin per il controllo degli accessi in IAM Identity Center](#)
- [\(Facoltativo\) Passaggio di attributi per il controllo degli accessi](#)
- [Risoluzione dei problemi](#)

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 l'endpoint SCIM e il token di accesso. Dovrai incollarli in un secondo momento quando configuri il provisioning nel tuo IdP.
 - a. Endpoint SCIM: ad esempio, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
 - b. Token di accesso: scegli Mostra token per copiare il valore.

 Warning

Questa è l'unica volta in cui puoi ottenere l'endpoint SCIM e il token di accesso. Assicurati di copiare questi valori prima di andare avanti. Inserirai questi valori per configurare il provisioning automatico nel tuo IdP più avanti in questo tutorial.

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 con OneLogin, consulta [Enabling Single Sign-On Between and on the Partner Network blog](#). OneLogin AWS AWS

Per configurare il provisioning in OneLogin

1. Accedi a OneLogin, 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 Configurazione dal pannello di navigazione.
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. 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. Nel riquadro di navigazione, scegli Provisioning.
6. Seleziona le caselle di controllo Abilita provisioning, Crea utente, Elimina utente e Aggiorna utente, quindi scegli Salva.
7. Nel pannello di navigazione, seleziona 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, and/or 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 a OneLogin, 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 dal pannello di navigazione.
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. Scegli Save (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'Nameattributo `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 A tale scopo, 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 in OneLogin, 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 azioni OneLogin, inclusi gli eventi di sincronizzazione, in Attività > Eventi.

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

OneLogin attualmente 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 user/group di sincronizzazione

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, in OneLogin, 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 gruppo OneLogin, 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](#)
- [PingOne](#)

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. Per ulteriori informazioni, consulta [Utilizzo della federazione delle identità SAML e SCIM con provider di identità esterni](#).

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 di PingFederate.

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](#)
- [Considerazioni](#)
- [Fase 1: abilitare il provisioning in IAM Identity Center](#)
- [Fase 2: Configurare il provisioning in PingFederate](#)
- [\(Facoltativo\) Fase 3: Configurazione degli attributi utente in base alla frequenza per PingFed il controllo degli accessi in IAM Identity Center](#)
- [\(Facoltativo\) Passaggio di attributi per il controllo degli accessi](#)
- [Risoluzione dei problemi](#)

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 Ping Identity sito Web.
- 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» in PingFederate, 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.
- Se hai replicato IAM Identity Center in altre regioni, devi aggiornare la configurazione del provider di identità per consentire l'accesso alle applicazioni AWS gestite e da tali regioni. Account AWS Per ulteriori dettagli, consultare [the section called “Fase 3: Aggiornare la configurazione dell'IdP esterno”](#). Consulta la PingFederate documentazione per ulteriori dettagli.

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 in PingFederate, 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 l'endpoint SCIM e il token di accesso. Dovrai incollarli in un secondo momento quando configuri il provisioning nel tuo IdP.

- a. Endpoint SCIM: ad esempio, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-55555555555`
- b. Token di accesso: scegli Mostra token per copiare il valore.

 Warning

Questa è l'unica volta in cui puoi ottenere l'endpoint SCIM e il token di accesso. Assicurati di copiare questi valori prima di andare avanti. Inserirai questi valori per configurare il provisioning automatico nel tuo IdP più avanti in questo tutorial.

5. Scegli Chiudi.

Ora che hai configurato il provisioning nella console IAM Identity Center, devi completare le attività rimanenti utilizzando la console PingFederate amministrativa. 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, consultare la documentazione di Ping. In sintesi, è necessario modificare `l'pf.provisioner.mode` impostazione nel `pingfederate-<version>/pingfederate/bin/run.properties` file con un valore diverso da OFF (che è l'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 con PingFederate.

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 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 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 **AWSIAMIdentityCenterchannel1**) 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 in PingFederate.

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 in PingFederate.

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'Nameattributo <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 tagCostCenter = 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

Per la risoluzione generale dei problemi relativi a SCIM e SAML con PingFederate, consulta le seguenti sezioni:

- [Alcuni utenti non riescono a sincronizzarsi in IAM Identity Center da un provider SCIM esterno](#)

- [Problemi relativi al contenuto delle asserzioni SAML create da IAM Identity Center](#)
- [Errore duplicato di utenti o gruppi durante il provisioning di utenti o gruppi con un provider di identità esterno](#)
- [Per ulteriori informazioni su PingFederate, consulta PingFederate la documentazione.](#)

Le seguenti risorse possono aiutarti a risolvere i problemi mentre lavori con: AWS

- [AWS re:Post](#)- Trova FAQs e collega altre risorse per aiutarti a risolvere i problemi.
- [Supporto AWS](#)- Richiedere supporto tecnico

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.

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](#)
- [Considerazioni](#)
- [Passaggio 1: abilitare il provisioning in IAM Identity Center](#)
- [Fase 2: Configurare il provisioning in PingOne](#)

- [\(Facoltativo\) Fase 3: Configurazione degli attributi utente PingOne per il controllo degli accessi in IAM Identity Center](#)
- [\(Facoltativo\) Passaggio di attributi per il controllo degli accessi](#)
- [Risoluzione dei problemi](#)

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 Identity](#) sito 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
- Se hai replicato IAM Identity Center in altre regioni, devi aggiornare la configurazione del provider di identità per consentire l'accesso alle applicazioni AWS gestite e Account AWS da tali regioni. Per ulteriori dettagli, consultare [the section called “Fase 3: Aggiornare la configurazione dell'IdP esterno”](#). Consulta la PingOne documentazione per ulteriori dettagli.

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.

- PingOne non 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 è necessario interrompere immediatamente il provisioning, eliminare il token BEARER SCIM pertinente e disattivarlo in IAM Identity Center. and/or [Esegui il provisioning di utenti e gruppi da un provider di identità esterno utilizzando SCIM](#)
- Se un attributo per un utente viene rimosso dal data store configurato in PingOne, 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 che sia unico all'interno della tua directory in PingOne, 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, con errori come 'SAML_215' o 'Invalid input '. Per risolvere questo problema PingOne, 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 l'endpoint SCIM e il token di accesso. Dovrai incollarli in un secondo momento quando configuri il provisioning nel tuo IdP.

- a. Endpoint SCIM: ad esempio, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
- b. Token di accesso: scegli Mostra token per copiare il valore.

 Warning

Questa è l'unica volta in cui puoi ottenere l'endpoint SCIM e il token di accesso. Assicurati di copiare questi valori prima di andare avanti. Inserirai questi valori per configurare il provisioning automatico nel tuo IdP più avanti in questo tutorial.

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 utente 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. 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. [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'Nameattributo `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

Per la risoluzione generale dei problemi relativi a SCIM e SAML con PingOne, consulta le seguenti sezioni:

- [Alcuni utenti non riescono a sincronizzarsi in IAM Identity Center da un provider SCIM esterno](#)

- [Problemi relativi al contenuto delle asserzioni SAML create da IAM Identity Center](#)
- [Errore duplicato di utenti o gruppi durante il provisioning di utenti o gruppi con un provider di identità esterno](#)
- [Per ulteriori informazioni su PingOne, consulta PingOne la documentazione.](#)

Le seguenti risorse possono aiutarti a risolvere i problemi mentre lavori con: AWS

- [AWS re:Post](#)- Trova FAQs e collega altre risorse per aiutarti a risolvere i problemi.
- [Supporto AWS](#)- Richiedere supporto tecnico

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 Microsoft Active Directory, Microsoft 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 origine dell'identità e un'istanza dell'organizzazione IAM Identity Center per configurare e testare un utente amministrativo. Questo utente amministrativo crea e gestisce utenti e gruppi e concede AWS l'accesso con set di autorizzazioni. Nei passaggi successivi, creerai quanto segue:

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

Per verificare che tutto sia stato creato correttamente, devi accedere e impostare 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. In alternativa, se desideri concedere agli utenti l'accesso all'applicazione, puoi seguire il [passaggio 1](#) di questa procedura e [configurare l'accesso all'applicazione](#).

Prerequisiti

Per completare questo tutorial sono necessari i seguenti prerequisiti:

- [Abilita IAM Identity Center](#) dispongono di un'[istanza organizzativa di IAM Identity Center](#).
 - Se disponi di un'[istanza di account](#) di IAM Identity Center, puoi creare utenti e gruppi e concedere loro l'accesso alle applicazioni. Per ulteriori informazioni, consulta [Accesso alle applicazioni](#).
- Accedi Console di gestione AWS e accedi alla console IAM Identity Center come:
 - 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.
 - [Per ulteriori informazioni sull'accesso a Console di gestione AWS, consulta la Guida.Accedi ad AWS](#)
- Puoi configurare l'autenticazione a più fattori per gli utenti del tuo IAM Identity Center. Per ulteriori informazioni, consulta [Configurazione della tecnologia MFA in IAM Identity Center](#).

Fase 1: Aggiungere un utente

1. Apri la [console Centro identità IAM](#).
2. Nel riquadro di navigazione di IAM Identity Center, scegli Utenti, quindi seleziona Aggiungi utente.
3. 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. Gli utenti devono ricordare il nome utente per accedere al portale di AWS accesso e non è possibile 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 iscriversi a IAM Identity Center. L'e-mail proviene da `no-reply@signin.aws`

ono-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, digita *Nikki*.
 - Cognome: inserisci il cognome dell'utente. Per questo tutorial, digita *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.
4. Scegli Next (Successivo). Viene visualizzata la pagina Aggiungi utente ai gruppi. Creeremo un gruppo a cui assegnare autorizzazioni amministrative invece di assegnarle direttamente. *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, digita *Admin team*.
 - b. Scegli Crea gruppo
 - c. Chiudi la scheda del browser Gruppi per tornare alla scheda Aggiungi browser utente
5. Nell'area Gruppi, seleziona il pulsante Aggiorna. Il *Admin team* gruppo viene visualizzato nell'elenco.

Seleziona la casella di controllo accanto a *Admin team*, quindi scegli Avanti.

6. 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 **Admin team** gruppo in modo che **Nikki** abbia accesso alle risorse.

Passaggio 2: Aggiungere le autorizzazioni amministrative

Important

Segui questi passaggi solo se hai abilitato un'[istanza organizzativa di IAM Identity Center](#).

1. Nel riquadro di navigazione di IAM Identity Center, in Autorizzazioni multiaccount, scegli. Account AWS
 2. Nella Account AWS pagina, 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 **Admin team** gruppo 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. AdministratorAccessScegli Next (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 Create (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 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. Nella pagina Passo 3: Rivedi e invia le assegnazioni, conferma che il *Admin team* gruppo sia selezionato e che il set di *AdministratorAccess* autorizzazioni sia selezionato, quindi scegli Invia.

La pagina si aggiorna con un messaggio che indica che Account AWS 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.

Complimenti!

Hai configurato correttamente il primo utente, gruppo e set di autorizzazioni.

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

Fase 3: test dell'accesso utente

Ora che *Nikki Wolf* si tratta di un utente dell'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, in questo passaggio successivo utilizzerai *Nikki's* le credenziali per accedere e impostare la sua password. Quando hai aggiunto l'utente *Nikki Wolf* nel passaggio

1, hai scelto di **Nikki** ricevere un'e-mail con le istruzioni per l'impostazione della password. È ora di aprire l'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 **Nikki 's** utente 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 in cui puoi impostare **Nikki 's** la password e [registrare il dispositivo MFA](#).

2. Dopo aver impostato **Nikki 's** la password, si passa alla pagina di accesso. Inserisci **nikkiw** e scegli Avanti, quindi inserisci **Nikki 's** la password 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 o AWS CLI AWS SDKs](#).

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.

Fasi successive

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 al tuo 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.

Tutorial video

Come risorsa aggiuntiva, puoi utilizzare questi tutorial video per saperne di più sulla configurazione di provider di identità esterni:

- [Migrazione tra provider di identità esterni in AWS IAM Identity Center](#)
- [Federazione dell'istanza esistente AWS IAM Identity Center con Microsoft Entra ID](#)

Configura la tua forza lavoro in IAM Identity Center

IAM Identity Center è la AWS soluzione per connettere gli utenti della forza lavoro ad applicazioni AWS gestite come Kiro e Amazon Quick e ad altre AWS risorse. Puoi connettere il tuo provider di identità esistente e sincronizzare utenti e gruppi dalla tua directory, oppure creare e gestire i tuoi utenti direttamente in IAM Identity Center.

Usi già IAM per l'accesso a Account AWS?

Non è necessario apportare modifiche ai Account AWS flussi di lavoro correnti per utilizzare IAM Identity Center per accedere alle applicazioni AWS gestite. Se utilizzi la [federazione con IAM](#) per Account AWS l'accesso, i tuoi utenti possono continuare ad accedere Account AWS nello stesso modo in cui hanno sempre fatto e tu puoi continuare a utilizzare i flussi di lavoro esistenti per gestire tale accesso.

Scegli l'approccio più adatto alla strategia di gestione delle identità della tua organizzazione e all'infrastruttura esistente.

Argomenti

- [Utenti, gruppi e provisioning in IAM Identity Center](#)
- [Manage your identity source](#)
- [Gestione degli utenti nella directory Identity Center](#)

Utenti, gruppi e provisioning in IAM Identity Center

IAM Identity Center ti consente di controllare chi può accedere e a quali risorse può accedere. È necessario assegnare il provisioning a un utente per accedere. È quindi possibile assegnare l'accesso solo a utenti o gruppi autorizzati. Scopri di più su utenti, gruppi e provisioning in IAM Identity Center.

Unicità del nome utente e dell'indirizzo e-mail

IAM Identity Center richiede che ogni utente abbia un nome utente univoco. Il nome utente è l'identificatore principale dell'utente. Il nome utente non deve necessariamente corrispondere all'indirizzo e-mail 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 i gruppi annidati (un gruppo all'interno di un gruppo). I gruppi sono utili per assegnare l'accesso a applicazioni 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 connettere la tua fonte di identità a IAM Identity Center. Con IAM Identity Center, puoi assegnare a utenti e gruppi l'accesso alle applicazioni connesse e Account AWS.

Il provisioning in IAM Identity Center varia in base alla fonte di identità utilizzata. Per ulteriori informazioni, consulta [Manage your identity source](#).

Deprovisioning di utenti e gruppi

Il deprovisioning è il processo di rimozione delle informazioni su utenti e gruppi da IAM Identity Center.

Se utilizzi Active Directory o un provider di identità esterno con IAM Identity Center, dovresti rimuovere utenti e gruppi da queste fonti di identità anziché da IAM Identity Center. L'eliminazione di utenti e gruppi di IAM Identity Center non li rimuoverà completamente se la fonte di identità è Active Directory o un provider di identità esterno.

Se devi eseguire il deprovisioning di utenti o gruppi di IAM Identity Center, devi prima [rimuovere tutte le assegnazioni di set di autorizzazioni](#) o applicazioni agli utenti o ai gruppi di cui desideri eseguire il deprovisioning. Altrimenti, avrai set di autorizzazioni e assegnazioni di applicazioni non assegnati nel tuo IAM Identity Center.

Manage your identity source

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:

- [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
- [Il tuo Active Directory locale o AWS gestito](#): scegli questa opzione se desideri connettere il tuo Active Directory (AD).
- [Directory Identity Center](#): quando abiliti IAM Identity Center per la prima volta, questa viene configurata automaticamente con una directory Identity Center come origine di identità predefinita, a meno che tu non scelga una fonte di identità diversa. Con la directory Identity Center, puoi creare utenti e gruppi e assegnare il loro livello di accesso alle tue Account AWS applicazioni.

Note

IAM Identity Center non supporta Simple AD SAMBA4 basato su sistema Simple AD come fonte di identità.

Argomenti

- [Considerazioni sulla modifica dell'origine dell'identità](#)
- [Cambia la fonte della tua identità](#)
- [Attributi utente e gruppo supportati in IAM Identity Center](#)
- [Provider di identità esterni](#)
- [Microsoft ADeleco](#)

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 fonte della tua identità](#) per ulteriori informazioni.

Passaggio dalla directory IAM Identity Center a quella di 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.

Important

Quando modifichi il tipo di origine dell'identità in IAM Identity Center da o verso Active Directory, tieni presente che l'ID Identity Store cambierà. Ciò può avere le seguenti implicazioni:

- L'URL del portale di AWS accesso predefinito cambierà. Dovrai comunicare il nuovo URL alla tua forza lavoro e aggiornare i segnalibri, gli elenchi di autorizzazioni del gateway o del firewall e le configurazioni in cui viene fatto riferimento a questo URL. Ti consigliamo di eseguire questa modifica in una finestra di manutenzione pianificata per ridurre al minimo le interruzioni per gli utenti.
- Se utilizzi una chiave KMS gestita dal cliente per la crittografia inattiva in IAM Identity Center e hai configurato la politica della chiave KMS con il contesto di crittografia, tieni presente che il contesto di crittografia per Identity Store cambierà. Ad esempio, nell'ARN dell'Identity Store «arn:aws:identitystore: :123456789012:identitystore/d-922763e9b3», «d-922763e9b3» è l'ID Identity Store. Per evitare interruzioni del servizio durante questa transizione, modifica temporaneamente la policy delle chiavi KMS utilizzando un pattern wildcard: «arn:aws:identitystore: :123456789012:identitystore/*».

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 APIs: se utilizzi Active Directory come fonte di identità, ti consigliamo di utilizzare le funzionalità di [creazione, aggiornamento](#) ed eliminazione con cautela. APIs 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 che li utilizzano. APIs
- 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 AWS accesso.
- Se gli utenti vengono eliminati o disabilitati nella console IAM Identity Center utilizzando Identity Store APIs, gli utenti con sessioni attive possono continuare ad accedere ad applicazioni e account integrati. Per informazioni sulla durata della sessione di autenticazione e sul comportamento degli utenti, consulta [Comprendere le sessioni di autenticazione in IAM Identity Center](#).

Per informazioni su come IAM Identity Center fornisce utenti e gruppi, consulta [Microsoft AD elenco](#).

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 continuano a funzionare finché il nuovo IdP invia le asserzioni corrette (ad esempio, nome SAML). IDs 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 apportate 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 solo in IAM Identity Center 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](#).
- Le sessioni utente esistenti vengono revocate alla scadenza della durata della sessione: una volta modificata la fonte di identità con un provider di identità esterno, le sessioni utente attive persistono per il resto della durata massima della sessione configurata nella console. Ad esempio, se la durata della sessione del portale di AWS accesso è impostata su otto ore e l'origine dell'identità è stata modificata nella quarta ora, le sessioni utente attive persistono per altre quattro ore. Per revocare le sessioni utente, vedere. [the section called “Termina le sessioni attive per gli utenti della forza lavoro”](#)

Se gli utenti vengono eliminati o disabilitati nella console IAM Identity Center utilizzando Identity Store APIs, gli utenti con sessioni attive possono continuare ad accedere ad applicazioni e account integrati. Per informazioni sulla durata della sessione di autenticazione e sul comportamento degli utenti, consulta [Comprendere le sessioni di autenticazione in IAM Identity Center](#).

Note

Non puoi revocare le sessioni utente dalla console IAM Identity Center dopo aver eliminato l'utente.

Per informazioni su come IAM Identity Center effettua il provisioning di utenti e gruppi, consulta. [Provider di identità esterni](#)

Passaggio da un IdP esterno a IAM Identity Center

Se cambi 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.
- Le sessioni utente esistenti vengono revocate alla scadenza della durata della sessione: una volta modificata la fonte di identità in IAM Identity Center, le sessioni utente attive persistono per la durata residua della durata massima della sessione configurata nella console. Ad esempio, se la durata della sessione del portale di AWS accesso è di otto ore e hai cambiato l'origine dell'identità alla quarta ora, le sessioni utente attive continuano a funzionare per altre quattro ore. Per revocare le sessioni utente, vedere. [the section called “Termina le sessioni attive per gli utenti della forza lavoro”](#)

Se gli utenti vengono eliminati o disabilitati nella console IAM Identity Center utilizzando Identity Store APIs, gli utenti con sessioni attive possono continuare ad accedere ad applicazioni e account integrati. Per informazioni sulla durata della sessione di autenticazione e sul comportamento degli utenti, consulta [Comprendere le sessioni di autenticazione in IAM Identity Center](#).

Note

Non sarai in grado di revocare le sessioni utente dalla console IAM Identity Center dopo aver eliminato l'utente.

- Supporto multiregionale: se hai replicato IAM Identity Center in altre regioni o hai intenzione di farlo, devi utilizzare un provider di identità esterno come fonte di identità. Per ulteriori informazioni, inclusi altri prerequisiti, consulta. [Utilizzo di IAM Identity Center su più Regioni AWS](#)

Per informazioni su come IAM Identity Center effettua il provisioning di utenti e gruppi, consulta [Gestione degli utenti nella directory Identity Center](#).

Passaggio da un IdP esterno a un altro IdP esterno

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

- Le assegnazioni e le iscrizioni funzionano con le asserzioni corrette: IAM Identity Center conserva tutte le tue assegnazioni. Le assegnazioni utente, le assegnazioni ai gruppi e le appartenenze ai gruppi continuano a funzionare finché il nuovo IdP invia le asserzioni corrette (ad esempio, il nome SAML). IDs

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 abbinati correttamente utenti e gruppi quando SCIM è abilitato.
- Le sessioni utente esistenti vengono revocate alla scadenza della durata della sessione: una volta modificata l'origine dell'identità con un provider di identità esterno diverso, le sessioni utente attive persistono per la durata residua della durata massima della sessione configurata nella console. Ad esempio, se la durata della sessione del portale di AWS accesso è di otto ore e l'origine dell'identità è stata modificata alla quarta ora, le sessioni utente attive persistono per altre quattro ore. Per revocare le sessioni utente, vedere. [the section called “Termina le sessioni attive per gli utenti della forza lavoro”](#)

Se gli utenti vengono eliminati o disabilitati nella console IAM Identity Center utilizzando Identity Store APIs, gli utenti con sessioni attive possono continuare ad accedere ad applicazioni e account integrati. Per informazioni sulla durata della sessione di autenticazione e sul comportamento degli utenti, consulta [Comprendere le sessioni di autenticazione in IAM Identity Center](#).

Note

Non puoi revocare le sessioni utente dalla console IAM Identity Center dopo aver eliminato l'utente.

Per informazioni su come IAM Identity Center effettua il provisioning di utenti e gruppi, consulta. [Provider di identità esterni](#)

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 degli 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.
- Se gli utenti vengono eliminati o disabilitati nella console IAM Identity Center utilizzando Identity Store APIs, gli utenti con sessioni attive possono continuare ad accedere ad applicazioni e account integrati. Per informazioni sulla durata della sessione di autenticazione e sul comportamento degli utenti, consulta [Comprendere le sessioni di autenticazione in IAM Identity Center](#).
- Supporto multiregionale: se hai replicato IAM Identity Center in altre regioni o intendi farlo, devi utilizzare un provider di identità esterno come fonte di identità. Per ulteriori informazioni, inclusi altri prerequisiti, consulta [Utilizzo di IAM Identity Center su più Regioni AWS](#).

Per informazioni su come IAM Identity Center effettua il provisioning di utenti e gruppi, consulta [Microsoft ADelenco](#).

Cambia la fonte della tua 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 procedere, esamina le informazioni contenute in [Considerazioni sulla modifica dell'origine dell'identità](#). Per completare questa procedura, avrai bisogno di un'istanza organizzativa di IAM Identity Center. Per ulteriori informazioni, consulta [Istanze di organizzazione e account di IAM Identity Center](#).

Warning

A seconda della distribuzione corrente, questa modifica rimuove tutte le assegnazioni di utenti e gruppi configurate in IAM Identity Center. Questa modifica rimuoverà anche i ruoli IAM del set di autorizzazioni dal tuo Account AWS. Di conseguenza, potrebbe essere necessario aggiornare le politiche relative alle risorse e assicurarti che ciò non interrompa l'accesso alle AWS KMS chiavi e ai cluster Amazon EKS. Per ulteriori informazioni, consulta [Riferimento ai set di autorizzazioni nelle politiche delle risorse, nelle mappe di configurazione dei cluster Amazon EKS e AWS KMS nelle politiche chiave](#).

Quando ciò si verifica, tutti gli utenti e i gruppi, incluso l'utente amministrativo in IAM Identity Center, perderanno l'accesso Single Sign-On alle proprie applicazioni. Account AWS

Per cambiare la fonte della tua identità

1. Apri la [console Centro identità IAM](#).
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Origine dell'identità. Scegli Azioni, quindi scegli Cambia origine dell'identità.
4. In Scegli l'origine dell'identità, seleziona la fonte a cui desideri passare, quindi scegli Avanti.

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

Important

La modifica della fonte di identità da o verso Active Directory elimina utenti e gruppi dalla directory Identity Center. Questa modifica rimuove anche tutte le assegnazioni configurate in IAM Identity Center.

Note

Se hai replicato IAM Identity Center in altre regioni, non sarai in grado di modificare il tipo di origine dell'identità. Puoi sostituire solo l'IdP esterno corrente con un altro. Per modificare il tipo di origine dell'identità, dovrai prima rimuovere tutte le regioni aggiuntive. Per ulteriori informazioni, consulta [Utilizzo di IAM Identity Center su più Regioni AWS](#)

Se stai passando a un provider di identità esterno, ti consigliamo di seguire la procedura riportata di seguito [Come connettersi a un provider di identità esterno](#).

5. Dopo aver letto il disclaimer e aver iniziato a procedere, digita ACCEPT.
6. Scegli Cambia fonte di identità. Se stai cambiando la fonte di identità in Active Directory, procedi al passaggio successivo.
7. Se si modifica la fonte di identità in Active Directory, si accede alla pagina Impostazioni. Nella pagina Impostazioni, esegui una delle seguenti operazioni:
 - Scegli Avvia configurazione guidata. Per informazioni su come completare la procedura di configurazione guidata, consulta [Configurazione guidata](#).

- Nella sezione Origine dell'identità, scegli Azioni, quindi scegli Gestisci sincronizzazione per configurare l'ambito di sincronizzazione, l'elenco di utenti e gruppi da sincronizzare.

Attributi utente e gruppo supportati in IAM Identity Center

Questa guida fornisce un riferimento per il supporto degli attributi SCIM in IAM Identity Center. Elenca gli attributi di utente e gruppo della specifica SCIM supportati nell'archivio di identità di IAM Identity Center e identifica gli attributi e gli attributi secondari specifici che non sono supportati.

Gli attributi sono informazioni che aiutano a definire e identificare singoli oggetti di utenti o gruppi, come `name`, `email` o `members`. IAM Identity Center supporta gli attributi più comunemente utilizzati sia tramite l'immissione manuale che il provisioning SCIM automatico.

- Per informazioni sulla specifica System for Cross-Domain Identity Management (SCIM), consulta <https://tools.ietf.org/html/rfc7642>.
- Per informazioni sul provisioning manuale e automatico, vedere [Provisioning quando gli utenti provengono da un IdP esterno](#).
- Per informazioni sulla mappatura degli attributi, vedere [Mappature degli attributi tra IAM Identity Center e la directory External Identity Provider](#).

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 non supportati

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'

Oggetti di gruppo non supportati

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).

Provider di identità esterni

Con IAM Identity Center, puoi connettere le identità della tua forza lavoro esistenti provenienti da provider di identità esterni (IdPs) tramite i protocolli Security Assertion Markup Language (SAML) 2.0 e System for Cross-Domain Identity Management (SCIM). Ciò consente agli utenti di accedere al portale di accesso con le proprie credenziali aziendali. AWS 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 o Microsoft 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.

Se si utilizza una directory autogestita in Active Directory o una AWS Managed Microsoft AD, vedere. [Microsoft ADelenco](#)

 Note

Il protocollo SAML 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.

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 [Esegui il provisioning di utenti e gruppi da un provider di identità esterno utilizzando SCIM](#) i tuoi utenti e gruppi. [Fornitura manuale](#) Indipendentemente dalla modalità di provisioning degli utenti, IAM Identity Center reindirizza l'Console di gestione AWS 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](#)

Argomenti

- [Come connettersi a un provider di identità esterno](#)
- [Come modificare i metadati di un provider di identità esterno in IAM Identity Center](#)
- [Utilizzo della federazione delle identità SAML e SCIM con provider di identità esterni](#)
- [Profilo SCIM e implementazione SAML 2.0](#)

Come connettersi a un provider di identità esterno

Esistono diversi prerequisiti, considerazioni e procedure di approvvigionamento per i dispositivi esterni supportati. IdPs Sono disponibili step-by-step tutorial per diversi argomenti: IdPs

- [CyberArk](#)
- [Google Workspace](#)
- [JumpCloud](#)
- [Microsoft Entra ID](#)
- [Okta](#)
- [OneLogin](#)

- [Ping Identity](#)

Per ulteriori informazioni sulle considerazioni relative alle applicazioni esterne IdPs supportate da IAM Identity Center, consulta [Utilizzo della federazione delle identità SAML e SCIM con provider di identità esterni](#).

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 Centro identità IAM](#).
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Origine dell'identità, quindi scegli Azioni > Cambia fonte di 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.

 Note

Il file di metadati SAML che scarichi contiene sia il servizio di asserzione consumer (ACS) IPv4 -only che quello dual-stack. URLs Inoltre, se il tuo IAM Identity Center viene replicato in altre regioni, il file di metadati contiene ACS per ogni regione aggiuntiva. URLs Se il tuo IdP esterno ha un limite al numero di ACS URLs, dovrai rimuovere l'ACS non necessario. URLs Ad esempio, se l'organizzazione ha adottato completamente gli endpoint dual-stack e non utilizza più IPv4 solo gli endpoint, è possibile rimuovere questi ultimi. Un approccio alternativo consiste nel non utilizzare il file di metadati ma nel copiare e incollare l'ACS URLs nell'IdP 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. Scegli Next (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.

Come modificare i metadati di un provider di identità esterno in IAM Identity Center

Puoi modificare i metadati del tuo provider di identità esterno che hai fornito in precedenza all'IAM Identity Center. Queste modifiche influiscono sulla capacità degli utenti di accedere e accedere alle AWS risorse tramite IAM Identity Center. La procedura seguente descrive come aggiornare i metadati dell'IdP esterno archiviati in IAM Identity Center. Per completare questa procedura, avrai bisogno di un'istanza organizzativa di IAM Identity Center. Per ulteriori informazioni, consulta [Istanze di organizzazione e account di IAM Identity Center](#).

Per modificare i metadati di un provider di identità esterno

1. Apri la [console Centro identità IAM](#).
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Origine dell'identità. Scegli Azioni, quindi scegli Gestisci autenticazione.
4. Nella sezione Metadati del provider di identità, scegli Modifica metadati IdP. Puoi apportare le modifiche all'URL di accesso dell'IdP e/o all'URL dell'emittente IdP per il tuo IdP esterno in questa pagina. Scegli Salva modifiche dopo aver apportato tutte le modifiche necessarie.

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 \(«»\) \(/rfc2822 #section -3.4.1\). name@domain.com https://tools.ietf.org/html](https://tools.ietf.org/html/rfc2822)
 - 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.
 - IAM Identity Center non supporta la firma delle richieste di autenticazione SAML inviate a siti esterni IdPs.
 - L'IdP deve supportare il Multiple Assertion Consumer Service (ACS) URLs se prevedi di replicare IAM Identity Center in altre regioni e sfruttare appieno i vantaggi di un IAM Identity Center multiregionale. Per ulteriori informazioni, consulta [Utilizzo di IAM Identity Center su più Regioni AWS](#). L'utilizzo di un singolo URL ACS può influire sull'esperienza utente in altre regioni. La tua regione principale continuerà a funzionare normalmente. Per ulteriori informazioni sull'esperienza utente in altre regioni con un unico URL ACS, consulta [the section called “Utilizzo di applicazioni AWS gestite senza più ACS URLs”](#) e [the section called “Account AWS resilienza di accesso senza più ACS URLs”](#).
- SCIM
 - [L'implementazione di IAM Identity Center SCIM si basa su SCIM RFCs 7642 \(https://tools.ietf.org/html/rfc7642\), 7643 \(/rfc7643\) e 7644 \(https://tools.ietf.org/html/rfc7644\) e sui requisiti di interoperabilità stabiliti nella bozza di marzo 2020 del https://tools.ietf.org/htmlBasic SCIM Profile 1.0 \(#rfc .section.4\). FastFed https://openid.net/specs/fastfed-scim-1_0-02.html](https://tools.ietf.org/html/rfc7642) Eventuali differenze tra questi documenti e l'attuale implementazione in IAM Identity Center sono

descritte nella sezione [Operazioni API supportate](#) della Guida per gli sviluppatori di IAM Identity Center SCIM Implementation.

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 Login ExternalId PDirectory
- Registri specifici per IDP, registri and/or di debug
- [Risoluzione dei problemi relativi a IAM Identity Center](#)

Note

Alcuni IdPs, come quelli inclusi in [Tutorial sulle fonti di identità di IAM Identity Center](#), 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 and/or endpoint con approcci federativi diversi 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 Console di gestione AWS 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 il provisioning, gli aggiornamenti e il deprovisioning degli utenti tra il gestore dell'identità digitale e il Centro identità IAM.

Per ulteriori informazioni su come implementare SCIM, consulta. [Esegui il provisioning di utenti e gruppi da un provider di identità esterno utilizzando SCIM](#) Per ulteriori dettagli sull'implementazione SCIM di IAM Identity Center, consulta la [IAM Identity Center SCIM Implementation](#) Developer Guide.

Argomenti

- [Esegui il provisioning di utenti e gruppi da un provider di identità esterno utilizzando SCIM](#)
- [Ruota i certificati SAML 2.0](#)

Esegui il provisioning di utenti e gruppi da un provider di identità esterno utilizzando SCIM

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 il tuo 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](#)
- [Genera un token di accesso](#)

- [Abilita il provisioning automatico](#)
- [Eliminare un token di accesso](#)
- [Disabilita il provisioning automatico](#)
- [Ruota un token di accesso](#)
- [Verifica e riconcilia le risorse con provisioning automatico](#)
- [Fornitura manuale](#)

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 sulle fonti di identità di IAM Identity Center](#) applicabile al tuo IdP.

- Se stai fornendo un indirizzo email principale, il valore di questo 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. In questo modo i tuoi utenti non perderanno AWS diritti, assegnazioni o autorizzazioni se devi cambiare il loro nome o indirizzo email.
- 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.
- Dopo aver configurato il provisioning automatico con SCIM per il tuo IdP, non puoi più aggiungere o modificare utenti nella console IAM Identity Center. Se devi aggiungere o modificare un utente, devi farlo dalla tua fonte di identità o IdP esterna.

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.

Genera un 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 [Abilita 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.

Abilita 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 sulle fonti di identità di IAM Identity Center](#) 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 l'endpoint SCIM e il token di accesso. Dovrai incollarli più tardi quando configuri il provisioning nel tuo IdP.
 - a. Endpoint SCIM: ad esempio, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
 - b. Token di accesso: scegli Mostra token per copiare il valore.

Warning

Questa è l'unica volta in cui puoi ottenere l'endpoint SCIM e il token di accesso. Assicurati di copiare questi valori prima di andare avanti. Inserirai questi valori per configurare il provisioning automatico nel tuo IdP più avanti in questo tutorial.

5. Scegli Chiudi.

Dopo aver completato questa procedura, è necessario configurare il provisioning automatico nel proprio IdP. Per ulteriori informazioni, consulta la pagina [Tutorial sulle fonti di identità di IAM Identity Center](#) dedicata al tuo IdP.

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.

Disabilita 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 [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.

Ruota 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 [Genera un 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 [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.

Verifica e riconcilia le risorse con provisioning automatico

SCIM ti consente di effettuare automaticamente il provisioning di utenti, gruppi e appartenenze ai gruppi dalla tua fonte di identità a IAM Identity Center. Questa guida ti aiuta a verificare e riconciliare queste risorse per mantenere una sincronizzazione accurata.

Perché controllare le tue risorse?

Un controllo regolare aiuta a garantire che i controlli di accesso rimangano accurati e che il tuo provider di identità (IdP) rimanga correttamente sincronizzato con IAM Identity Center. Ciò è particolarmente importante per la conformità alla sicurezza e la gestione degli accessi.

Risorse che puoi controllare:

- Utenti
- Gruppi
- Appartenenze ai gruppi

È possibile utilizzare i [comandi AWS Identity Store API o CLI](#) per eseguire il controllo e la riconciliazione. Negli esempi seguenti vengono utilizzati AWS CLI i comandi. Per le alternative alle API, fai riferimento alle [operazioni corrispondenti](#) nel riferimento all'API di Identity Store.

Come controllare le risorse

Ecco alcuni esempi su come controllare queste risorse utilizzando AWS CLI i comandi.

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Accesso dell'amministratore a IAM Identity Center.
- AWS CLI installato e configurato. Per informazioni, consulta la [Guida per l'utente dell'interfaccia a riga di AWS comando](#).
- Autorizzazioni IAM richieste per i comandi Identity Store.

Fase 1: Elenca le risorse correnti

È possibile visualizzare le risorse correnti utilizzando il AWS CLI.

Note

Quando si utilizza AWS CLI, l'impaginazione viene gestita automaticamente a meno che non venga specificato. `--no-paginate` Se stai chiamando direttamente l'API (ad esempio, con un SDK o uno script personalizzato), gestiscila `NextToken` nella risposta. In questo modo puoi recuperare tutti i risultati su più pagine.

Example per gli utenti

```
aws identitystore list-users \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

Example per gruppi

```
aws identitystore list-groups \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

Example per appartenenze a gruppi

```
aws identitystore list-group-memberships \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

```
--group-id GROUP_ID
```

Fase 2: confrontalo con la fonte della tua identità

Confronta le risorse elencate con la tua fonte di identità per identificare eventuali discrepanze, ad esempio:

- Risorse mancanti che devono essere fornite in IAM Identity Center.
- Risorse aggiuntive che devono essere rimosse da IAM Identity Center.

Example per gli utenti

```
# Create missing users
aws identitystore create-user \
  --identity-store-id IDENTITY_STORE_ID \
  --user-name USERNAME \
  --display-name DISPLAY_NAME \
  --name GivenName=FIRST_NAME,FamilyName=LAST_NAME \
  --emails Value=EMAIL,Primary=true

# Delete extra users
aws identitystore delete-user \
  --identity-store-id IDENTITY_STORE_ID \
  --user-id USER_ID
```

Example per gruppi

```
# Create missing groups
aws identitystore create-group \
  --identity-store-id IDENTITY_STORE_ID \
  [group attributes]

# Delete extra groups
aws identitystore delete-group \
  --identity-store-id IDENTITY_STORE_ID \
  --group-id GROUP_ID
```

Example per appartenenze a gruppi

```
# Add missing members
aws identitystore create-group-membership \
```

```
--identity-store-id IDENTITY_STORE_ID \  
--group-id GROUP_ID \  
--member-id '{"UserId": "USER_ID"}'  
  
# Remove extra members  
aws identitystore delete-group-membership \  
--identity-store-id IDENTITY_STORE_ID \  
--membership-id MEMBERSHIP_ID
```

Considerazioni

- I comandi sono soggetti alle [quote di servizio e alla limitazione delle API](#).
- Se riscontri molte differenze durante la riconciliazione, apporta piccole modifiche graduali a Identity Store. AWS Questo ti aiuta a evitare errori che riguardano più utenti.
- La sincronizzazione SCIM può ignorare le modifiche manuali. Controlla le impostazioni del tuo IdP per comprendere questo comportamento.

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](#).

Ruota 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 al contempo 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

La pagina Gestisci i certificati SAML 2.0 mostra le icone colorate degli indicatori di stato 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 scaduto.
- Giallo: indica che un certificato scade dopo 90 giorni o meno.
- Verde: indica che un certificato è valido e rimane 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.

Microsoft ADelelenco

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 Service. Questa 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 in Cloud AWS. Puoi anche utilizzarla 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 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 Directory Service tuo account di AWS Organizations gestione.
- IAM Identity Center non supporta Simple AD basato su SAMBA 4 come directory connessa.
- IAM Identity Center non è in grado di sincronizzare Foreign Security Principal (). FSPs Se un gruppo AWS Managed Microsoft AD contiene membri di un dominio affidabile come FSPs, tali membri non verranno sincronizzati.

Per una dimostrazione sul processo di utilizzo di Active Directory come fonte di identità per IAM Identity Center, guarda il seguente YouTube video:

[Utilizzo di Active Directory come fonte di identità per AWS IAM Identity Center | Amazon Web Services](#)

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 punto 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, usa AWS Managed Microsoft AD. Per ulteriori informazioni, consulta:

- [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 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.

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.

Note

IAM Identity Center non supporta Simple AD SAMBA4 basato su sistema Simple AD come fonte di identità.

AWS Managed Microsoft AD

1. Consulta le linee guida contenute in [Microsoft ADelenco](#).

2. Segui 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 in [Microsoft ADeleco](#).
2. Segui 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 in [Provider di identità esterni](#).
2. Segui 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 Active Directory a IAM Identity Center, puoi specificare un utente a cui concedere le autorizzazioni amministrative e quindi sincronizzare quell'utente dalla tua directory in IAM Identity Center.

1. Apri la [console Centro identità IAM](#).
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 [Creare un set di autorizzazioni](#).

Eseguire il provisioning quando gli utenti provengono da Active Directory

IAM Identity Center utilizza la connessione fornita da 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](#)

- [Mappature degli attributi tra IAM Identity Center e la directory External Identity Provider](#)
- [Sincronizzazione AD configurabile con IAM Identity Center](#)

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 Centro identità IAM](#).

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 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

Note

Per poter utilizzare AWS applicazioni, come IAM Identity Center per leggere gli utenti delle Directory Service directory dai domini affidabili, gli Directory Service account richiedono le autorizzazioni per l' `userAccountControl` attributo sugli utenti affidabili. Senza i permessi di lettura per questo attributo, AWS le applicazioni non sono in grado di determinare se l'account è abilitato o disabilitato.

L'accesso in lettura a questo attributo viene fornito per impostazione predefinita quando viene creato un trust. Se neghi l'accesso a questo attributo (scelta non consigliata), impedirai ad applicazioni come Identity Center di leggere utenti affidabili. La soluzione consiste nel consentire specificamente l'accesso in lettura all'`userAccountControl` attributo sugli account di AWS servizio nell'unità organizzativa AWS riservata (con il prefisso AWS_).

- 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. Di seguito sono riportate le considerazioni relative all'utilizzo di AD Connector:
 - 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 Directory Service per Microsoft Active Directory.

 Note

IAM Identity Center non funziona con le directory Simple AD SAMBA4 basate su Simple AD.

Mappature degli attributi tra IAM Identity Center e la directory External Identity Provider

Le mappature degli attributi vengono utilizzate per mappare i tipi di attributi esistenti in IAM Identity Center con attributi simili nella fonte di identità esterna, ad Google Workspace esempio, e. Microsoft Active Directory (AD) Okta IAM Identity Center recupera gli attributi utente dalla fonte di identità e li mappa agli attributi utente di IAM Identity Center.

Se il tuo IAM Identity Center è sincronizzato per utilizzare un provider di identità (IdP) esterno, ad Google Workspace esempioOkta, Ping o come fonte di identità, dovrai mappare i tuoi attributi nel tuo IdP.

IAM Identity Center inserisce automaticamente un set di attributi nella scheda Mappature degli attributi che si trova nella pagina di configurazione. IAM Identity Center utilizza questi attributi utente per compilare le asserzioni SAML (come attributi SAML) che vengono inviate all'applicazione. Questi attributi utente vengono a loro volta recuperati dalla fonte dell'identità. Ogni applicazione determina l'elenco degli attributi SAML 2.0 necessari per il single sign-on di successo. Per ulteriori informazioni, consulta [Mappa gli attributi dell'applicazione agli attributi di IAM Identity Center](#).

IAM Identity Center gestisce anche un set di attributi per te nella sezione Mappature degli attributi della pagina di configurazione di Active Directory se utilizzi Active Directory come fonte di identità. Per ulteriori informazioni, consulta [Mappatura degli attributi utente tra IAM Identity Center e la directory Microsoft AD](#).

Attributi del provider di identità esterno supportati

La tabella seguente elenca tutti gli attributi del provider di identità esterno (IdP) supportati e può essere mappata 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 tra IAM Identity Center e Microsoft AD

La tabella seguente elenca le mappature predefinite degli attributi utente in IAM Identity Center con gli attributi utente nella directory. Microsoft AD IAM Identity Center supporta solo l'elenco degli attributi nell'attributo User nella colonna IAM Identity Center.

Attributo utente in IAM Identity Center	Esegue il mapping a questo attributo in Active Directory
displayname	<code>\${displayname}</code>
emails[?primary].value *	<code>\${mail}</code>
externalid	<code>\${objectguid}</code>
name.givenname	<code>\${givenname}</code>
name.familyname	<code>\${sn}</code>
name.middlename	<code>\${initials}</code>

Attributo utente in IAM Identity Center	Esegue il mapping a questo attributo in Active Directory
sid	\${objectsid}
username	\${userprincipalname}

* L'attributo email in IAM Identity Center deve essere univoco all'interno della directory.

Attributo di gruppo in IAM Identity Center	Esegue il mapping a questo attributo in Active Directory
externalid	\${objectguid}
description	\${description}
displayname	\${samaccountname}@{associateddomain}

Considerazioni

- Se non hai assegnazioni per utenti e gruppi in IAM Identity Center quando abiliti la sincronizzazione AD configurabile, vengono utilizzate le mappature predefinite nelle tabelle precedenti. Per informazioni su come personalizzare queste mappature, consulta [Configura le mappature degli attributi per la sincronizzazione](#)
- Alcuni attributi di IAM Identity Center non possono essere modificati perché sono immutabili e mappati per impostazione predefinita su attributi di directory Microsoft AD specifici.

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.

Microsoft ADAttributi supportati per IAM Identity Center

La tabella seguente elenca tutti gli attributi di Microsoft AD directory supportati e che possono essere mappati agli attributi utente in IAM Identity Center.

Attributi supportati nella directory Microsoft AD

`${samaccountname}`

`${description}`

`${objectguid}`

`${objectsid}`

`${givenname}`

`${sn}`

`${initials}`

`${mail}`

`${userprincipalname}`

`${displayname}`

`${distinguishedname}`

`${proxyaddresses[?type == "SMTP"].value}`

`${proxyaddresses[?type == "smtp"].value}`

`${useraccountcontrol}`

`${associateddomain}`

Considerazioni

- È possibile specificare qualsiasi combinazione di attributi di Microsoft AD directory supportati da mappare a un singolo attributo mutabile in IAM Identity Center.

Attributi IAM Identity Center supportati per Microsoft AD

La tabella seguente elenca tutti gli attributi di IAM Identity Center supportati e che possono essere mappati agli attributi utente nella 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 for Active Directory

`${user:AD_GUID}`

`${user:AD_SID}`

`${user:email}`

`${user:familyName}`

`${user:givenName}`

`${user:middleName}`

`${user:name}`

`${user:preferredUsername}`

`${user:subject}`

Mappatura degli attributi utente tra IAM Identity Center e la directory Microsoft AD

Puoi utilizzare la seguente procedura per specificare in che modo gli attributi utente in IAM Identity Center devono essere mappati agli attributi corrispondenti nella tua Microsoft AD directory.

Per mappare gli attributi in IAM Identity Center agli attributi nella tua directory

1. Apri la [console Centro identità IAM](#).
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 **\${mail}**.
5. Scegli Save changes (Salva modifiche).

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.

- Con questo metodo di sincronizzazione, puoi fare quanto segue:
 - 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 AWS o 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.

Prerequisiti e considerazioni

Prima di utilizzare la sincronizzazione AD configurabile, tenete 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 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).

- **Sincronizzazione AD configurabile:** l'utilizzo della sincronizzazione AD configurabile per assegnare assegnazioni a un gruppo in Active Directory che contiene gruppi nidificati potrebbe 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 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](#)

Argomenti

- [Come funziona la sincronizzazione AD configurabile](#)
- [Configura le mappature degli attributi per la sincronizzazione](#)
- [Configurazione di sincronizzazione da Active Directory a IAM Identity Center per la prima volta](#)
- [Aggiungi utenti e gruppi all'ambito di sincronizzazione](#)
- [Rimuovi utenti e gruppi dall'ambito di sincronizzazione](#)
- [Metti in pausa e riprendi la sincronizzazione](#)
- [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. Per ulteriori informazioni sui prerequisiti, consulta. [Prerequisiti e considerazioni](#)

Creazione

Dopo aver collegato la directory autogestita in Active Directory o la AWS Managed Microsoft AD directory gestita da Directory Service a 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.

Puoi assegnare l'accesso a nuovi utenti o gruppi solo dopo che sono stati sincronizzati nell'archivio di identità di IAM Identity Center.

Aggiorna

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 le mappature degli attributi per la sincronizzazione

Per ulteriori informazioni sugli attributi disponibili, vedere. [Mappature degli attributi tra IAM Identity Center e la directory External Identity Provider](#)

Per configurare le mappature degli attributi in IAM Identity Center nella tua directory

1. Apri la [console Centro identità IAM](#).

2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Identity source, scegli Azioni, quindi scegli Manage Sync.
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. Scegli Save changes (Salva modifiche). Questo riporta alla pagina Manage Sync.

Configurazione di sincronizzazione da Active Directory a IAM Identity Center per la prima volta

Se sincronizzi utenti e gruppi da Active Directory a IAM Identity Center per la prima volta, segui questi passaggi. In alternativa, puoi seguire i passaggi descritti in [Cambia la fonte della tua identità](#) per modificare la fonte dell'identità da IAM Identity Center ad Active Directory.

Configurazione guidata

1. Apri la [console Centro identità IAM](#).

 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 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

Note

Quando aggiungi gruppi all'ambito di sincronizzazione, sincronizza i gruppi direttamente dal dominio locale affidabile anziché dai gruppi del AWS Managed Microsoft AD dominio. I gruppi sincronizzati direttamente dal dominio affidabile contengono oggetti utente effettivi a cui IAM Identity Center può accedere e sincronizzare correttamente.

Aggiungi gli utenti e i gruppi di Active Directory a IAM Identity Center seguendo questi passaggi.

Come aggiungere utenti

1. Apri la [console Centro identità IAM](#).
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. Se l'utente specificato non viene visualizzato nell'elenco, scegli l'icona di aggiornamento per aggiornare l'elenco degli utenti.

Per aggiungere gruppi

1. Apri la [console Centro identità IAM](#).
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). Se il gruppo specificato non viene visualizzato 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, consulta [Come funziona la sincronizzazione AD configurabile](#).

Per rimuovere utenti

1. Apri la [console Centro identità IAM](#).
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 Centro identità IAM](#).

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 Centro identità IAM](#).
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 Centro identità IAM](#).
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.

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 assegnare un nome al gruppo IAMIdentityCenterAllUsersAndGroups.
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.

Gestione degli utenti nella directory 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](#).

Esecuzione del 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 Directory Service. Per ulteriori informazioni, consulta Considerazioni per [Passaggio dalla directory IAM Identity Center a quella di 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

- [Aggiungi utenti alla directory del tuo Identity Center](#)
- [Aggiungi gruppi alla directory del tuo Identity Center](#)
- [Aggiungere utenti ai gruppi](#)
- [Elimina i gruppi in IAM Identity Center](#)
- [Eliminare gli utenti in IAM Identity Center](#)
- [Rimuovi utenti dai gruppi](#)
- [Modifica le proprietà utente della directory Identity Center](#)

Aggiungi utenti alla directory del tuo Identity Center

Gli utenti e i gruppi creati nella directory di Identity Center sono disponibili solo in IAM Identity Center. Utilizza la seguente procedura per aggiungere utenti alla directory del tuo Identity Center. In alternativa, è possibile chiamare l'operazione AWS API [CreateUser](#) per aggiungere utenti.

Console

Aggiunta di un utente

1. Apri la [console Centro identità IAM](#).
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 oggetto Invito a partecipare AWS IAM Identity Center. L'e-mail invita l'utente per conto della tua azienda ad accedere al portale di AWS accesso IAM Identity Center e registra una password. L'invito via e-mail scadrà tra sette giorni. In tal caso, puoi inviare nuovamente l'e-mail scegliendo Reimposta password, quindi scegliendo Invia un'e-mail all'utente con le istruzioni per reimpostare la password. Prima che l'utente accetti l'invito, vedrai il link di verifica Invia e-mail, che serve a verificare il suo indirizzo e-mail. Tuttavia, questo passaggio è facoltativo e scomparirà dopo che l'utente avrà accettato l'invito e registrato una password.

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, consulta [Email interregionali con Amazon SES](#).

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 ti fornisce l'URL del portale di AWS accesso e i dettagli della password che puoi inviare manualmente all'utente dal tuo indirizzo e-mail. L'utente dovrà verificare il proprio indirizzo e-mail. Puoi avviare il processo scegliendo Invia il link di verifica via e-mail. Il link di verifica via email scadrà tra sette giorni. In tal caso, puoi inviare nuovamente il link di verifica dell'e-mail scegliendo Reimposta password, quindi scegliendo Genera una password monouso e condividi la password con l'utente.
- 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 [Esegui il provisioning di utenti e gruppi da un provider di identità esterno utilizzando SCIM](#).
- 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. Scegli Next (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 eventuali modifiche. Dopo aver confermato che sono state specificate le informazioni corrette per entrambi i passaggi, scegli Aggiungi utente.

AWS CLI

Aggiunta di un utente

Il `create-user` comando seguente crea un nuovo utente nella directory di Identity Center.

```
aws identitystore create-user \
```

```
--identity-store-id d-1234567890 \  
--user-name johndoe \  
--name "GivenName=John,FamilyName=Doe" \  
--display-name "John Doe" \  
--emails "Type=work,Value=johndoe@example.com"
```

Output:

```
{  
  "UserId": "1234567890-abcdef",  
  "IdentityStoreId": "d-1234567890"  
}
```

 Note

Quando crei utenti con il comando `create-user` CLI o l'operazione [CreateUser](#) API, gli utenti non dispongono di password. Puoi aggiornare le impostazioni in IAM Identity Center per inviare a questi utenti un'e-mail di verifica dopo il primo tentativo di accesso in modo che possano configurare una password. Se non abiliti questa impostazione, devi generare una password monouso e condividerla con l'utente. Per ulteriori informazioni, consulta [Invia una password monouso agli utenti creati con API o CLI](#).

Aggiungi gruppi alla directory del tuo Identity Center

Utilizza la procedura seguente per aggiungere gruppi alla directory dell'Identity Center. In alternativa, è possibile chiamare l'operazione AWS API [CreateGroup](#) per aggiungere gruppi.

Console

Per aggiungere un gruppo

1. Apri la [console Centro identità IAM](#).
2. Scegliere Groups (Gruppi).
3. Seleziona Crea gruppo.
4. Inserisci il nome e la 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.

AWS CLI

Per aggiungere un gruppo

Il `create-group` comando seguente crea un nuovo gruppo nella directory di Identity Center.

```
aws identitystore create-group \  
  --identity-store-id d-1234567890 \  
  --display-name "Developers" \  
  --description "Group that contains all developers"
```

Output:

```
{  
  "GroupId": "1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p",  
  "IdentityStoreId": "d-1234567890"  
}
```

Dopo aver aggiunto questo gruppo alla directory di Identity Center, puoi assegnare l'accesso Single Sign-On al gruppo. Per ulteriori informazioni, consulta [Assegna l'accesso a utenti o gruppi a Account AWS](#).

Aggiungere utenti ai gruppi

Utilizza la procedura seguente per aggiungere utenti come membri di un gruppo creato in precedenza nella directory dell'Identity Center. In alternativa, è possibile chiamare l'operazione AWS API [CreateGroupMembership](#) per aggiungere un utente come membro di un gruppo.

Console

Per aggiungere un utente come membro di un gruppo

1. Apri la [console Centro identità IAM](#).
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.

AWS CLI

Per aggiungere un utente come membro di un gruppo

Il `create-group-membership` comando seguente aggiunge un utente a un gruppo nella directory di Identity Center.

```
aws identitystore create-group-membership \  
  --identity-store-id d-1234567890 \  
  --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \  
  --member-id UserId=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Output:

```
{  
  "MembershipId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",  
  "IdentityStoreId": "d-1234567890"  
}
```

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 dell'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 sull'eliminazione di gruppi in IAM, consulta [Eliminazione di un gruppo di utenti IAM nella Guida per l'utente](#).AWS Identity and Access Management

Console

Come eliminare un gruppo

1. Apri la [console Centro identità IAM](#).
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 elimini 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.

AWS CLI

Come eliminare un gruppo

Il `delete-group` comando seguente elimina il gruppo specificato dalla directory di Identity Center.

```
aws identitystore delete-group \  
  --identity-store-id d-1234567890 \  
  --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

Eliminare gli utenti in IAM Identity Center

Quando elimini un utente dalla tua directory IAM Identity Center, rimuove il suo accesso Account AWS e le sue applicazioni. Dopo aver eliminato un utente, non puoi annullare questa azione. Utilizza la procedura seguente per eliminare un utente nella directory del tuo 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 [Comprendere le sessioni di autenticazione 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

Console

Come eliminare un utente

1. Apri la [console Centro identità IAM](#).
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.

AWS CLI

Come eliminare un utente

Il `delete-user` comando seguente elimina un utente dalla directory dell'Identity Center.

```
aws identitystore delete-user \  
  --identity-store-id d-1234567890 \  
  --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Rimuovi utenti dai gruppi

Utilizzare la procedura seguente per rimuovere membri da un gruppo. In alternativa, puoi chiamare l'operazione AWS API [DeleteGroupMembership](#) per rimuovere un utente da un gruppo.

Console

Come rimuovere un utente da un gruppo

1. Apri la [console Centro identità IAM](#).
2. Scegliere Groups (Gruppi).
3. Scegli il gruppo che desideri aggiornare.
4. Nella pagina dei dettagli del gruppo, nella sezione Utenti di questo gruppo, scegli gli utenti da rimuovere.
5. Scegli Rimuovi utenti dal gruppo.
6. Nella finestra di dialogo Rimuovi utenti, scegli Rimuovi utenti dal gruppo per verificare che desideri rimuovere l'accesso degli utenti all'account e alle applicazioni assegnate al gruppo.

AWS CLI

Come rimuovere un utente da un gruppo

Il `delete-group-membership` comando seguente rimuove un'appartenenza a un gruppo.

```
aws identitystore delete-group-membership  
  --identity-store-id d-1234567890 \  
  --membership-id a1b2c3d4-5678-90ab-cdef-EXAMPLE33333
```


Modifica le proprietà utente della directory Identity Center

Utilizzare la procedura seguente per modificare le proprietà di un utente nella directory di Identity Center. In alternativa, è possibile chiamare l'operazione AWS API [UpdateUser](#) per aggiornare le proprietà dell'utente.

Console

Per modificare le proprietà degli utenti in IAM Identity Center

1. Apri la [console Centro identità IAM](#).
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.

AWS CLI

Per modificare le proprietà degli utenti in IAM Identity Center

Il `update-user` comando seguente aggiorna il nickname dell'utente.

```
aws identitystore update-user \  
  --identity-store-id d-1234567890 \  
  --nickname new-nickname
```

```
--user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--operations '{"AttributePath":"nickName","AttributeValue":"Johnny"}'
```

Configura l'accesso della forza lavoro alle risorse AWS

Imposta il modo in cui gli utenti della tua forza lavoro autenticano e accedono alle AWS risorse tramite IAM Identity Center. Questa sezione tratta i seguenti componenti che regolano l'accesso degli utenti della forza lavoro al tuo ambiente: AWS

- **Sessioni di autenticazione:** scopri come IAM Identity Center gestisce diversi tipi di sessioni utente, dalle sessioni interattive del portale alle sessioni applicative in background, e come interagiscono tra loro.
- **Gestione degli accessi degli utenti:** configura la durata delle sessioni, disabilita gli account utente e implementa blocchi di accesso a livello di organizzazione per mantenere la sicurezza e la conformità.
- **Gestione delle password:** per gli utenti creati nella directory Identity Center, imposta i requisiti per le password, gestisci la configurazione delle credenziali utente e gestisci la reimpostazione delle password per gli utenti.
- **Autenticazione a più fattori:** per gli utenti creati nella directory Identity Center, migliora la sicurezza con l'MFA utilizzando app di autenticazione, chiavi di sicurezza o autenticator integrati per proteggere gli accessi degli utenti.

Argomenti

- [Comprendere le sessioni di autenticazione in IAM Identity Center](#)
- [Configura la durata della sessione in IAM Identity Center](#)
- [Disabilita l'accesso degli utenti e le applicazioni in IAM Identity Center Account AWS](#)
- [Nega l'accesso degli utenti con Service Control Policies](#)
- [Gestione dell'accesso per gli utenti nella directory Identity Center](#)

Comprendere le sessioni di autenticazione in IAM Identity Center

Quando un utente [AWS accede al portale di accesso](#), IAM Identity Center crea una sessione di autenticazione che rappresenta l'identità verificata dell'utente.

Una volta autenticato, l'utente può accedere a tutte le applicazioni assegnate Account AWS e [AWS gestite dal cliente e alle applicazioni gestite dal cliente](#) per le quali gli amministratori hanno concesso l'autorizzazione all'uso, senza accessi aggiuntivi.

Tipi di sessioni di autenticazione

Sessioni interattive per utenti

Dopo che un utente ha effettuato l'accesso al portale di AWS accesso, IAM Identity Center crea una sessione interattiva per l'utente. Questa sessione rappresenta lo stato di autenticazione dell'utente all'interno di IAM Identity Center e funge da base per la creazione di altri tipi di sessione. Le sessioni interattive con l'utente possono durare per la durata configurata in IAM Identity Center, che può arrivare fino a 90 giorni.

Le sessioni interattive con l'utente sono il meccanismo di autenticazione principale. Terminano quando l'utente si disconnette o quando un amministratore termina la sessione. La durata di queste sessioni deve essere configurata con cura in base ai requisiti di sicurezza dell'organizzazione.

Per informazioni sulla configurazione della durata della sessione interattiva dell'utente, vedere [the section called “Configura la durata della sessione”](#).

Sessioni applicative

Le sessioni applicative sono le connessioni autenticate tra utenti e applicazioni AWS gestite (come Kiro o Amazon Quick) che IAM Identity Center stabilisce tramite Single Sign-On.

Per impostazione predefinita, le sessioni applicative hanno una durata di un'ora, ma vengono aggiornate automaticamente finché la sessione interattiva utente sottostante rimane valida. Questo meccanismo di aggiornamento offre agli utenti un'esperienza senza interruzioni, pur mantenendo i controlli di sicurezza. Al termine di una sessione interattiva dell'utente, tramite la disconnessione dell'utente o un'azione dell'amministratore, le sessioni dell'applicazione terminano al successivo tentativo di aggiornamento, in genere entro 30 minuti.

Sessioni in background degli utenti

Le sessioni utente in background sono sessioni di lunga durata progettate per applicazioni che devono eseguire processi per ore o giorni senza interruzioni. Attualmente, questo tipo di sessione si applica principalmente ad [Amazon SageMaker Studio](#), dove i data scientist possono eseguire lavori di formazione sull'apprendimento automatico che richiedono molte ore per essere completati.

Per informazioni sulla configurazione della durata della sessione utente in background, consulta [Sessioni utente in background](#).

Sessioni Kiro

Puoi estendere le sessioni di Kiro per consentire agli sviluppatori che utilizzano Kiro in IDEs di mantenere l'autenticazione per un massimo di 90 giorni. Questa funzionalità riduce le interruzioni di accesso mentre lavori sul codice.

Queste sessioni sono indipendenti da altri tipi di sessione e non influiscono sulle sessioni interattive degli utenti o su altre applicazioni AWS gestite. A seconda di quando hai abilitato IAM Identity Center, questa funzionalità potrebbe essere abilitata per impostazione predefinita.

Per informazioni sulla configurazione di sessioni Kiro estese, consulta. [???](#)

Sessioni di ruolo IAM create da IAM Identity Center

IAM Identity Center crea un tipo diverso di sessione quando gli utenti accedono alla Console di gestione AWS sala operatoria. AWS CLI In questi casi, IAM Identity Center utilizza la sessione di accesso per ottenere una sessione IAM assumendo un ruolo IAM specificato nel set di autorizzazioni dell'utente.

Important

A differenza delle sessioni applicative, le sessioni di ruolo IAM operano in modo indipendente una volta stabilite. Persistono per la durata configurata nel set di autorizzazioni, che può arrivare fino a 12 ore, indipendentemente dallo stato della sessione di accesso originale. Questo comportamento garantisce che le operazioni CLI di lunga durata o le sessioni della console non vengano interrotte inaspettatamente.

Modi per terminare le sessioni utente in IAM Identity Center

Iniziato dall'utente

Quando un utente si disconnette dal portale di AWS accesso, la sessione di accesso termina, impedendo all'utente di accedere a nuove risorse.

Le sessioni applicative esistenti, tuttavia, non terminano all'istante. Al contrario, termineranno entro circa 30 minuti, quando tenderanno il prossimo aggiornamento e scopriranno che la sessione di accesso non è più valida. Le sessioni di ruolo IAM esistenti continuano fino alla scadenza in base alla configurazione del set di autorizzazioni, che potrebbe avvenire fino a 12 ore dopo.

Avviato dall'amministratore

Chiunque disponga delle autorizzazioni amministrative di IAM Identity Center nell'organizzazione, in genere amministratori IT o team di sicurezza, può terminare la sessione di un utente. Questa azione funziona come se gli utenti si disconnettessero autonomamente, permettendo agli amministratori di richiedere agli utenti di effettuare nuovamente l'accesso quando necessario. Questa funzionalità è utile quando le politiche di sicurezza cambiano o quando vengono rilevate attività sospette.

Quando un amministratore di IAM Identity Center [elimina un utente](#) o [disabilita l'accesso di un utente](#), l'utente perde l'accesso al portale di AWS accesso e gli viene impedito di accedere nuovamente per avviare una nuova applicazione o sessione di ruolo IAM. L'utente perderà l'accesso alle sessioni applicative esistenti entro 30 minuti. Tutte le sessioni di ruolo IAM esistenti continueranno in base alla durata della sessione configurata nel set di autorizzazioni IAM Identity Center. La durata massima della sessione può essere di 12 ore.

Cosa succede all'accesso degli utenti quando si termina una sessione

Questo riferimento fornisce informazioni dettagliate su come si comportano le sessioni di IAM Identity Center quando vengono intraprese azioni amministrative. Le tabelle di questa sezione mostrano la durata e gli effetti delle azioni di gestione degli utenti e delle modifiche delle autorizzazioni sull'accesso al portale di AWS accesso, alle applicazioni e alle Account AWS sessioni.

Gestione degli utenti

Questa tabella riassume in che modo le modifiche alla gestione degli utenti influiscono sull'accesso alle AWS risorse, alle sessioni dell'applicazione e alle sessioni AWS dell'account.

Azione	L'utente perde l'accesso a IAM Identity Center	L'utente non può creare nuove sessioni applicative	L'utente non può accedere alle sessioni applicative esistenti	L'utente perde l'accesso alle Account AWS sessioni esistenti
Accesso dell'utente disabilitato	Efficace immediatamente	Efficace immediatamente	Entro 30 minuti	Entro 12 ore o meno. La durata dipende dalla durata di scadenza della sessione di ruolo

Azione	L'utente perde l'accesso a IAM Identity Center	L'utente non può creare nuove sessioni applicative	L'utente non può accedere alle sessioni applicative esistenti	L'utente perde l'accesso alle Account AWS sessioni esistenti
				IAM configurata per il set di autorizzazioni.
Utente eliminato	Efficace immediatamente	Efficace immediatamente	Entro 30 minuti	Entro 12 ore o meno. La durata dipende dalla durata di scadenza della sessione di ruolo IAM configurata per il set di autorizzazioni.
Sessione utente revocata	L'utente deve effettuare nuovamente e l'accesso per riottenere l'accesso	Efficace immediatamente	Entro 30 minuti	Entro 12 ore o meno. La durata dipende dalla durata di scadenza della sessione di ruolo IAM configurata per il set di autorizzazioni.

Azione	L'utente perde l'accesso a IAM Identity Center	L'utente non può creare nuove sessioni applicative	L'utente non può accedere alle sessioni applicative esistenti	L'utente perde l'accesso alle Account AWS sessioni esistenti
L'utente si disconnette	L'utente deve effettuare nuovamente l'accesso per riottenere l'accesso	Efficace immediatamente	Entro 30 minuti	Entro 12 ore o meno. La durata dipende dalla durata di scadenza della sessione di ruolo IAM configurata per il set di autorizzazioni.

Appartenenza a un gruppo

Questa tabella riassume in che modo le modifiche alle autorizzazioni degli utenti e alle appartenenze ai gruppi influiscono sull'accesso alle AWS risorse, alle sessioni dell'applicazione e alle sessioni dell'account. AWS

Azione	L'utente perde l'accesso a IAM Identity Center	L'utente non può creare nuove sessioni applicative	L'utente non può accedere alle sessioni applicative esistenti	L'utente perde l'accesso alle Account AWS sessioni esistenti
Applicazione o Account AWS accesso rimossi dall'utente	No: l'utente può continuare ad accedere a IAM Identity Center	Efficace immediatamente	Entro 1 ora	Entro 12 ore o meno. La durata dipende dalla durata di scadenza della sessione di ruolo IAM configurata per il set di autorizzazioni.

Azione	L'utente perde l'accesso a IAM Identity Center	L'utente non può creare nuove sessioni applicative	L'utente non può accedere alle sessioni applicative esistenti	L'utente perde l'accesso alle Account AWS sessioni esistenti
Utente rimosso dal gruppo a cui era stata assegnata un'applicazione o Account AWS	No: l'utente può continuare ad accedere a IAM Identity Center	Entro 1 ora	Entro 2 ore	Entro 12 ore o meno. La durata dipende dalla durata di scadenza della sessione di ruolo IAM configurata per il set di autorizzazioni.
Applicazione o Account AWS accesso rimossi dal gruppo	No: l'utente può continuare ad accedere a IAM Identity Center	Efficace immediatamente	Entro 1 ora	Entro 12 ore o meno. La durata dipende dalla durata di scadenza della sessione di ruolo IAM configurata per il set di autorizzazioni.

Note

Il portale di AWS accesso AWS CLI rifletterà le autorizzazioni utente aggiornate entro 1 ora dall'aggiunta o dalla rimozione di un utente da quel gruppo.

Informazioni sulle differenze di orario

- Efficace immediatamente: azioni che richiedono una riautenticazione immediata.
- Entro 30 minuti - 2 ore: le sessioni applicative richiedono tempo per verificare con IAM Identity Center e scoprire eventuali modifiche.

- Entro 12 ore o meno, le sessioni di ruolo IAM funzionano in modo indipendente e terminano solo alla scadenza della durata configurata.

Disconnessione singola

[IAM Identity Center non supporta SAML Single Logout \(un protocollo che disconnette automaticamente gli utenti da tutte le applicazioni connesse quando si disconnettono da una\) avviato da un provider di identità che funge da fonte di identità](#). Inoltre, non invia SAML Single Logout alle [applicazioni SAML 2.0](#) che utilizzano IAM Identity Center come provider di identità.

Le migliori pratiche per la gestione delle sessioni

Una gestione efficace delle sessioni richiede una configurazione e un monitoraggio accurati. Le organizzazioni devono configurare la durata delle sessioni in base ai propri requisiti di sicurezza, in genere utilizzando durate più brevi per applicazioni e ambienti sensibili.

L'implementazione di processi per terminare le sessioni quando gli utenti cambiano ruolo o lasciano l'organizzazione è essenziale per mantenere i limiti di sicurezza. La revisione regolare delle sessioni attive dovrebbe essere integrata nelle pratiche di monitoraggio della sicurezza per rilevare comportamenti anomali che potrebbero indicare problemi di sicurezza, come modelli di accesso insoliti, orari o luoghi di accesso imprevisti o accesso a risorse al di fuori delle normali funzioni lavorative.

Configura la durata della sessione in IAM Identity Center

Puoi configurare la durata della sessione per gli utenti della tua forza lavoro quando utilizzano le applicazioni Portale di accesso AWS e che funzionano con IAM Identity Center, incluso Kiro. IAM Identity Center offre i seguenti tipi di sessione: sessioni interattive utente, sessioni utente in background e sessioni estese per Kiro.

Argomenti

- [Sessioni interattive per utenti](#)
- [Sessioni in background degli utenti](#)
- [Sessioni estese per Kiro](#)
- [Visualizza e termina le sessioni attive per gli utenti della tua forza lavoro](#)
- [Considerazioni sulla durata della sessione per l'utilizzo delle fonti di identità, della AWS CLI e AWS SDKs](#)

Sessioni interattive per utenti

Le sessioni interattive dell'utente sono sessioni legate all'accesso di un utente al portale di AWS accesso o all'accesso alle [applicazioni AWS gestite](#). La durata della sessione di autenticazione nelle applicazioni Portale di accesso AWS è il periodo di tempo massimo durante il quale un utente può accedere senza eseguire nuovamente l'autenticazione. Se si termina una sessione attiva del portale di AWS accesso, vengono interrotte anche tutte le sessioni per queste applicazioni gestite.

La durata predefinita della sessione per le sessioni interattive con l'utente è di 8 ore. È possibile specificare una durata diversa, da un minimo di 15 minuti a un massimo di 90 giorni. I valori di durata personalizzati devono essere inseriti in minuti e devono essere compresi tra 15 minuti e 129.600 minuti (90 giorni). Per ulteriori informazioni, consulta [Comprendere le sessioni di autenticazione in IAM Identity Center](#).

Per considerazioni quali il modo in cui le fonti di identità di IAM Identity Center potrebbero influire sulla durata della sessione interattiva dell'utente, consulta [the section called “Considerazioni per le fonti di identità, la AWS CLI e AWS SDKs”](#)

Per configurare la durata di una sessione interattiva con l'utente

1. Apri la console Centro identità IAM.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Autenticazione.
4. In Autenticazione, accanto a Durata della sessione, scegli Configura. Viene visualizzata una finestra di dialogo Configura la durata della sessione.
5. Nella finestra di dialogo Configura la durata della sessione, in Sessioni interattive utente, scegli la durata massima della sessione per gli utenti selezionando la freccia a discesa. Scegli la durata della sessione, quindi scegli Salva.

Note

Le modifiche alla durata della sessione si applicano solo alle nuove sessioni. Le sessioni correnti mantengono la loro durata originale.

6. Si torna alla scheda Autenticazione. Sopra la scheda viene visualizzato un messaggio di notifica verde che indica che le impostazioni della sessione sono state aggiornate correttamente.

Sessioni in background degli utenti

Le sessioni utente in background consentono a un utente di avviare un processo di lunga durata su un'applicazione AWS gestita come [Amazon SageMaker Studio](#), senza che l'utente debba rimanere connesso durante l'esecuzione del processo. Il processo viene eseguito immediatamente e utilizza la funzionalità [affidabile di propagazione dell'identità](#) di IAM Identity Center per garantire che le autorizzazioni dell'utente vengano mantenute mentre il lavoro viene eseguito in background. Il processo può continuare a essere eseguito anche se l'utente spegne il computer, la sessione di accesso a IAM Identity Center scade o l'utente si disconnette dal portale di accesso. AWS Questa funzionalità consente ai data scientist, agli ingegneri dell'apprendimento automatico e ad altri di avviare flussi di lavoro di analisi e apprendimento automatico eseguiti in background senza il coinvolgimento attivo dell'utente.

Le sessioni utente in background sono abilitate per impostazione predefinita per le applicazioni AWS gestite supportate come Amazon SageMaker Studio. Per utilizzare questa funzionalità, tuttavia, devi abilitare la propagazione delle identità affidabili in Amazon SageMaker Studio quando crei o aggiorni un dominio. Per ulteriori informazioni, consulta [Abilita la propagazione delle identità affidabili nel tuo dominio Amazon SageMaker AI](#).

La durata predefinita della sessione per le sessioni utente in background è di 7 giorni. È possibile specificare una durata diversa, da un minimo di 15 minuti a un massimo di 90 giorni. I valori di durata personalizzati devono essere inseriti in minuti e devono essere compresi tra 15 minuti e 129.600 minuti (90 giorni).

Tieni presente le seguenti considerazioni per le sessioni utente in background:

- Una sessione utente in background può essere creata solo quando un utente avvia manualmente un processo in Amazon SageMaker Studio. Questa funzionalità non è supportata per i flussi di lavoro automatizzati e pianificati.
- Per un elenco delle AWS regioni che supportano le sessioni in background degli utenti, consulta [AWS Regioni supportate](#).
- È possibile visualizzare le sessioni utente in background in CloudTrail. Per informazioni, vedere [Identificazione dei dettagli della sessione in background dell'utente](#).
- Puoi anche terminare le sessioni attive per un utente della tua organizzazione. Per informazioni, consulta [Termina le sessioni attive per gli utenti della tua forza lavoro](#).

Per configurare la durata di una sessione utente in background

1. Apri la console Centro identità IAM.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Autenticazione.
4. In Autenticazione, accanto a Durata della sessione, scegli Configura. Viene visualizzata la finestra di dialogo Configura la durata della sessione.
5. Nella finestra di dialogo Configura la durata della sessione, se la casella di controllo Abilita sessioni utente in background non è già selezionata, selezionala. Deseleziona la casella di controllo per disabilitare le sessioni utente in background.

Note

Le sessioni correnti non vengono influenzate se si disattivano le sessioni utente in background.

6. In Sessioni utente in background, scegli la durata massima della sessione selezionando la freccia a discesa. Scegli la durata della sessione, quindi scegli Salva.

Note

Le modifiche alla durata della sessione si applicano solo alle nuove sessioni. Le sessioni correnti mantengono la loro durata originale.

7. Si torna alla scheda Autenticazione. Sopra la scheda viene visualizzato un messaggio di notifica verde che indica che le impostazioni della sessione sono state aggiornate correttamente.

Note

Un'applicazione gestita dal cliente non può creare una sessione utente in background.

Sessioni estese per Kiro

Se i tuoi sviluppatori usano Kiro come parte di un ambiente di sviluppo integrato (IDE), puoi impostare la durata della sessione per Kiro su 90 giorni. A seconda di quando hai abilitato IAM Identity Center, la durata della sessione estesa per Kiro potrebbe essere abilitata per impostazione predefinita.

Questa sessione estesa non influisce sulla durata della sessione del portale di AWS accesso o di altre applicazioni AWS gestite.

Per considerazioni come il modo in cui le fonti di identità di IAM Identity Center potrebbero influire sulla durata estesa della sessione, consulta [the section called “Considerazioni per le fonti di identità, la AWS CLI e AWS SDKs”](#).

Note

Kiro è accessibile dalle console impostate come commerciali Regioni AWS che sono abilitate di default. Se l'istanza di IAM Identity Center si trova in una regione in cui Kiro non è attualmente accessibile, l'attivazione della durata estesa della sessione di 90 giorni non sostituirà l'impostazione predefinita. Ciò significa che la durata della sessione rimane invariata, indipendentemente dal fatto che abiliti o meno la durata della sessione estesa di 90 giorni. Per informazioni, vedi [AWS Regioni supportate per Kiro](#).

Per estendere una sessione per Kiro

1. Apri la console Centro identità IAM.
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Autenticazione.
4. In Autenticazione, accanto a Durata della sessione, scegli Configura. Viene visualizzata una finestra di dialogo Configura la durata della sessione.
5. Nella finestra di dialogo Configura la durata della sessione, seleziona la casella di controllo Abilita sessioni estese per Kiro. Deseleziona la casella di controllo per disabilitare le sessioni di sessione estese per Kiro.
6. Scegli Salva per tornare alla pagina Impostazioni.

Visualizza e termina le sessioni attive per gli utenti della tua forza lavoro

In qualità di amministratore di IAM Identity Center, puoi visualizzare l'elenco delle sessioni attive degli utenti della tua forza lavoro e, se necessario, terminare una o più sessioni per un utente. Ad esempio, potresti dover terminare le sessioni di un utente quando:

- L'utente non richiede più le sessioni.

- L'utente non deve mantenere lo stato di autenticazione corrente. Ciò può verificarsi quando l'utente lascia l'azienda o le sue autorizzazioni cambiano.

Puoi visualizzare e terminare queste sessioni utilizzando la console IAM Identity Center. I tuoi utenti possono anche visualizzare e terminare le proprie sessioni utilizzando il portale di AWS accesso. Per informazioni su come gli utenti della forza lavoro possono visualizzare e terminare le sessioni senza l'assistenza di un amministratore, consulta [Visualizzazione e fine della sessione attiva](#).

Note

La fine di una sessione attiva per un utente di IAM Identity Center non pone fine a nessuna sessione di ruolo IAM attiva in sala operatoria Console di gestione AWS . AWS CLI Per ulteriori informazioni, consulta [Comprendere le sessioni di autenticazione in IAM Identity Center](#).

Per terminare una sessione attiva per un utente della forza lavoro (console IAM Identity Center)

1. Apri la console Centro identità IAM.
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 per questo utente.
5. Cerca sessioni utente in background (opzionale)

Per cercare le sessioni in base all'Amazon Resource Name (ARN) del processo che utilizza la sessione, nell'elenco Tipo di sessione, scegli Sessioni utente in background, quindi inserisci l'ARN del lavoro nella casella di ricerca.

Note

Puoi terminare solo le sessioni attive caricate. Se un utente ha molte sessioni, scegli Carica altre sessioni attive per visualizzare sessioni aggiuntive.

6. Seleziona la casella di controllo accanto a ogni sessione che desideri terminare, quindi scegli Termina sessioni.

7. Viene visualizzata una finestra di dialogo che conferma che stai terminando le sessioni attive per questo utente. Esamina le informazioni e, se vuoi continuare, digita `confirm`, quindi scegli **Termina sessioni**.
8. Verrai reindirizzato alla pagina dell'utente. Viene visualizzato un messaggio di notifica verde per indicare che le sessioni selezionate sono state terminate correttamente.

Considerazioni sulla durata della sessione per l'utilizzo delle fonti di identità, della AWS CLI e AWS SDKs

Di seguito sono riportate alcune considerazioni per la configurazione della durata della sessione se si utilizza Microsoft Active Directory (AD) o un provider di identità esterno (IdP) come origine dell'identità, oppure i AWS Software Development Kit (SDKs) o altri strumenti di sviluppo per accedere ai servizi a livello di AWS programmazione. AWS Command Line Interface AWS

Microsoft Active Directory, sessioni interattive per gli utenti e sessioni estese per Kiro

Se utilizzi Microsoft Active Directory (AD) come origine dell'identità e configuri la durata della sessione per le sessioni interattive con l'utente o le sessioni estese per Kiro, tieni a mente le seguenti considerazioni.

Note

Queste considerazioni non si applicano alle sessioni utente in background.

Indipendentemente dal fatto che si utilizzi AD AWS Managed Microsoft AD Connector o sia configurato in AWS Directory Service, la durata massima dei ticket utente Kerberos definita in Microsoft AD può influire sulla durata di validità delle sessioni interattive utente e delle sessioni estese per Kiro. Per ulteriori informazioni su questa impostazione, vedi [Durata massima del ticket utente](#) sul sito Web di Microsoft.

- **AWS Managed Microsoft AD:** Se si utilizza configure AWS Managed Microsoft AD in AWS Directory Service, la durata massima dei ticket utente Kerberos è fissata a 10 ore. Pertanto, la durata della sessione interattiva dell'utente è impostata sull'impostazione più breve tra quelle dell'impostazione IAM Identity Center e su 10 ore. Ad esempio, se imposti la durata della sessione interattiva dell'utente su 12 ore, gli utenti devono autenticarsi nuovamente nel portale di AWS accesso dopo 10 ore. Lo stesso limite di 10 ore si applica alle sessioni prolungate per Kiro.

- **AD Connector:** se si utilizza AD Connector configurato in AWS Directory Service, la durata massima per i ticket Kerberos utente è definita in Microsoft AD dietro AD Connector. Il valore predefinito è 10 ore e ha lo stesso effetto sulle sessioni interattive degli utenti e sulle sessioni estese. AWS Managed Microsoft AD. Sebbene questo limite possa essere configurabile in Microsoft AD, si consiglia di collaborare con l'amministratore IT per valutare i rischi, soprattutto perché questa impostazione può influire sulla durata della sessione per altre applicazioni client Microsoft AD.

Provider di identità esterni, sessioni interattive con gli utenti e sessioni estese per Kiro

Se utilizzi un provider di identità (IdP) esterno e configuri la durata della sessione per sessioni interattive utente o sessioni estese per Kiro, tieni a mente le seguenti considerazioni.

Note

Queste considerazioni non si applicano alle sessioni utente in background.

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 (interattiva per l'utente) e di una sessione estesa 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. Allo stesso modo, se imposti una sessione estesa di 90 giorni per Kiro, gli utenti Kiro devono autenticarsi nuovamente dopo 90 giorni.
- Se `SessionNotOnOrAfter` viene passato in un'asserzione SAML, il valore della durata della sessione viene impostato sul valore più breve tra la sessione del portale di AWS accesso (interattiva per l'utente) o la durata della sessione estesa 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. Allo stesso modo, se imposti una sessione estesa di 90 giorni per Kiro, gli utenti Kiro devono autenticarsi nuovamente in Kiro dopo 18 ore.
- Se la durata della sessione del tuo IdP è più lunga di quella impostata in IAM Identity Center, i tuoi utenti possono iniziare una nuova sessione di IAM Identity Center senza reinserire le proprie credenziali, in base alla sessione di accesso ancora valida con il tuo IdP.

AWS CLI e sessioni SDK

Se si utilizza la AWS CLI 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 gestite. AWS SDKs AWS

- 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

Note

Per i casi d'uso di accesso all'account, se gli utenti utilizzano il set di autorizzazioni 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 per 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.

Le versioni minime SDKs supportano la gestione delle sessioni di IAM Identity Center

Di seguito sono elencate le versioni minime SDKs che supportano la gestione delle sessioni di IAM Identity Center.

SDK	Versione minima
Python	1.26.10
PHP	3,245,0
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: 1.18.0 credentials/v1.13.0, config/v
È V2	2,1253,0
È V3	v3.210.0
C++	1,9,372
.NET	v3.7.400.0

Disabilita l'accesso degli utenti e le applicazioni in IAM Identity Center Account AWS

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. La disabilitazione dell'accesso degli utenti impedisce loro di AWS accedere al portale di accesso e gli utenti non avranno più accesso alle applicazioni assegnate Account AWS e a quelle assegnate. Usa Disabilita l'accesso utente per la rimozione temporanea dell'accesso quando potresti dover ripristinare l'accesso in un secondo momento.

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 [Comprendere le sessioni di autenticazione in IAM Identity Center](#).

Per disabilitare l'accesso degli utenti in IAM Identity Center

1. Apri la [console Centro identità IAM](#).

 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.

Nega l'accesso degli utenti con Service Control Policies

Per negare immediatamente l'accesso per effettuare chiamate API autorizzate quando l'accesso di un utente IAM Identity Center è disabilitato o l'utente viene eliminato, puoi:

1. [Aggiungi o aggiorna](#) la [politica in linea](#) dei set di autorizzazioni assegnati all'utente aggiungendo un Deny effetto esplicito per tutte le azioni su tutte le risorse.
2. Specificare la chiave `aws:userid` o `identitystore:userid` condition.

In alternativa, puoi utilizzare una [policy di controllo dei servizi](#) per negare l'accesso dell'utente a tutti gli account membri dell'organizzazione.

Example Esempio: SCP per negare l'accesso

Questa politica di rifiuto blocca tutte le AWS azioni per un utente specifico, indipendentemente dalle altre autorizzazioni che potrebbero essere state concesse altrove. Questa politica ha la precedenza su qualsiasi politica. Allow

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "aws:UserId": "*:deleteduser@domain.com"
        }
      }
    }
  ]
}
```

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "identitystore:UserId": "DELETEDUSER_ID"
        }
      }
    }
  ]
}
```

```
}  
  }  
    ]  
  }
```

Gestione dell'accesso per gli utenti nella directory Identity Center

Scopri come gestire le password e l'autenticazione a più fattori (MFA) per gli utenti nella directory IAM Identity Center. Queste funzionalità di sicurezza aiutano a proteggere gli account utente.

Note

Queste funzionalità non si applicano agli utenti di Active Directory o agli utenti di provider di identità esterni.

Gli amministratori possono gestire sia le password che l'MFA tramite la console IAM Identity Center. Queste funzionalità di sicurezza funzionano solo con la directory Identity Center integrata.

Gestione delle password

La gestione delle password include le seguenti funzionalità:

- Reimpostazione delle password con istruzioni via e-mail
- Genera password monouso
- Configura la verifica automatica delle e-mail per gli utenti creati tramite API

AWS applica requisiti di sicurezza fissi, tra cui regole di complessità e restrizioni sul riutilizzo delle password.

MFA

L'MFA è abilitata per impostazione predefinita e supporta fino a otto dispositivi per utente.

I tipi di dispositivi supportati includono:

- App di autenticazione

- Chiavi di sicurezza
- Autenticatori biometrici integrati

Gli amministratori possono registrare e gestire i dispositivi MFA per gli utenti.

Argomenti

- [Configurazione delle password degli utenti](#)
- [MFA per gli utenti della directory Identity Center](#)

Configurazione delle password degli utenti

Per gli utenti creati nella directory Identity Center, gli amministratori possono gestire le politiche relative alle password, gestire gli utenti senza password iniziali e reimpostare le password quando necessario. Queste funzionalità di gestione delle password si applicano solo agli utenti nella directory integrata di Identity Center. Se utilizzi Active Directory o un provider di identità esterno, devi gestire le password in tali sistemi.

Opzioni di gestione delle password

- Requisiti relativi alle password: requisiti di sicurezza che gli utenti devono soddisfare quando impostano o modificano le password. Ciò include regole di complessità e restrizioni di riutilizzo.
- Configurazione unica della password: configura la verifica e-mail per gli utenti creati tramite API o CLI che non dispongono di password iniziali. Puoi anche generare password temporanee per l'accesso immediato.
- Reimpostazione delle password: reimposta le password per gli utenti bloccati o che necessitano di nuove credenziali. Puoi inviare istruzioni per la reimpostazione tramite e-mail o generare password monouso.

Argomenti

- [Requisiti relativi alle password per la gestione delle identità in IAM Identity Center](#)
- [Invia una password monouso agli utenti creati con API o CLI](#)
- [Reimposta la password utente di IAM Identity Center per un utente finale](#)

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 Directory](#) esempio 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 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.

Invia una password monouso agli utenti creati con API o CLI

Quando crei utenti con l'operazione [CreateUser](#) API o il comando `create-user` CLI, gli utenti non dispongono di password. Puoi aggiornare le impostazioni in IAM Identity Center per inviare a questi utenti un'e-mail di verifica dopo il primo tentativo di accesso, se hai specificato un'e-mail per l'utente al momento della creazione. Dopo aver ricevuto l'e-mail di verifica, l'utente deve impostare una password per accedere.

Se non abiliti questa impostazione, devi [generare una password monouso](#) e condividerla con gli utenti che crei utilizzando il comando `CreateUser` API o `create-user` CLI.

Per inviare un'e-mail di verifica dell'indirizzo e-mail agli utenti creati con il CreateUser comando API o **create-user** CLI

1. Apri la [console Centro identità IAM](#).
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Autenticazione.
4. Nella sezione Autenticazione standard, scegli Configura.
5. Nella finestra di dialogo Configura l'autenticazione standard, seleziona la casella di controllo Invia e-mail OTP. Poi, scegli Salva. Lo stato viene aggiornato da Disabilitato a Attivato.

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 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 si connette 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, vedi [Reimpostazione della password utente del portale di AWS accesso](#).

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 Centro identità IAM](#).
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.

MFA per gli utenti della directory Identity Center

 Important

L'MFA in IAM Identity Center non è attualmente supportata per i provider di [identità esterni](#).

IAM Identity Center è preconfigurato con l'autenticazione a più fattori (MFA) attivata per impostazione predefinita in modo che tutti gli utenti debbano accedere con MFA oltre al nome utente e alla password. Ciò garantisce che gli utenti debbano accedere al portale di AWS accesso utilizzando i seguenti due fattori:

- Il loro nome utente e la loro 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](#).

Argomenti

- [Tipi di MFA disponibili per IAM Identity Center](#)
- [Configurazione della tecnologia MFA in IAM Identity Center](#)
- [Registrazione di un dispositivo MFA per gli utenti](#)
- [Ridenominazione ed eliminazione dei dispositivi MFA in IAM Identity Center](#)

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.

- [FIDO2 autenticatori](#), 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 uno solo. Account AWS Puoi anche configurare le impostazioni MFA in modo che richieda l'autenticazione MFA ogni volta che tentano di accedere da un nuovo dispositivo o browser o quando accedono da un indirizzo IP sconosciuto. Per ulteriori informazioni su come configurare le impostazioni MFA per gli utenti, vedere [Scegli i tipi di MFA per l'autenticazione degli utenti](#) e [Configurazione dell'applicazione dei dispositivi MFA](#)

FIDO2 autenticatori

[FIDO2](#) è uno standard che include CTAP2 [WebAuthn](#) e si basa sulla crittografia a chiave pubblica. Le credenziali FIDO sono resistenti al phishing perché sono uniche per il sito Web in cui sono state create, ad esempio. AWS

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

Argomenti

- [Autenticatori integrati](#)
- [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. Directory Service include 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

È possibile 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 compatibili Directory Service, come Amazon RDS for SQL Server.

Se la tua MFA è disabilitata sulla console IAM Identity Center e hai configurato RADIUS MFA con, 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 della tecnologia MFA in IAM Identity Center

Puoi configurare le funzionalità di autenticazione a più fattori (MFA) in IAM Identity Center quando la tua origine di identità è configurata con l'identity store AWS Managed Microsoft AD di IAM Identity Center o AD Connector. L'MFA in IAM Identity Center non è attualmente supportata per i provider di [identità esterni](#).

Di seguito sono riportate le raccomandazioni generali sulla MFA, a seconda delle impostazioni e delle preferenze organizzative di IAM Identity Center.

- Gli utenti sono invitati a registrare più autenticator 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 stai già utilizzando RADIUS MFA con cui hai configurato 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](#).
- Il YouTube video seguente fornisce una panoramica di MFA e IAM Identity Center:

[IAM Identity Center: impostazioni predefinite di autenticazione a più fattori per le nuove istanze](#)

Argomenti

- [Richiedi agli utenti l'MFA](#)
- [Scegli i tipi di MFA per l'autenticazione degli utenti](#)
- [Configurazione dell'applicazione dei dispositivi MFA](#)
- [Consenti agli utenti di registrare i propri dispositivi MFA](#)

Richiedi agli utenti l'MFA

È possibile utilizzare i passaggi seguenti per determinare la frequenza con cui agli utenti della forza lavoro viene richiesta l'autenticazione a più fattori (MFA) ogni volta che tentano di accedere al portale di accesso. AWS Prima di iniziare, ti consigliamo di comprendere il [Tipi di MFA disponibili per IAM Identity Center](#)

Important

Le istruzioni contenute 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.

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 configurare l'MFA

1. Apri la [console Centro identità IAM](#).
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:

- Ogni volta che accedono (sempre attivo)

In questa modalità (l'impostazione predefinita), IAM Identity Center richiede che agli utenti con un dispositivo MFA registrato venga richiesto ogni volta che accedono. Questa è l'impostazione più sicura e garantisce l'applicazione delle politiche organizzative o di conformità richiedendo che l'MFA venga utilizzata ogni volta che accedono AWS al portale di accesso. Ad esempio, PCI DSS consiglia vivamente l'MFA durante ogni accesso per accedere alle applicazioni che supportano transazioni di pagamento ad alto rischio.

- Solo quando il loro contesto di accesso cambia (sensibile al contesto)

In questa modalità, 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, ma è meno sicura dell'opzione always-on. Agli utenti viene richiesta l'autenticazione a più fattori solo se il contesto di accesso cambia.

- Mai (disabilitato)

In questa modalità, tutti gli utenti accederanno solo con il nome utente e la password standard. La scelta di questa opzione disabilita l'MFA di IAM Identity Center e non è consigliata.

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

Note

Se utilizzi già RADIUS MFA con 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. Scegli Salva modifiche.

Argomenti correlati

- [Scegli i tipi di MFA per l'autenticazione degli utenti](#)
- [Configurazione dell'applicazione dei dispositivi MFA](#)
- [Consenti agli utenti di registrare i propri dispositivi MFA](#)

Scegli i tipi di MFA per l'autenticazione degli utenti

Utilizza la procedura seguente per scegliere i tipi di dispositivi con cui gli utenti possono autenticarsi quando viene richiesta l'autenticazione a più fattori (MFA) nel portale di accesso. AWS

Per configurare i tipi di MFA per i tuoi utenti

1. Apri la [console Centro identità IAM](#).

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](#).
 - Chiavi di sicurezza e autenticatori integrati
 - App di autenticazione
6. Scegli Save changes (Salva 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 ulteriori informazioni sulla MFA in IAM, consulta [Autenticazione a AWS più fattori](#) in IAM.

Per configurare l'applicazione dei dispositivi MFA per i tuoi utenti

1. Apri la [console Centro identità IAM](#).
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 `ActiveDirectoryemail`. 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. Scegli Save changes (Salva modifiche).

Consenti agli utenti di registrare i propri dispositivi MFA

Gli amministratori di IAM Identity Center possono consentire agli utenti di registrare autonomamente i propri dispositivi MFA.

Per consentire agli utenti di registrare i propri dispositivi MFA

1. Apri la [console Centro identità IAM](#).
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. Scegli Save changes (Salva modifiche).

Note

Dopo aver configurato l'autoregistrazione per i tuoi utenti, potresti voler inviare loro un link alla procedura. [Registrazione del dispositivo per l'MFA](#) Questo argomento fornisce istruzioni su come configurare i propri dispositivi MFA.

Registrazione di un dispositivo MFA per gli utenti

Gli amministratori di IAM Identity Center possono configurare un nuovo dispositivo MFA per l'accesso da parte di un utente specifico nella console IAM Identity Center. Gli amministratori devono avere 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 Centro identità IAM](#).
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. 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 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.

Ridenominazione ed eliminazione dei dispositivi MFA in IAM Identity Center

Gli amministratori di IAM Identity Center possono utilizzare le seguenti procedure per rinominare o eliminare il dispositivo MFA di un utente.

Per rinominare un dispositivo MFA

1. Apri la [console Centro identità IAM](#).
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 Centro identità IAM](#).
2. Nel riquadro di navigazione a sinistra, seleziona Users (Utenti). Scegliete 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.

Configurare 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 relative console applicative o tramite l'applicazione APIs. 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 Console di gestione AWS a un gruppo specifico Account AWS dell'organizzazione. Per ulteriori informazioni, consulta [Configurare l'accesso a Account AWS](#).

Argomenti

- [AWS applicazioni gestite](#)
- [Applicazioni gestite dal cliente](#)
- [Panoramica sulla propagazione delle identità affidabili](#)
- [Configurazione della propria applicazione 2.0 OAuth](#)
- [Ruota i certificati IAM Identity Center](#)
- [Comprendi le proprietà dell'applicazione nella console IAM Identity Center](#)
- [Assegna l'accesso degli utenti alle applicazioni nella console IAM Identity Center](#)
- [Rimuovi l'accesso degli utenti alle applicazioni SAML 2.0](#)
- [Mappa gli attributi dell'applicazione agli attributi di IAM Identity Center](#)

AWS applicazioni gestite

AWS IAM Identity Center semplifica e semplifica il compito di connettere gli utenti della forza lavoro ad applicazioni AWS gestite come Kiro e Amazon Quick. Con IAM Identity Center, puoi connettere il tuo provider di identità esistente una sola volta e sincronizzare utenti e gruppi dalla tua directory, oppure creare e gestire i tuoi utenti direttamente in IAM Identity Center. Fornendo un punto di federazione, IAM Identity Center elimina la necessità di configurare la federazione o la sincronizzazione di utenti e gruppi per ogni applicazione e riduce il lavoro amministrativo. È inoltre possibile avere una [visione comune delle assegnazioni di utenti e gruppi](#).

Per una tabella delle AWS applicazioni che funzionano con IAM Identity Center, consulta [AWS applicazioni gestite che è possibile utilizzare con IAM Identity Center](#).

Controllo dell'accesso alle applicazioni AWS gestite

L'accesso alle applicazioni AWS gestite è controllato in due modi:

- Accesso iniziale all'applicazione

IAM Identity Center gestisce questo processo tramite assegnazioni all'applicazione. Per impostazione predefinita, le assegnazioni sono obbligatorie per le applicazioni AWS gestite. Se sei un amministratore dell'applicazione, puoi scegliere se richiedere assegnazioni a un'applicazione.

Se le assegnazioni sono obbligatorie, quando gli utenti accedono a Portale di accesso AWS, solo gli utenti assegnati all'applicazione direttamente o tramite un'assegnazione di gruppo possono visualizzare il riquadro dell'applicazione.

Se le assegnazioni non sono obbligatorie, 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 accesso AWS.

Important

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.

- Accesso alle risorse dell'applicazione

L'applicazione gestisce tutto ciò tramite assegnazioni di risorse indipendenti che controlla.

AWS le applicazioni gestite forniscono un'interfaccia utente amministrativa che è possibile utilizzare per gestire l'accesso alle risorse dell'applicazione. Ad esempio, gli amministratori di Quick possono assegnare agli utenti l'accesso ai dashboard in base all'appartenenza al gruppo. La maggior parte delle applicazioni AWS gestite offre inoltre un' Console di gestione AWS 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.

Condivisione delle informazioni sull'identità

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 del servizio (SCPs) per controllare quali applicazioni possono accedere alle informazioni in quali account AWS Organizations.

Ad esempio, se abiliti l'accesso solo nell'account di AWS Organizations gestione, le applicazioni negli account dei membri non avranno accesso alle informazioni. Tuttavia, se si abilita l'accesso in tutti gli account, è possibile utilizzare questa opzione SCPs per impedire l'accesso a tutte le applicazioni ad eccezione di quelle che si desidera autorizzare.

Le politiche di controllo dei servizi sono una funzionalità di AWS Organizations. Per istruzioni su come allegare un SCP, consulta [Allegare e scollegare le politiche di controllo del servizio](#) nella Guida per l'utente AWS Organizations.

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 [Gestione degli utenti nella directory 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 [Microsoft AD elenco](#)
 - Provider di identità esterno: per ulteriori informazioni, vedere [Provider di identità esterni](#).

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.

Limitazione dell'uso di applicazioni gestite AWS

Quando attivi per la prima volta IAM Identity Center, diventa disponibile come fonte di identità per le applicazioni AWS gestite su tutti gli account del tuo AWS Organizations. Per limitare le applicazioni, è necessario implementare le politiche di controllo del servizio (SCP). SCPs sono una funzionalità AWS Organizations che è possibile utilizzare per controllare centralmente le autorizzazioni massime che le identità (utenti e ruoli) dell'organizzazione possono avere. Puoi utilizzarla SCPs 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. Per ulteriori informazioni, consulta [Service control policies \(SCPs\)](#) nella Guida per l'AWS Organizations utente.

Il seguente esempio di SCP blocca l'accesso alle informazioni su utenti e gruppi di IAM Identity Center e impedisce l'avvio dell'applicazione, tranne negli account designati (1111 e 222222222222):

```
{
  "Sid": "DenyIdCExceptInDesignatedAWSAccounts",
  "Effect": "Deny",
  "Action": [
    "identitystore:*",
    "sso:*",
    "sso-directory:*",
    "sso-oauth:*"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalAccount": [
        "111111111111",
        "222222222222"
      ]
    }
  }
}
```

AWS applicazioni gestite che è possibile utilizzare con IAM Identity Center

IAM Identity Center ti consente di connettere la tua fonte di identità esistente o di creare utenti una sola volta. Ciò consente agli amministratori delle applicazioni di gestire l'accesso alle seguenti applicazioni AWS gestite senza federazione separata o sincronizzazione di utenti e gruppi.

Tutte le applicazioni AWS gestite nella tabella seguente si integrano con le [istanze organizzative di IAM Identity Center](#). La tabella fornisce inoltre informazioni su quanto segue per un'applicazione AWS gestita supportata:

- Se l'applicazione si integra anche con le istanze di account di IAM Identity Center
- Se l'applicazione può abilitare la propagazione affidabile dell'identità tramite IAM Identity Center
- Se l'applicazione supporta IAM Identity Center configurato con una chiave KMS gestita dal cliente
- Se l'applicazione supporta l'implementazione in regioni aggiuntive di IAM Identity Center

Note

Le applicazioni che supportano l'implementazione in regioni aggiuntive di IAM Identity Center supportano anche IAM Identity Center configurato con una chiave KMS gestita dal cliente.

Tutte le applicazioni AWS gestite elencate qui supportano l'implementazione nella regione principale. Per ulteriori informazioni, consulta [the section called “Distribuzione e gestione di applicazioni AWS gestite su più piattaforme Regioni AWS”](#).

AWS applicazioni gestite che si integrano con IAM Identity Center

AWS applicazione gestita	Integrato con le istanze di account di IAM Identity Center	Consente la propagazione affidabile delle identità tramite IAM Identity Center	Supporta IAM Identity Center configurato con una chiave KMS gestita dal cliente	Supporta l'implementazione in regioni aggiuntive di IAM Identity Center
Amazon Athena SQL	Sì	Sì	Sì	No
Amazon CodeCatalyst	Sì	No	Sì	No
Amazon DataZone	Sì	Sì	Sì	No
Funzionalità di Amazon EKS	Sì	Sì	Sì	No
Amazon EMR su EC2	Sì	Sì	Sì	No
Amazon EMR su EKS	Sì	Sì	Sì	No
Amazon EMR Serverless	Sì	Sì	Sì	No
Amazon EMR Studio	Sì	Sì	Sì	No
Amazon Kendra	No	No	Sì	No
Grafana gestito da Amazon	No	No	Sì	No
Amazon Monitron	No	No	No	No
OpenSearch Servizio Amazon	Sì	Sì	Sì	No

AWS applicazione gestita	Integrato con le istanze di account di IAM Identity Center	Consente la propagazione affidabile delle identità tramite IAM Identity Center	Supporta IAM Identity Center configurato con una chiave KMS gestita dal cliente	Supporta l'implementazione in regioni aggiuntive di IAM Identity Center
OpenSearch Servizio Amazon Serverless Service	Sì	Sì	Sì	No
Amazon Q Business	Sì	Sì	Sì	No
Amazon Quick	Sì	Sì	Sì	No
Amazon Redshift	Sì ²	Sì	Sì	Sì
Amazon S3 Access Grants	Sì	Sì	Sì	Sì
Amazon SageMaker Studio	No	Sì	Sì	No
Amazon SageMaker Unified Studio	Sì	Sì	Sì	No
Amazon WorkMail	Sì	Sì	Sì	No
Amazon WorkSpaces	Sì	No	Sì	No
Amazon WorkSpaces Secure Browser	No	No	Sì	No
AWS App Studio	Sì	No	No	No
AWS Deadline Cloud	Sì	No	Sì	Sì
AWS Glue	Sì	Sì	Sì	No
AWS IoT Events	No	No	No	No

AWS applicazione gestita	Integrato con le istanze di account di IAM Identity Center	Consente la propagazione affidabile delle identità tramite IAM Identity Center	Supporta IAM Identity Center configurato con una chiave KMS gestita dal cliente	Supporta l'implementazione in regioni aggiuntive di IAM Identity Center
AWS IoT SiteWise	No	No	No	No
AWS Lake Formation	Sì	Sì	Sì	Sì
AWS re:Post Private	Sì	No	Sì	No
Catena di approvvigionamento di AWS	Sì	No	Sì	No
AWS Systems Manager	No	No	Sì	Sì, Fleet Manager Remote Desktop
AWS Transfer Family app web	Sì	Sì	Sì	No
AWS Trasformazione	Sì	No	Sì	No
Accesso verificato da AWS	No	No	Sì	No
Kiro	Sì ¹	Sì	Sì	No
Approvazione multiparte	No	Sì	Sì	No
OpenSearch user interface (Dashboards)	Sì	Sì	Sì	No

¹ Per Kiro, le istanze di account di IAM Identity Center sono supportate a meno che gli utenti non richiedano l'accesso al set completo di funzionalità di Kiro sui siti Web. AWS Per ulteriori informazioni, consulta [Configurare Kiro nella Guida per l'utente di Kiro](#).

² Per Amazon Redshift, sono supportate le istanze di account di IAM Identity Center ad eccezione di applicazioni come Query Editor v2 che richiedono set di autorizzazioni, che non sono supportate dalle istanze dell'account.

Note

Alcuni AWS servizi, come Amazon Connect, non AWS Client VPN sono elencati in questa tabella, sebbene sia possibile utilizzarli con IAM Identity Center. Questo perché si integrano con IAM Identity Center utilizzando esclusivamente SAML e sono quindi classificati come applicazioni [gestite dal cliente](#).

Avvio rapido: configurazione di IAM Identity Center per testare AWS le applicazioni gestite

Se l'amministratore non ti ha già fornito l'accesso a IAM Identity Center, puoi utilizzare i passaggi descritti in questo argomento per configurare IAM Identity Center per testare le applicazioni AWS gestite. Imparerai come abilitare IAM Identity Center, creare un utente direttamente in IAM Identity Center e assegnarlo a un'applicazione AWS gestita.

Questo argomento fornisce passaggi rapidi su come abilitare IAM Identity Center in uno dei seguenti modi:

- Con AWS Organizations: se scegli questa opzione, viene creata un'istanza organizzativa di IAM Identity Center.
- Solo in base alle tue esigenze Account AWS: se scegli questa opzione, viene creata un'istanza di account di IAM Identity Center.

Per informazioni su questi tipi di istanze, consulta [Istanze di organizzazione e account di IAM Identity Center](#).

Prerequisiti

Prima di abilitare IAM Identity Center, conferma quanto segue:

- Ne possiedi uno Account AWS: se non ne possiedi uno Account AWS, consulta la sezione Guida [introduttiva alla gestione dell'AWS account Account AWS](#) nella Guida di riferimento per la gestione dell'account.

- L'applicazione AWS gestita funziona con IAM Identity Center: consulta l'elenco [AWS applicazioni gestite che è possibile utilizzare con IAM Identity Center](#) per confermare che l'applicazione AWS gestita che desideri testare funzioni con IAM Identity Center.
- Hai esaminato le considerazioni regionali: assicurati che l'applicazione AWS gestita che desideri testare sia supportata nel luogo in Regione AWS cui abiliti IAM Identity Center. Per ulteriori informazioni, consulta la documentazione dell'applicazione AWS gestita.

Note

È necessario distribuire l'applicazione AWS gestita nella stessa regione in cui si prevede di abilitare IAM Identity Center.

Configurazione di un'istanza organizzativa di IAM Identity Center per testare le applicazioni AWS gestite

Note

Questo argomento descrive come abilitare IAM Identity Center con AWS Organizations, che è il metodo consigliato per abilitare IAM Identity Center.

Conferma le tue autorizzazioni

Per abilitare IAM Identity Center con AWS Organizations, devi accedere alla Console di AWS gestione in uno dei modi seguenti:

- Un utente con autorizzazioni amministrative nel Account AWS luogo in cui verrà abilitato IAM Identity Center. AWS Organizations
- L'utente root (non consigliato a meno che non esistano altri utenti amministrativi).

Important

L'utente root ha accesso a tutti i AWS servizi e le risorse dell'account. Come procedura consigliata in materia di sicurezza, a meno che non si disponga di altre credenziali, non utilizzare le credenziali root dell'account per accedere AWS alle risorse. Queste credenziali forniscono un accesso illimitato all'account e sono difficili da revocare.

Passaggio 1. Abilita IAM Identity Center con AWS Organizations

1. Effettua una delle seguenti operazioni per accedere a Console di gestione AWS.
 - 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 con una versione autonoma Account AWS (credenziali IAM): accedi utilizzando le tue credenziali IAM con autorizzazioni amministrative.
2. Nella home page della console di AWS gestione, seleziona il servizio IAM Identity Center o accedi alla console [IAM Identity Center](#).
3. Scegli Abilita e abilita IAM Identity Center con AWS Organizations. Quando lo fai, crei un'[istanza organizzativa](#) di IAM Identity Center.

Passaggio 2. Crea un utente amministrativo in IAM Identity Center

Questa procedura descrive come creare un utente direttamente nella directory integrata di Identity Center. Questa directory non è connessa a nessun'altra directory che l'amministratore potrebbe utilizzare per gestire gli utenti della forza lavoro. Dopo aver creato l'utente in IAM Identity Center, specificherai nuove credenziali per questo utente. Quando accedi come questo utente per testare la tua applicazione AWS gestita, accederai con le nuove credenziali, non con le credenziali esistenti che utilizzi per accedere alle risorse aziendali.

Note

Ti consigliamo di utilizzare questo metodo per creare utenti solo a scopo di test.

1. Nel pannello di navigazione della console IAM Identity Center, scegli Utenti, quindi scegli Aggiungi utente.
2. Segui le indicazioni nella console per aggiungere l'utente. Mantieni selezionata l'opzione Invia un'e-mail a questo utente con le istruzioni per l'impostazione della password e assicurati di specificare un indirizzo e-mail a cui hai accesso.
3. Nel riquadro di navigazione, scegli Account AWS, seleziona la casella di controllo accanto al tuo account e scegli Assegna utenti o gruppi.
4. Scegli la scheda Utenti, seleziona la casella di controllo accanto all'utente che hai appena aggiunto e scegli Avanti.

5. Scegli Crea set di autorizzazioni e segui le indicazioni nella console per creare il set di autorizzazioni AdministratorAccess predefinito.
6. Al termine, il nuovo set di autorizzazioni viene visualizzato nell'elenco. Chiudi la scheda Set di autorizzazioni nella finestra del browser, torna alla scheda Assegna utenti e gruppi e scegli l'icona di aggiornamento accanto a Crea set di autorizzazioni.
7. Nella scheda Assegna utenti e gruppi del browser, il nuovo set di autorizzazioni viene visualizzato nell'elenco. Seleziona la casella di controllo accanto al nome del set di autorizzazioni, scegli Avanti e quindi scegli Invia.
8. Disconnettiti dalla console .

Fase 3. Accedi al portale di AWS accesso come utente amministrativo

Il portale di AWS accesso è un portale Web che fornisce all'utente creato l'accesso alla console di AWS gestione. Prima di poter accedere al portale di AWS accesso, è necessario accettare l'invito a iscriversi a IAM Identity Center e attivare le credenziali utente.

1. Controlla la tua email per l'oggetto Invito a iscriverti a AWS IAM Identity Center.
2. Scegli Accetta invito e segui le istruzioni sulla pagina di registrazione per impostare una nuova password, accedere e registrare un dispositivo MFA per il tuo utente.
3. Dopo aver registrato il dispositivo MFA, si apre il portale di AWS accesso.
4. Nel portale di AWS accesso, seleziona il tuo Account AWS e scegli AdministratorAccess. Verrai reindirizzato alla console di AWS gestione.

Passaggio 4. Configura l'applicazione AWS gestita per utilizzare IAM Identity Center

1. Dopo aver effettuato l'accesso alla console di AWS gestione, apri la console per l'applicazione AWS gestita che intendi utilizzare.
2. Segui le indicazioni nella console per configurare l'applicazione AWS gestita per utilizzare IAM Identity Center. Durante questo processo, puoi assegnare l'utente che hai creato all'applicazione.

Configurazione di un'istanza di account di IAM Identity Center per testare le applicazioni AWS gestite

Note

Un'istanza di account di IAM Identity Center limita la distribuzione a una singola Account AWS. È necessario abilitare questa istanza nella Regione AWS stessa AWS applicazione che si desidera testare.

Conferma la tua app

Tutte le applicazioni AWS gestite che funzionano con IAM Identity Center possono essere utilizzate con le istanze organizzative di IAM Identity Center. Tuttavia, solo alcune di queste applicazioni possono essere utilizzate con le istanze di account di IAM Identity Center. Consulta l'elenco di [AWS applicazioni gestite che è possibile utilizzare con IAM Identity Center](#)

Fase 1. Abilitazione di un'istanza account del Centro identità IAM

1. Effettua una delle seguenti operazioni per accedere a. Console di gestione AWS
 - 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 con una versione autonoma Account AWS (credenziali IAM): accedi utilizzando le tue credenziali IAM con autorizzazioni amministrative.
2. Nella home page della console di AWS gestione, seleziona il servizio IAM Identity Center o accedi alla console [IAM](#) Identity Center.
3. Scegli Abilita .
4. Nella AWS Organizations pagina Abilita IAM Identity Center con, scegli Abilita un'istanza di account di IAM Identity Center.
5. Nella pagina Abilita l'istanza dell'account di IAM Identity Center, esamina le informazioni e, facoltativamente, aggiungi i tag che desideri associare a questa istanza di account. Quindi scegli Abilita.

Passaggio 2. Crea un utente in IAM Identity Center

Questa procedura descrive come creare un utente direttamente nella directory integrata di Identity Center. Questa directory non è connessa a nessun'altra directory che l'amministratore potrebbe utilizzare per gestire gli utenti della forza lavoro. Dopo aver creato l'utente in IAM Identity Center, specificherai nuove credenziali per questo utente. Quando accedi come utente per testare la tua applicazione AWS gestita, accederai con le nuove credenziali. Le nuove credenziali non ti consentiranno di accedere ad altre risorse aziendali.

Note

Si consiglia di utilizzare questo metodo per creare utenti solo a scopo di test.

1. Nel pannello di navigazione della console IAM Identity Center, scegli Utenti, quindi scegli Aggiungi utente.
2. Segui le indicazioni nella console per aggiungere l'utente. Mantieni selezionata l'opzione Invia un'e-mail a questo utente con le istruzioni per l'impostazione della password e assicurati di specificare un indirizzo e-mail a cui hai accesso.
3. Disconnettiti dalla console .

Fase 3. Accedi al portale di AWS accesso come utente IAM Identity Center

Il portale di AWS accesso è un portale web che fornisce all'utente che hai creato l'accesso alla console di AWS gestione. Prima di poter accedere al portale di AWS accesso, è necessario accettare l'invito a iscriversi a IAM Identity Center e attivare le credenziali utente.

1. Controlla la tua email per l'oggetto Invito a iscriverti a AWS IAM Identity Center.
2. Scegli Accetta invito e segui le istruzioni sulla pagina di registrazione per impostare una nuova password, accedere e registrare un dispositivo MFA per il tuo utente.
3. Dopo aver registrato il dispositivo MFA, si apre il portale di AWS accesso. Quando le applicazioni saranno disponibili, le troverai nella scheda Applicazioni.

 Note

AWS le applicazioni che supportano le istanze di account consentono agli utenti di accedere alle applicazioni senza richiedere autorizzazioni aggiuntive. Pertanto, la scheda Account rimarrà vuota.

Passaggio 4. Configura l'applicazione AWS gestita per utilizzare IAM Identity Center

1. Dopo aver effettuato l'accesso alla console di AWS gestione, apri la console per l'applicazione AWS gestita che intendi utilizzare.
2. Segui le indicazioni nella console per configurare l'applicazione AWS gestita per utilizzare IAM Identity Center. Durante questo processo, puoi assegnare l'utente che hai creato all'applicazione.

Visualizzazione e modifica dei dettagli di un'applicazione AWS gestita

Dopo aver connesso un'applicazione AWS gestita a IAM Identity Center utilizzando la console o APIs per l'applicazione, l'applicazione viene registrata con IAM Identity Center. Dopo aver registrato un'applicazione con IAM Identity Center, puoi visualizzare e modificare i dettagli dell'applicazione nella console IAM Identity Center.

Le informazioni sull'applicazione includono se sono richieste 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. [Panoramica sulla propagazione delle identità affidabili](#)

Per visualizzare e modificare le informazioni su un'applicazione AWS gestita nella console IAM Identity Center

1. Apri la [console Centro identità IAM](#).
2. Selezionare Applications (Applicazioni).
3. Scegli la scheda AWS gestita.
4. Scegli il link per l'applicazione gestita che desideri aprire e visualizzare.
5. Se desideri modificare le informazioni su un'applicazione AWS gestita, scegli Azione, quindi scegli Modifica dettagli.

6. È possibile modificare il nome visualizzato, la descrizione dell'applicazione e il metodo di assegnazione di utenti e gruppi.
 - a. Per modificare il nome visualizzato, immettete il nome desiderato nel campo Nome visualizzato e scegliete Salva modifiche.
 - b. Per modificare la descrizione, inserisci la descrizione desiderata nel campo Descrizione e scegli Salva modifiche.
 - c. Per modificare il metodo di assegnazione di utenti e gruppi, apporta la modifica desiderata e scegli Salva modifiche. Per ulteriori informazioni, consulta [the section called “Utenti, gruppi e provisioning”](#).

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.

Per disabilitare un' AWS applicazione gestita

1. Apri la [console Centro identità IAM](#).
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 Disattiva applicazione, scegliete Disabilita.
6. Nell'elenco delle applicazioni AWS gestite, lo stato dell'applicazione appare come Inattivo.

Note

Se un'applicazione AWS gestita è disabilitata, è possibile ripristinare la capacità degli utenti di autenticarsi nell'applicazione scegliendo Azioni e quindi Abilita.

Attivazione di sessioni di console con identità migliorata

Una sessione con identità avanzata 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 Kiro Pro di Kiro su app e siti Web. AWS](#)

Puoi abilitare sessioni di console con identità migliorata senza apportare modifiche ai modelli di accesso o alla federazione esistenti nella console. AWS 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](#)
- [Come abilitare le sessioni identity-enhanced-console](#)
- [Come funzionano le sessioni di console con identità migliorata](#)

Prerequisiti e considerazioni

Prima di abilitare le sessioni della console con identità migliorata, esamina i seguenti prerequisiti e considerazioni:

- Se i tuoi utenti accedono a Kiro da AWS app e siti Web tramite un abbonamento a Kiro Pro, devi abilitare le sessioni di console con identità migliorata.

Note

Gli utenti Kiro possono accedere a Kiro senza sessioni con identità avanzata, ma non avranno accesso ai loro abbonamenti Kiro Pro.

- [Le sessioni di console con identità migliorata richiedono un'istanza organizzativa di IAM Identity Center.](#)
- L'integrazione con Kiro non è supportata se abiliti IAM Identity Center in un opt-in. Regione AWS
- Per abilitare le sessioni di console con identità migliorata, devi disporre delle seguenti autorizzazioni:
 - `sso:CreateApplication`

- `sso:GetSharedSsoConfiguration`
- `sso:ListApplications`
- `sso:PutApplicationAssignmentConfiguration`
- `sso:PutApplicationAuthenticationMethod`
- `sso:PutApplicationGrant`
- `sso:PutApplicationAccessScope`
- `signin:CreateTrustedIdentityPropagationApplicationForConsole`
- `signin:ListTrustedIdentityPropagationApplicationsForConsole`
- Per consentire agli utenti di utilizzare sessioni di console con identità avanzata, è necessario concedere loro l'autorizzazione in una politica basata sull'identità. `sts:setContext` Per informazioni, consulta [Concessione agli utenti delle autorizzazioni](#) per l'utilizzo di sessioni di console con identità avanzata.

Come abilitare le sessioni identity-enhanced-console

Puoi abilitare sessioni di console con identità migliorata nella console Kiro o nella console IAM Identity Center.

Abilita sessioni di console con identità migliorata nella console Kiro

Prima di abilitare le sessioni di console con identità avanzata, 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 Centro identità IAM. Scegli Enable e crea un'istanza organizzativa di IAM Identity Center. Per informazioni, consulta [Abilita IAM Identity Center](#).
2. Connetti la tua fonte di identità a IAM Identity Center e fornisci agli utenti IAM Identity Center. Puoi connettere la tua fonte di identità esistente a IAM Identity Center o utilizzare la directory Identity Center se non stai già utilizzando un'altra fonte di identità. Per ulteriori informazioni, consulta [Tutorial sulle fonti di identità di IAM Identity Center](#).
3. Dopo aver completato la configurazione di IAM Identity Center, apri la console Kiro e segui i passaggi in [Abbonamenti nella Guida](#) per l'utente di Kiro. Assicurati di abilitare le sessioni di console con identità migliorata.

 Note

Se non disponi di autorizzazioni sufficienti per abilitare le sessioni di console con identità avanzata, 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 sessioni di console con identità migliorata 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 identità migliorata nella console IAM Identity Center.

1. Apri la console Centro identità IAM.
2. Nel pannello di navigazione scegli Impostazioni.
3. In Abilita sessioni con identità migliorata, scegli Abilita.
4. Nel secondo messaggio, scegli Abilita.
5. Dopo aver abilitato le sessioni della console con identità avanzata, viene visualizzato un messaggio di conferma nella parte superiore della pagina Impostazioni.
6. Nella sezione Dettagli, lo stato delle sessioni con identità avanzata è Abilitato.

Come funzionano le sessioni di console con identità migliorata

IAM Identity Center migliora la sessione corrente della console di un utente per includere l'ID utente IAM Identity Center attivo e l'ID di sessione IAM Identity Center.

Le sessioni di console con funzionalità di identità migliorate 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.

Applicazioni gestite dal cliente

IAM Identity Center funge da servizio di identità centrale per gli utenti e i gruppi della forza lavoro. 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. Con una singola connessione, IAM Identity Center rappresenta il tuo IdP di fronte a più utenti Servizi AWS e consente alle tue applicazioni OAuth 2.0 di richiedere l'accesso ai dati di questi servizi per conto dei tuoi utenti. Puoi anche utilizzare IAM Identity Center per assegnare ai tuoi utenti l'accesso alle applicazioni [SAML 2.0](#). Ciò include AWS servizi come Amazon Connect e AWS Client VPN, che si integrano con IAM Identity Center utilizzando esclusivamente SAML e sono quindi classificati come applicazioni gestite dai clienti.

- Se la tua applicazione supporta JSON Web Tokens (JWTs), puoi utilizzare la funzionalità di propagazione dell'identità affidabile di IAM Identity Center per consentire all'applicazione di richiedere l'accesso ai dati per conto dei tuoi utenti. Servizi AWS La propagazione affidabile delle identità si basa sul OAuth 2.0 Authorization Framework e include un'opzione per consentire alle applicazioni di scambiare token di identità provenienti da un server di autorizzazione OAuth 2.0 esterno con token emessi da IAM Identity Center e riconosciuti da. Servizi AWS Per ulteriori informazioni, consulta [Casi d'uso affidabili per la propagazione delle identità](#).
- Se la tua applicazione supporta SAML 2.0, puoi collegarla a un'[istanza organizzativa](#) di IAM Identity Center. Puoi utilizzare IAM Identity Center per assegnare l'accesso alla tua applicazione SAML 2.0.

 Note

Quando integri applicazioni gestite dal cliente con un'istanza IAM Identity Center che utilizza una [chiave KMS gestita dal cliente](#), verifica se l'applicazione richiama il servizio IAM Identity Center APIs per confermare se l'applicazione necessita delle autorizzazioni per le chiavi KMS. [Segui le linee guida per concedere le autorizzazioni chiave KMS ai flussi di lavoro personalizzati nelle politiche chiave KMS di base della Guida per l'utente di IAM Identity Center.](#)

Argomenti

- [Accesso Single Sign-On alle applicazioni SAML 2.0 e 2.0 OAuth](#)
- [Configurazione di applicazioni SAML 2.0 gestite dal cliente](#)

Accesso Single Sign-On alle applicazioni SAML 2.0 e 2.0 OAuth

IAM Identity Center ti consente di fornire ai tuoi utenti l'accesso Single Sign-On alle applicazioni SAML 2.0 o 2.0. OAuth I seguenti argomenti forniscono una panoramica di alto livello di SAML 2.0 e 2.0. OAuth

Argomenti

- [SAML 2.0](#)
- [OAuth 2.0](#)

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

 Note

IAM Identity Center non supporta la convalida delle firme delle richieste di autenticazione SAML in entrata dalle applicazioni SAML.

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 sovvenzioni 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 AWS Software Development Kit (). Kit di strumenti AWS SDKs 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. Consultate la documentazione Servizi AWS relativa alle differenze regionali.

OpenID Connect (OIDC) è un protocollo di autenticazione basato sul Framework 2.0. OAuth OIDC specifica come utilizzare 2.0 per l'autenticazione. OAuth Tramite il [servizio OIDC di IAM Identity Center APIs](#), un'applicazione registra un client OAuth 2.0 e utilizza uno di questi flussi per ottenere un token di accesso che fornisce le autorizzazioni protette a IAM Identity Center. APIs 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 OAuth sovvenzioni 2.0

OAuth I flussi di sovvenzioni 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 Regione AWS soluzione. Consulta la documentazione relativa Servizio AWS a ciascuna di esse 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 conatterà e registrarsi con l'istanza di IAM Identity Center. A seconda dell'applicazione, in qualità di amministratore, devi fornire agli 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.

Note

Se hai clienti che lo utilizzano `device.sso.region.amazonaws.com`, devi aggiornare il flusso di autorizzazione per utilizzare Proof Key for Code Exchange (PKCE). Per ulteriori informazioni, consulta [Configurazione dell'autenticazione di IAM Identity Center con la Guida AWS CLI](#) per l'AWS Command Line Interface utente.

1. Quando il flusso inizia da un dispositivo con un 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 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 2.0 possono richiedere. OAuth Quando un client OAuth 2.0 si registra con il [servizio IAM Identity Center OIDC](#), specifica gli ambiti per dichiarare le azioni previste, per le quali l'utente deve fornire il consenso.

OAuth I client 2.0 utilizzano scope i 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

Scope	Description	Servizi supportati da
<code>sso:account:access</code>	Accedi agli account e ai set di autorizzazioni gestiti da IAM Identity Center.	Centro identità IAM
<code>codewhisperer:analysis</code>	Abilita l'accesso all'analisi del codice Kiro.	ID Builder AWS e IAM Identity Center
<code>codewhisperer:completions</code>	Abilita l'accesso ai suggerimenti di codice in linea di Kiro.	ID Builder AWS e IAM Identity Center
<code>codewhisperer:conversations</code>	Abilita l'accesso alla chat di Kiro.	ID Builder AWS e IAM Identity Center
<code>codewhisperer:taskassist</code>	Abilita l'accesso a Kiro Agent per lo sviluppo del software.	ID Builder AWS e IAM Identity Center
<code>codewhisperer:transformations</code>	Abilita l'accesso a Kiro Agent per la trasformazione del codice.	ID Builder AWS e IAM Identity Center
<code>codecatalyst:read_write</code>	Leggi e scrivi sulle tue CodeCatalyst risorse Amazon, permettendo l'accesso a tutte le tue risorse esistenti.	ID Builder AWS e IAM Identity Center

Scope	Description	Servizi supportati da
<code>verified_access:application:connect</code>	Abilita Accesso verificato da AWS	Accesso verificato da AWS
<code>redshift:connect</code>	Connect ad Amazon Redshift	Amazon Redshift
<code>datazone:domain:access</code>	Accedi al tuo ruolo di esecuzione del DataZone dominio	Amazon DataZone
<code>nosqlworkbench:datamodeladviser</code>	Crea e leggi modelli di dati	NoSQL Workbench
<code>transform:read_write</code>	Abilita l'accesso a AWS Transform Agent per la trasformazione del codice	AWS Trasformazione

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 la OAuth versione 2.0 e gli utenti devono accedere da tali applicazioni Servizi AWS, 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. Servizi AWS

Argomenti

- [Configura un'applicazione dal catalogo di applicazioni IAM Identity Center](#)
- [Configura la tua applicazione SAML 2.0](#)

Configura un'applicazione dal 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.

Utilizza questa procedura per configurare una relazione di fiducia 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 Centro identità IAM](#).
2. Selezionare Applications (Applicazioni).
3. Scegli la scheda Gestione clienti.
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, inizia 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 [Comprendi 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. Seleziona 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 Centro identità IAM](#).
2. Selezionare Applications (Applicazioni).
3. Scegli la scheda Gestione clienti.
4. Scegli Aggiungi applicazione.
5. Nella pagina Seleziona tipo di applicazione, alla voce Preferenze di impostazione, scegli Applicazione da configurare presente.
6. In Tipo di applicazione, scegli SAML 2.0.
7. Scegli Next (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 [Comprendi 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. Seleziona Invia. Verrai indirizzato alla pagina dei dettagli dell'applicazione che hai appena aggiunto.

Panoramica sulla propagazione delle identità affidabili

La propagazione affidabile delle identità è una funzionalità di IAM Identity Center che consente agli amministratori di concedere autorizzazioni Servizi AWS in base agli attributi degli utenti, come le associazioni di gruppo. Con la propagazione affidabile delle identità, il contesto dell'identità viene aggiunto a un ruolo IAM per identificare l'utente che richiede l'accesso alle risorse. AWS Questo contesto viene propagato ad altri. Servizi AWS

Il contesto di identità comprende le informazioni che vengono Servizi AWS utilizzate per prendere decisioni di autorizzazione quando ricevono richieste di accesso. Queste informazioni includono metadati che identificano il richiedente (ad esempio, un utente IAM Identity Center), il Servizio AWS cui accesso è richiesto (ad esempio, Amazon Redshift) e l'ambito di accesso (ad esempio, accesso in sola lettura). La ricezione Servizio AWS utilizza questo contesto e tutte le autorizzazioni assegnate all'utente per autorizzare l'accesso alle sue risorse.

Vantaggi della propagazione affidabile delle identità

La propagazione affidabile delle identità consente agli amministratori di Servizi AWS concedere autorizzazioni a risorse, come i dati, utilizzando le identità aziendali della forza lavoro. Inoltre, possono verificare chi ha avuto accesso a quali dati consultando i registri di servizio o. AWS CloudTrail Se sei un amministratore di IAM Identity Center, altri Servizio AWS amministratori potrebbero chiederti di abilitare la propagazione affidabile delle identità.

Abilitare la propagazione affidabile delle identità

Il processo di abilitazione della propagazione delle identità attendibili prevede i due passaggi seguenti:

1. Abilita IAM Identity Center e connetti la tua fonte di identità esistente a IAM Identity Center: continuerai a gestire le identità della tua forza lavoro nella tua fonte di identità esistente; collegandola a IAM Identity Center si crea un riferimento alla tua forza lavoro che tutti, Servizi AWS nel tuo caso d'uso, possono condividere. È inoltre disponibile per i proprietari dei dati da utilizzare in casi d'uso futuri.
2. Connetti il Servizi AWS tuo caso d'uso a IAM Identity Center: l'amministratore di ciascuno Servizio AWS dei casi d'uso di Trusted Identity Propagation segue le indicazioni contenute nella rispettiva documentazione del servizio per connettere il servizio a IAM Identity Center.

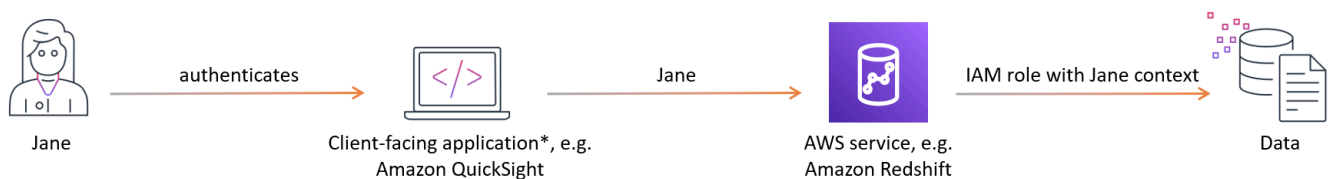
Note

Se il tuo caso d'uso riguarda un'applicazione sviluppata da terze parti o da un cliente, abilita la propagazione dell'identità affidabile configurando una relazione di fiducia tra il provider di identità che autentica gli utenti dell'applicazione e IAM Identity Center. Ciò consente all'applicazione di sfruttare il flusso di propagazione delle identità affidabili descritto in precedenza.

Per ulteriori informazioni, consulta [Utilizzo di applicazioni con un emittente di token affidabile](#).

Come funziona la propagazione delle identità attendibili

Il diagramma seguente mostra il flusso di lavoro di alto livello per la propagazione delle identità affidabili:



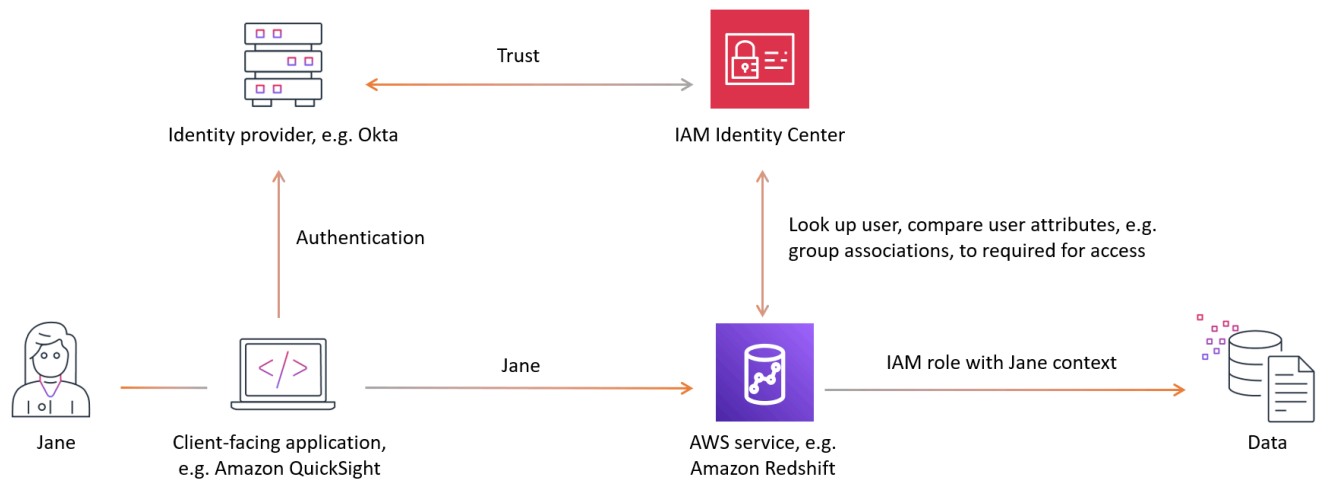
1. Gli utenti si autenticano con un'applicazione rivolta al client, ad esempio Quick.
2. L'applicazione rivolta al client richiede l'accesso per utilizzare e interrogare Servizio AWS i dati e include informazioni sull'utente.

Note

Alcuni casi d'uso affidabili di propagazione delle identità riguardano strumenti che interagiscono con i Servizi AWS utilizzando driver di servizio. Puoi scoprire se ciò si applica al tuo caso d'uso nella [guida ai casi d'uso](#).

3. Servizio AWS Verifica l'identità dell'utente con IAM Identity Center e confronta gli attributi degli utenti, come le loro associazioni di gruppo, con quelli richiesti per l'accesso. Servizio AWS Autorizza l'accesso purché l'utente o il suo gruppo disponga delle autorizzazioni necessarie.
4. Servizi AWS possono registrare l'identificatore utente nei propri registri AWS CloudTrail di servizio. Consulta la documentazione del servizio per i dettagli.

L'immagine seguente fornisce una panoramica dei passaggi descritti in precedenza nel flusso di lavoro di propagazione delle identità affidabili:



Argomenti

- [Prerequisiti e considerazioni](#)
- [Casi d'uso affidabili per la propagazione delle identità](#)
- [Servizi di autorizzazione](#)

Prerequisiti e considerazioni

Prima di configurare la propagazione delle identità affidabili, esamina i prerequisiti e le considerazioni seguenti.

Argomenti

- [Prerequisiti](#)
- [Considerazioni](#)
- [Considerazioni per le applicazioni gestite dai clienti](#)

Prerequisiti

Per utilizzare la propagazione affidabile delle identità, assicuratevi che l'ambiente soddisfi i seguenti prerequisiti:

- Abilita e fornisci IAM Identity Center

- Per utilizzare la propagazione affidabile delle identità, devi abilitare IAM Identity Center nella stessa area in Regione AWS cui sono abilitate le AWS applicazioni e i servizi a cui gli utenti accederanno. Per informazioni, consulta [Abilita IAM Identity Center](#).
- È consigliata un'istanza organizzativa di IAM Identity Center: ti consigliamo di utilizzare un'[istanza organizzativa](#) di IAM Identity Center da abilitare nell'account di gestione di AWS Organizations. Puoi [delegare l'amministrazione](#) di un'istanza organizzativa di IAM Identity Center a un account membro. Se scegli un'[istanza di account](#) di IAM Identity Center, tutto ciò a cui desideri Servizi AWS che gli utenti accedano con una propagazione dell'identità affidabile deve risiedere nello stesso in Account AWS cui abiliti IAM Identity Center. Per ulteriori informazioni, consulta [Istanze account del Centro identità IAM](#).
- Connetti il tuo provider di identità esistente a IAM Identity Center e fornisci utenti e gruppi a IAM Identity Center. Per ulteriori informazioni, consulta [Tutorial sulle fonti di identità di IAM Identity Center](#).
- Connetti le applicazioni e i servizi AWS gestiti nel tuo use case di propagazione dell'identità affidabile a IAM Identity Center. Per utilizzare la propagazione affidabile delle identità, le applicazioni AWS gestite devono essere connesse a IAM Identity Center.

Considerazioni

Tieni presente le seguenti considerazioni durante la configurazione e l'utilizzo della propagazione affidabile delle identità:

- Istanza tra organizzazione e account di IAM Identity Center
 - Un'[istanza organizzativa](#) di IAM Identity Center ti offrirà il massimo controllo e flessibilità per estendere i tuoi casi d'uso a più Account AWS utenti e Servizi AWS... Se non sei in grado di utilizzare un'istanza organizzativa, il tuo caso d'uso potrebbe essere supportato dalle istanze di account di IAM Identity Center. Per ulteriori informazioni su quali istanze di account di IAM Identity Center supportano Servizi AWS nel tuo caso d'uso, consulta. [AWS applicazioni gestite che è possibile utilizzare con IAM Identity Center](#)
- 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.

Considerazioni per le applicazioni gestite dai clienti

La vostra forza lavoro può trarre vantaggio dalla propagazione affidabile delle identità anche se gli utenti interagiscono con applicazioni rivolte ai clienti che non sono gestite, ad esempio AWS Tableau, da applicazioni sviluppate su misura. È possibile che agli utenti di queste applicazioni non venga eseguito il provisioning in IAM Identity Center. Per consentire il riconoscimento e l'autorizzazione senza problemi dell'accesso degli utenti alle AWS risorse, IAM Identity Center consente di configurare una relazione di fiducia tra il provider di identità che autentica gli utenti e IAM Identity Center. Per ulteriori informazioni, consulta [Utilizzo di applicazioni con un emittente di token affidabile](#).

Inoltre, la configurazione della propagazione affidabile dell'identità per l'applicazione richiederà:

- L'applicazione deve utilizzare il framework OAuth 2.0 per l'autenticazione. La propagazione affidabile delle identità non supporta le integrazioni SAML 2.0.
- L'applicazione deve essere riconosciuta da IAM Identity Center. Segui le linee guida specifiche per il tuo [caso d'uso](#).

Casi d'uso affidabili per la propagazione delle identità

In qualità di amministratore di IAM Identity Center, ti potrebbe essere chiesto di aiutarti a configurare la propagazione delle identità affidabili dalle applicazioni rivolte agli utenti verso. Servizi AWS Per supportare questa richiesta, avrai bisogno delle seguenti informazioni:

- Con quale applicazione rivolta ai clienti si interfaccieranno i tuoi utenti?
- Quali Servizi AWS vengono utilizzati per interrogare i dati e autorizzare l'accesso ai dati?
- Cosa Servizio AWS autorizza l'accesso ai dati?

Il vostro ruolo nell'abilitare casi d'uso affidabili di propagazione delle identità che non coinvolgono applicazioni di terze parti o applicazioni sviluppate su misura consiste nel:

1. [Abilita IAM Identity Center](#).
2. [Connect la tua fonte di identità esistente a IAM Identity Center](#).

I passaggi rimanenti della configurazione dell'identità affidabile per questi casi d'uso vengono eseguiti all'interno delle applicazioni Servizi AWS connesse e. Gli amministratori delle applicazioni connesse Servizi AWS o connesse devono fare riferimento alle rispettive guide per l'utente per una guida completa specifica sul servizio.

Il vostro ruolo nell'abilitare casi d'uso affidabili di propagazione delle identità che coinvolgono applicazioni di terze parti o applicazioni sviluppate su misura include le fasi di [connessione della fonte delle identità](#), [Abilita IAM Identity Center](#) nonché:

1. Configurazione della connessione del tuo provider di identità (IdP) all'applicazione di terze parti o sviluppata su misura.
2. Consentire a IAM Identity Center di riconoscere l'applicazione di terze parti o sviluppata su misura.
3. Configurazione del tuo IdP come emittente di token affidabile in IAM Identity Center. Per ulteriori informazioni, consulta [Utilizzo di applicazioni con un emittente di token affidabile](#).

Gli amministratori delle applicazioni connesse Servizi AWS devono fare riferimento alle rispettive guide per l'utente per una guida completa specifica sul servizio.

Casi d'uso di analisi, data lakehouse e machine learning

Puoi abilitare casi d'uso affidabili di propagazione con i seguenti servizi di analisi e apprendimento automatico:

- Amazon Redshift: per indicazioni, consulta. [Propagazione affidabile delle identità con Amazon Redshift](#)
- Amazon EMR: per indicazioni, consulta. [Propagazione affidabile delle identità con Amazon EMR](#)
- Amazon Athena: per indicazioni, consulta. [Propagazione affidabile delle identità con Amazon Athena](#)
- SageMaker Studio: per ulteriori informazioni, consulta [Propagazione affidabile delle identità con Amazon Studio SageMaker](#).

Casi d'uso aggiuntivi

Puoi abilitare IAM Identity Center e la propagazione delle identità affidabili con questi elementi aggiuntivi Servizi AWS:

- Amazon Q Business: per indicazioni, consulta:
 - [Flusso di lavoro di amministrazione per le app che utilizzano IAM Identity Center](#).
 - [Configurazione di un'applicazione Amazon Q Business utilizzando IAM Identity Center](#).
 - [Configura Amazon Q Business con la propagazione delle identità affidabile di IAM Identity Center](#).

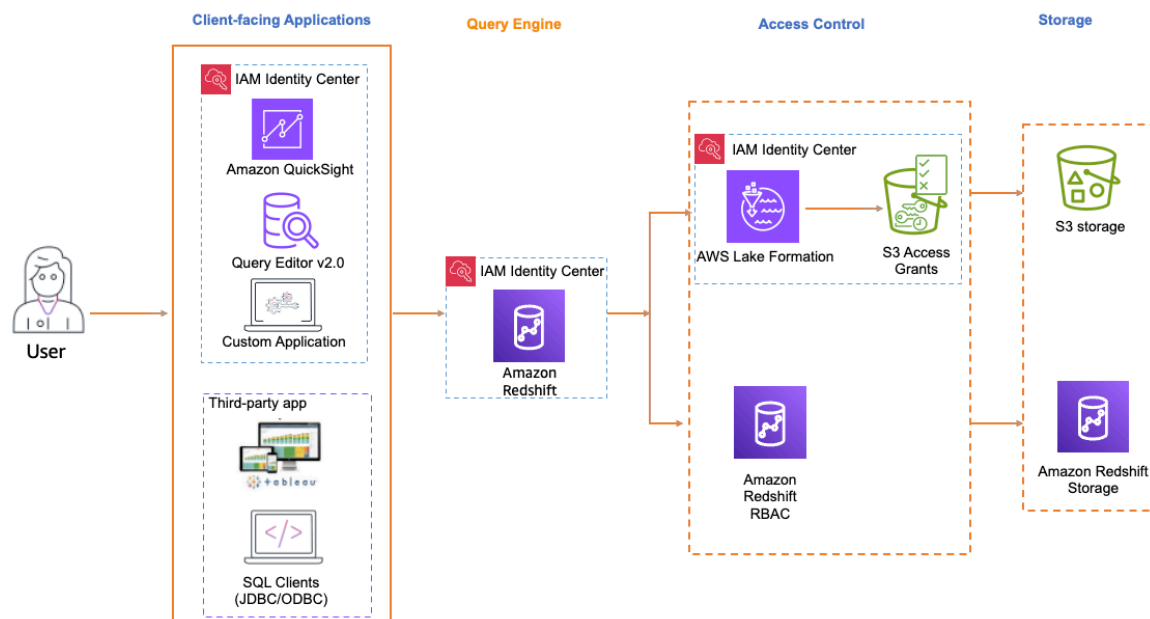
- Amazon OpenSearch Service: per informazioni, consulta:
 - [IAM Identity Center Trusted Identity Propagation Support per Amazon OpenSearch Service](#).
 - [Interfaccia OpenSearch utente centralizzata \(dashboard\) con Amazon OpenSearch Service](#).
- AWS Transfer Family- per informazioni, consulta:
 - [App web Transfer Family](#).

Argomenti

- [Propagazione affidabile delle identità con Amazon Redshift](#)
- [Propagazione affidabile delle identità con Amazon EMR](#)
- [Propagazione affidabile delle identità con Amazon Athena](#)
- [Propagazione affidabile delle identità con Amazon Studio SageMaker](#)

Propagazione affidabile delle identità con Amazon Redshift

I passaggi per abilitare la propagazione affidabile delle identità dipendono dal fatto che gli utenti interagiscano con applicazioni gestite o con applicazioni AWS gestite dai clienti. Il diagramma seguente mostra una configurazione affidabile di propagazione delle identità per applicazioni rivolte ai AWS client, AWS gestite o esterne, che interrogano i dati di Amazon Redshift con il controllo degli accessi fornito da Amazon Redshift o da servizi di autorizzazione, come Amazon S3. AWS Lake Formation Access Grants



Quando la propagazione affidabile delle identità su Amazon Redshift è abilitata, gli amministratori di Redshift possono configurare Redshift per creare automaticamente ruoli per IAM Identity Center come provider di identità, mappare i ruoli Redshift ai gruppi in IAM Identity Center e utilizzare il controllo degli accessi basato sui ruoli di Redshift per concedere l'accesso.

Applicazioni supportate rivolte ai clienti

AWS applicazioni gestite

Le seguenti applicazioni AWS gestite rivolte ai client supportano la propagazione affidabile delle identità su Amazon Redshift:

- [Amazon Redshift Query Editor V2](#)
- [Rapido](#)

 Note

Se utilizzi Amazon Redshift Spectrum per accedere a database o tabelle esterni, prendi AWS Glue Data Catalog in considerazione la possibilità di [configurare Lake Formation e Access Grants Amazon S3](#) per fornire un controllo granulare degli accessi.

Applicazioni gestite dai clienti

Le seguenti applicazioni gestite dai clienti supportano la propagazione affidabile delle identità su Amazon Redshift:

- Tableau tra cui Tableau Desktop, e Tableau Server Tableau Prep
 - Per abilitare la propagazione affidabile delle identità per gli utenti di Tableau, consulta [Integrate Tableau and Okta with Amazon Redshift using IAM Identity Center AWS](#) nel Big Data Blog.
- Client SQL (e) DBeaver DBVisualizer
 - Per abilitare la propagazione affidabile delle identità per gli utenti di SQL Client (DBeaver and DBVisualizer), consulta [Integrate Identity Provider \(IdP\) con Amazon Redshift Query Editor V2 e SQL Client utilizzando IAM Identity Center per un Single Sign-On senza interruzioni](#) nel Big Data Blog. AWS

Configurazione della propagazione affidabile delle identità con Amazon Redshift Query Editor V2

La procedura seguente illustra come ottenere una propagazione affidabile delle identità da Amazon Redshift Query Editor V2 ad Amazon Redshift.

Prerequisiti

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

1. [Abilita IAM Identity Center](#). [L'istanza dell'organizzazione](#) è consigliata. Per ulteriori informazioni, consulta [Prerequisiti e considerazioni](#).
2. Effettua [il provisioning di utenti e gruppi dalla tua fonte di identità a IAM Identity Center](#).

L'abilitazione della propagazione affidabile delle identità include le attività eseguite da un amministratore IAM Identity Center nella console IAM Identity Center e le attività eseguite da un amministratore Amazon Redshift nella console Amazon Redshift.

Attività eseguite dall'amministratore di IAM Identity Center

L'amministratore di IAM Identity Center doveva completare le seguenti attività:

1. Crea un [ruolo IAM](#) nell'account in cui esiste il cluster Amazon Redshift o l'istanza Serverless con la seguente politica di autorizzazione. Per ulteriori informazioni, consulta la sezione Creazione di [ruoli IAM](#).
 - I seguenti esempi di policy includono le autorizzazioni necessarie per completare questo tutorial. Per utilizzare questa politica, sostituisci la *italicized placeholder text* politica dell'esempio con le tue informazioni. Per ulteriori indicazioni, consulta [Creare un criterio](#) o [Modificare un criterio](#).

Politica di autorizzazione:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRedshiftApplication",
      "Effect": "Allow",
```

```

        "Action": [
            "redshift:DescribeQev2IdcApplications",
            "redshift-serverless:ListNamespaces",
            "redshift-serverless:ListWorkgroups",
            "redshift-serverless:GetWorkgroup"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AllowIDCPermissions",
        "Effect": "Allow",
        "Action": [
            "sso:DescribeApplication",
            "sso:DescribeInstance"
        ],
        "Resource": [
            "arn:aws:sso:::instance/Your-IAM-Identity-Center-Instance
ID",
            "arn:aws:sso:::111122223333:application/Your-IAM-Identity-
Center-Instance-ID/*"
        ]
    }
]
}

```

Politica di fiducia:

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "redshift-serverless.amazonaws.com",
                    "redshift.amazonaws.com"
                ]
            },
            "Action": [

```

```

        "sts:AssumeRole",
        "sts:SetContext"
    ]
}

```

2. Crea un set di autorizzazioni nell'account di AWS Organizations gestione in cui è abilitato IAM Identity Center. Lo utilizzerai nel passaggio successivo per consentire agli utenti federati di accedere a Redshift Query Editor V2.
 - a. Vai alla console IAM Identity Center, in Autorizzazioni multi-account, scegli Set di autorizzazioni.
 - b. Scegli Create permission set (Crea set di autorizzazioni).
 - c. Scegli Set di autorizzazioni personalizzato, quindi scegli Avanti.
 - d. In Politiche AWS gestite, scegli **AmazonRedshiftQueryEditorV2ReadSharing**.
 - e. In Politica in linea, aggiungi la seguente politica:

JSON

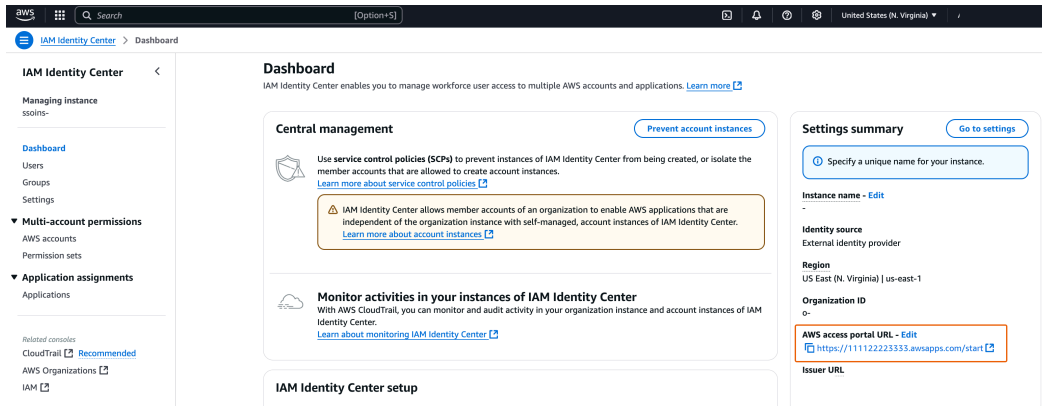
```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeQev2IdcApplications",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource": "*"
    }
  ]
}

```

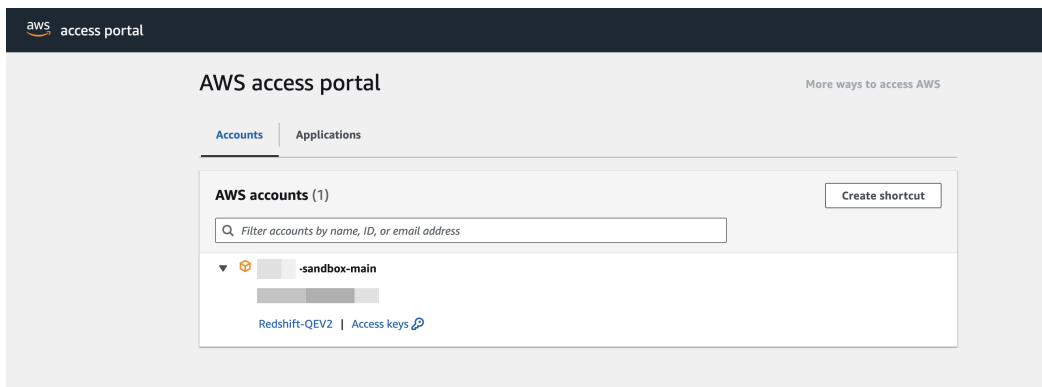
- f. Seleziona Avanti e quindi fornisci un nome per il nome del set di autorizzazioni. Ad esempio, **Redshift-Query-Editor-V2**.

- g. In Relay state, facoltativo, imposta lo stato di inoltro predefinito sull'URL di Query Editor V2, utilizzando il formato: `https://your-region.console.aws.amazon.com/sqlworkbench/home`
- h. Controlla le impostazioni e scegli Crea.
- i. Vai alla dashboard di IAM Identity Center e copia l'URL del portale di AWS accesso dalla sezione Riepilogo delle impostazioni.



- j. Apri una nuova finestra del browser in incognito e incolla l'URL.

Verrai reindirizzato al tuo portale di AWS accesso, assicurandoti di accedere con un utente IAM Identity Center.



Per ulteriori informazioni sul set di autorizzazioni, consulta [Gestisci Account AWS con set di autorizzazioni](#).

3. Consenti agli utenti federati di accedere a Redshift Query Editor V2.
 - a. Nell'account di AWS Organizations gestione, apri la console IAM Identity Center.
 - b. Nel pannello di navigazione, in Autorizzazioni multiaccount, scegli. Account AWS
 - c. Nella Account AWS pagina, seleziona l'accesso a Account AWS cui desideri assegnare l'accesso.

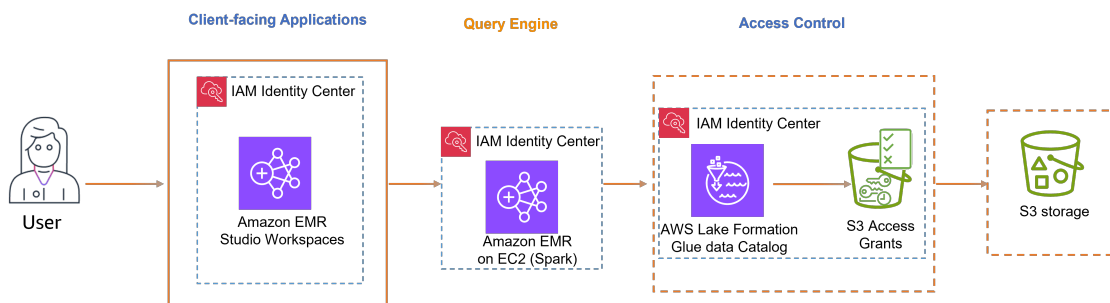
- d. Scegli Assegna utenti o gruppi.
- e. Nella pagina Assegna utenti e gruppi, scegli gli utenti e/o i gruppi per cui desideri creare il set di autorizzazioni. Quindi, seleziona Successivo.
- f. Nella pagina Assegna set di autorizzazioni, scegli il set di autorizzazioni creato nel passaggio precedente. Quindi, seleziona Successivo.
- g. Nella pagina Rivedi e invia le assegnazioni, rivedi le selezioni e scegli Invia.

Attività eseguite da un amministratore di Amazon Redshift

Per abilitare la propagazione affidabile delle identità su Amazon Redshift è necessario che un amministratore del cluster Amazon Redshift o un amministratore di Amazon Redshift Serverless esegua una serie di attività nella console Amazon Redshift. Per ulteriori informazioni, consulta [Integrare Identity Provider \(IdP\) con Amazon Redshift Query Editor V2 e SQL Client utilizzando IAM Identity Center per un Single Sign-On senza interruzioni](#) nel Big Data Blog.AWS

Propagazione affidabile delle identità con Amazon EMR

Il diagramma seguente mostra una configurazione di propagazione delle identità affidabile per Amazon EMR Studio che utilizza Amazon EMR su Amazon EC2 con controllo degli accessi fornito da Amazon S3. AWS Lake Formation Access Grants



Applicazioni rivolte ai clienti supportate

- Amazon EMR Studio

Per abilitare la propagazione affidabile delle identità, segui questi passaggi:

- [Configura Amazon EMR Studio](#) come applicazione rivolta ai client per il cluster Amazon EMR.
- Configura [Amazon EMR Cluster su Amazon EC2](#) con. Apache Spark

- Consigliato: [AWS Lake Formation Amazon S3 Access Grants](#) per fornire un controllo granulare degli accessi alle posizioni dei dati sottostanti in S3 AWS Glue Data Catalog e alle relative ubicazioni.

Configurazione della propagazione affidabile delle identità con Amazon EMR Studio

La procedura seguente illustra come configurare Amazon EMR Studio per la propagazione di identità affidabili nelle query su gruppi di lavoro Amazon Athena o cluster Amazon EMR in esecuzione.

Apache Spark

Prerequisiti

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

1. [Abilita IAM Identity Center](#). [L'istanza dell'organizzazione](#) è consigliata. Per ulteriori informazioni, consulta [Prerequisiti e considerazioni](#).
2. Effettua [il provisioning di utenti e gruppi dalla tua fonte di identità a IAM Identity Center](#).

Per completare la configurazione della propagazione delle identità affidabili da Amazon EMR Studio, l'amministratore di EMR Studio deve eseguire i seguenti passaggi.

Passaggio 1. Creare i ruoli IAM richiesti per EMR Studio

In questa fase, l'Studioamministratore di Amazon EMR crea un ruolo di servizio IAM e un ruolo utente IAM per EMR. Studio

1. [Crea un ruolo di servizio EMR Studio: EMR Studio assume questo ruolo](#) IAM per gestire in sicurezza aree di lavoro e notebook, connettersi ai cluster e gestire le interazioni con i dati.
 - a. Passa alla console IAM () e crea un ruolo IAM. <https://console.aws.amazon.com/iam/>
 - b. Seleziona Servizio AWS come entità affidabile, quindi scegli Amazon EMR. Allega le seguenti politiche per definire le autorizzazioni e la relazione di fiducia del ruolo.

Per utilizzare queste politiche, sostituisci la *italicized placeholder text* politica dell'esempio con le tue informazioni. Per ulteriori indicazioni, consulta [Creare un criterio](#) o [Modificare un criterio](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectActions",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "Your-AWS-Account-ID"
        }
      }
    },
    {
      "Sid": "BucketActions",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetEncryptionConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "Your-AWS-Account-ID"
        }
      }
    }
  ]
}
```

Per un riferimento di tutte le autorizzazioni dei ruoli di servizio, vedere Autorizzazioni dei ruoli di [servizio EMR Studio](#).

2. [Crea un ruolo utente EMR Studio per l'autenticazione di IAM Identity Center](#): EMR Studio assume questo ruolo quando un utente accede tramite IAM Identity Center per gestire aree di lavoro, cluster EMR, job, repository git. Questo ruolo viene utilizzato per avviare il flusso di lavoro di propagazione delle identità affidabili.

Note

Il ruolo utente di EMR Studio non deve includere le autorizzazioni per accedere alle posizioni Amazon S3 delle tabelle in Catalog. AWS Glue AWS Lake Formation le autorizzazioni e le località lacustri registrate verranno utilizzate per ricevere autorizzazioni temporanee.

La seguente policy di esempio può essere utilizzata in un ruolo che consente a un utente di EMR Studio di utilizzare i gruppi di lavoro Athena per eseguire query.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDefaultEC2SecurityGroupsCreationInVPCWithEMRTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-
policies": "true"
        }
      }
    }
  ]
}
```

```

    },
    {
      "Sid": "AllowAddingEMRTagsDuringDefaultSecurityGroupCreation",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:*:*:security-group/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true",
          "ec2:CreateAction": "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid": "AllowSecretManagerListSecrets",
      "Action": [
        "secretsmanager:ListSecrets"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Sid": "AllowSecretCreationWithEMRTagsAndEMRStudioPrefix",
      "Effect": "Allow",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true"
        }
      }
    },
    {
      "Sid": "AllowAddingTagsOnSecretsWithEMRStudioPrefix",
      "Effect": "Allow",
      "Action": "secretsmanager:TagResource",
      "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*"
    },
    {
      "Sid": "AllowPassingServiceRoleForWorkspaceCreation",

```

```

        "Action": "iam:PassRole",
        "Resource": [
            "arn:aws:iam::111122223333:role/service-
role/AmazonEMRStudio_ServiceRole_Name"
        ],
        "Effect": "Allow"
    },
    {
        "Sid": "AllowS3ListAndLocationPermissions",
        "Action": [
            "s3:ListAllMyBuckets",
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws:s3:::*",
        "Effect": "Allow"
    },
    {
        "Sid": "AllowS3ReadOnlyAccessToLogs",
        "Action": [
            "s3:GetObject"
        ],
        "Resource": [
            "arn:aws:s3:::aws-logs-Your-AWS-Account-ID-Region/
elasticmapreduce/*"
        ],
        "Effect": "Allow"
    },
    {
        "Sid": "AllowAthenaQueryExecutions",
        "Effect": "Allow",
        "Action": [
            "athena:StartQueryExecution",
            "athena:GetQueryExecution",
            "athena:GetQueryResults",
            "athena:StopQueryExecution",
            "athena:ListQueryExecutions",
            "athena:GetQueryResultsStream",
            "athena:ListWorkGroups",
            "athena:GetWorkGroup",
            "athena:CreatePreparedStatement",
            "athena:GetPreparedStatement",
            "athena>DeletePreparedStatement"
        ],

```

```

        "Resource": "*"
    },
    {
        "Sid": "AllowGlueSchemaManipulations",
        "Effect": "Allow",
        "Action": [
            "glue:GetDatabase",
            "glue:GetDatabases",
            "glue:GetTable",
            "glue:GetTables",
            "glue:GetPartition",
            "glue:GetPartitions"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AllowQueryEditorToAccessWorkGroup",
        "Effect": "Allow",
        "Action": "athena:GetWorkGroup",
        "Resource": "arn:aws:athena:*:111122223333:workgroup*"
    },
    {
        "Sid": "AllowConfigurationForWorkspaceCollaboration",
        "Action": [
            "elasticmapreduce:UpdateEditor",
            "elasticmapreduce:PutWorkspaceAccess",
            "elasticmapreduce>DeleteWorkspaceAccess",
            "elasticmapreduce:ListWorkspaceAccessIdentities"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Condition": {
            "StringEquals": {
                "elasticmapreduce:ResourceTag/creatorUserId":
"${aws:userId}"
            }
        }
    },
    {
        "Sid": "DescribeNetwork",
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeVpcs",
            "ec2:DescribeSubnets",

```

```
        "ec2:DescribeSecurityGroups"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ListIAMRoles",
      "Effect": "Allow",
      "Action": [
        "iam:ListRoles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AssumeRole",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": "*"
    }
  ]
}
```

La seguente politica di attendibilità consente a EMR Studio di assumere il ruolo:

 Note

Sono necessarie autorizzazioni aggiuntive per utilizzare EMR Studio Workspaces e EMR Notebooks. Per ulteriori informazioni, consulta [Creare politiche di autorizzazione per gli utenti di EMR Studio](#).

Puoi trovare ulteriori informazioni ai seguenti link:

- [Definisci le autorizzazioni IAM personalizzate con le policy gestite dal cliente](#)
- [Autorizzazioni per i ruoli di servizio EMR Studio](#)

Passaggio 2. Crea e configura il tuo EMR Studio

In questo passaggio, creerai un Amazon EMR Studio nella console EMR Studio e utilizzerai i ruoli IAM in cui hai creato. [Passaggio 1. Creare i ruoli IAM richiesti per EMR Studio](#)

1. Accedere alla console EMR Studio, selezionare Create Studio e l'opzione Configurazione personalizzata. Puoi creare un nuovo bucket S3 o utilizzare un bucket esistente. Puoi selezionare la casella per crittografare i file dell'area di lavoro con le tue chiavi KMS. Per ulteriori informazioni, consulta [AWS Key Management Service](#).

The screenshot shows the 'Create a Studio' page in the Amazon EMR console. The page is divided into several sections:

- Setup options:** Three radio buttons are visible: 'Interactive workloads', 'Batch jobs', and 'Custom' (which is selected).
- Studio settings:**
 - Studio name:** A text input field containing 'Studio_1'.
 - Description - optional:** A text area with the placeholder 'Describe the Studio'.
 - S3 location for Workspace storage:** A section with a heading 'Specify an Amazon S3 location where Workspace work will be saved.' and two radio buttons: 'Create new bucket' (selected) and 'Select existing location'.
 - Encrypt Workspace files with your own AWS KMS key:** A checkbox that is currently unchecked.

2. In Ruolo di servizio per consentire a Studio di accedere alle tue risorse, seleziona il ruolo di servizio creato in [Passaggio 1. Creare i ruoli IAM richiesti per EMR Studio](#) dal menu.
3. Scegli IAM Identity Center in Authentication. Seleziona il ruolo utente creato in [Passaggio 1. Creare i ruoli IAM richiesti per EMR Studio](#).

The screenshot shows the 'Create Studio' page in the Amazon EMR console, specifically the 'Authentication' section. The page is divided into several sections:

- Service role to let Studio access your AWS resources:** A dropdown menu showing 'AmazonEMRStudio'.
- Authentication:** A section with a heading 'Choose an authentication method for your Studio.' and two radio buttons: 'AWS Identity and Access Management (IAM)' and 'IAM Identity Center (AWS Single Sign-On)' (which is selected).
- User role:** A dropdown menu showing 'emrstudio-userrole-1dc'.
- Connect EMR Studio to IAM Identity Center:** A section with a heading 'Instance of IAM Identity Center' and a text input field containing 'arn:aws:sso::instance:ssoins-...'.

4. Seleziona la casella Trusted Identity Propagation. Scegli Solo utenti e gruppi assegnati nella sezione Accesso all'applicazione, che ti consentirà di concedere solo agli utenti e ai gruppi autorizzati l'accesso a questo studio.

5. (Facoltativo): puoi configurare VPC e sottorete se utilizzi questo Studio con cluster EMR.

Trusted identity propagation [Info](#)
Control and log the access that a user has across connected applications.

☒ **Enable trusted identity propagation**
When users make requests to applications that are connected through Identity Center, share their user identity information from EMR Studio. This setting applies for the lifetime of the Studio. You can't turn it off later.

The following features aren't supported from a Studio with trusted identity propagation: creating EMR on EC2 clusters without a template, using EMR Serverless applications, launching EMR on EKS clusters, using a runtime role, and enabling SQL Explorer or Workspace collaboration.

Application access [Info](#)
Choose who can access your application
Specify whether only assigned users and groups can access your application.

☒ **Only assigned users and groups**
Only the users and groups that you specify from your Identity Center directory can access this application.

☐ **All users and groups**
Any user or group from your IAM Identity Center directory can access this application.

▼ Networking and security - optional

VPC [Info](#)
Select a VPC for your Studio to use when it communicates with EMR clusters. To use condition keys like those in the example [service role policies for Amazon EMR](#), you must tag the VPC with the `for-use-with-amazon-emr-managed-policies` key and value `true`. To manage tags, use [VPC Dashboard](#).

Select a VPC

Subnets [Info](#)
Select the subnets that your Studio can use when it communicates with EMR clusters. To use condition keys like those in the example [service role policies for Amazon EMR](#), you must tag each subnet with the `for-use-with-amazon-emr-managed-policies` key and value `true`. To manage tags, use [VPC Dashboard](#).

6. Controlla tutti i dettagli e seleziona Create Studio.

7. Dopo aver configurato un cluster WorkGroup Athena o EMR, accedi all'URL dello Studio per:

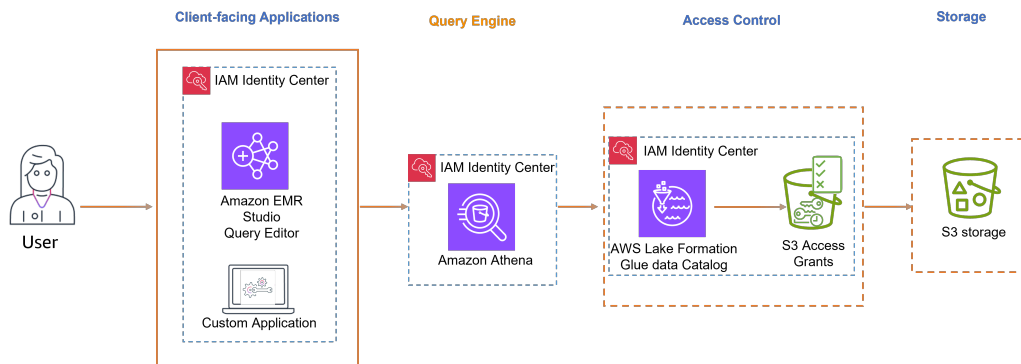
- a. Esegui le interrogazioni Athena con l'editor di query.
- b. Esegui i job Spark nell'area di lavoro usando notebook. Jupyter

Propagazione affidabile delle identità con Amazon Athena

I passaggi per abilitare la propagazione affidabile delle identità dipendono dal fatto che gli utenti interagiscano con applicazioni gestite o con applicazioni AWS gestite dai clienti. Il diagramma seguente mostra una configurazione di propagazione dell'identità affidabile per applicazioni rivolte ai client, AWS gestite o esterne, che utilizza Amazon Athena per AWS interrogare i dati di Amazon S3 con il controllo degli accessi fornito da Amazon S3. AWS Lake Formation Access Grants

Note

- La propagazione affidabile delle identità con Amazon Athena richiede l'uso di Trino.
- I client Apache Spark e SQL connessi ad Amazon Athena tramite driver ODBC e JDBC non sono supportati.



AWS applicazioni gestite

La seguente applicazione AWS gestita rivolta ai client supporta la propagazione affidabile delle identità con Athena:

- Amazon EMR Studio

Per abilitare la propagazione affidabile delle identità, segui questi passaggi:

- [Configura Amazon EMR Studio](#) come applicazione rivolta ai client per Athena. L'editor di query in EMR Studio è necessario per eseguire Athena Queries quando è abilitata la propagazione delle identità affidabili.
- [Configura Athena](#) Workgroup.
- [Configura AWS Lake Formation](#) per abilitare il controllo granulare degli accessi per le AWS Glue tabelle in base all'utente o al gruppo in IAM Identity Center.
- [Configura Amazon S3 Access Grants](#) per consentire l'accesso temporaneo alle posizioni dei dati sottostanti in S3.

Note

Sia Lake Formation che Amazon S3 Access Grants sono necessari per il controllo degli accessi ai AWS Glue Data Catalog e per i risultati delle query Athena in Amazon S3.

Applicazioni gestite dal cliente

Per abilitare la propagazione affidabile delle identità per gli utenti di applicazioni sviluppate su misura, consulta [Access Servizi AWS programmaticamente using trusted identity propagation](#) nel Security Blog.AWS

Configurazione della propagazione affidabile delle identità con i gruppi di lavoro Amazon Athena

La procedura seguente illustra come configurare i gruppi di lavoro Amazon Athena per la propagazione di identità affidabili.

Prerequisiti

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

1. [Abilita IAM Identity Center](#). [L'istanza dell'organizzazione](#) è consigliata. Per ulteriori informazioni, consulta [Prerequisiti e considerazioni](#).
2. Effettua [il provisioning di utenti e gruppi dalla tua fonte di identità a IAM Identity Center](#).
3. Questa configurazione richiede [Amazon EMR Studio](#) e [Amazon S3 AWS Lake Formation](#) Access Grants.

Configurazione della propagazione affidabile delle identità con Athena

Per configurare la propagazione delle identità affidabili con Athena, l'amministratore di Athena deve:

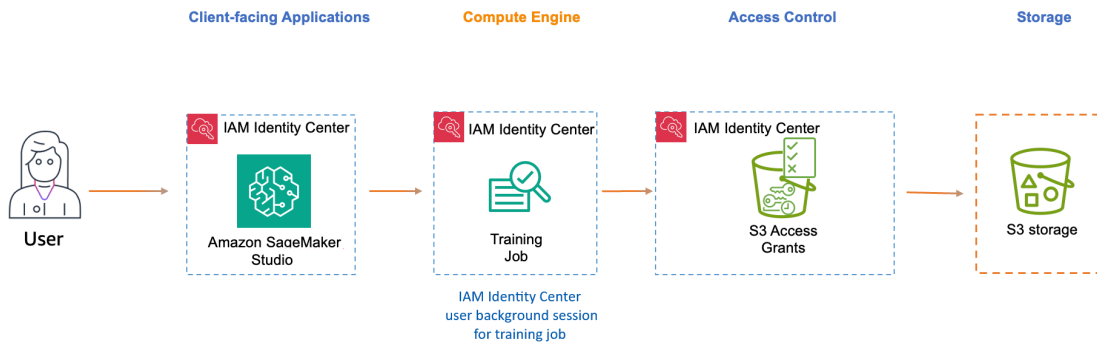
1. Esamina [le considerazioni e le limitazioni relative all'utilizzo dei gruppi di lavoro Athena abilitati per IAM Identity Center](#).
2. [Crea un gruppo di lavoro Athena abilitato per IAM Identity Center](#).

Propagazione affidabile delle identità con Amazon Studio SageMaker

[Amazon SageMaker Studio](#) si integra con IAM Identity Center e supporta [sessioni utente in background](#) e la propagazione affidabile delle identità. Le sessioni utente in background consentono a un utente di avviare un processo di lunga durata su SageMaker Studio, senza che l'utente debba rimanere connesso durante l'esecuzione del lavoro. Il processo viene eseguito immediatamente e in background, utilizzando le autorizzazioni dell'utente che ha avviato il processo. Il processo può continuare a essere eseguito anche se l'utente spegne il computer, la sessione di accesso a IAM Identity Center scade o l'utente si disconnette dal portale di accesso. AWS La durata predefinita della sessione per le sessioni utente in background è di 7 giorni, ma è possibile specificare una durata massima di 90 giorni. La propagazione affidabile delle identità consente di fornire un accesso

granulare a AWS risorse come i bucket Amazon S3 in base all'identità dell'utente o all'appartenenza al gruppo.

Il diagramma seguente mostra una configurazione di propagazione delle identità affidabile per SageMaker Studio, con accesso ai dati archiviati in un bucket Amazon S3. Le sessioni utente in background sono abilitate per IAM Identity Center, che consente l'esecuzione del processo di formazione di SageMaker Studio in background. Il controllo degli accessi per i dati di formazione è fornito da Amazon S3Access Grants.



AWS applicazione gestita

La seguente applicazione AWS gestita rivolta ai client supporta la propagazione affidabile delle identità:

- [Amazon SageMaker Studio](#)

Per abilitare la propagazione affidabile delle identità e le sessioni in background degli utenti, segui questi passaggi:

- [Configura SageMaker Studio come applicazione rivolta al client.](#)
- [Configura Amazon S3 Access Grants](#) per consentire l'accesso temporaneo alle posizioni dei dati sottostanti in Amazon S3.

Configurazione di una propagazione affidabile delle identità con Studio SageMaker

La procedura seguente illustra come configurare SageMaker Studio per la propagazione affidabile delle identità e le sessioni in background degli utenti.

Prerequisiti

Prima di iniziare con questo tutorial, dovrai completare le seguenti attività:

1. [Abilita IAM Identity Center](#). È richiesta un'istanza dell'organizzazione. Per ulteriori informazioni, consulta [Prerequisiti e considerazioni](#).
2. Effettua [il provisioning di utenti e gruppi dalla tua fonte di identità a IAM Identity Center](#).
3. [Verifica che le sessioni utente in background siano abilitate](#) nella console IAM Identity Center. Per impostazione predefinita, le sessioni utente in background sono abilitate e la durata della sessione è impostata su 7 giorni. È possibile modificare questa durata.

Per configurare la propagazione delle identità attendibili da SageMaker Studio, l'amministratore di SageMaker Studio deve eseguire le seguenti operazioni.

Passaggio 1: abilitare la propagazione delle identità affidabili in un dominio Studio nuovo o esistente SageMaker

SageMaker Studio utilizza i domini per organizzare i profili utente, le applicazioni e le risorse associate. Per abilitare la propagazione affidabile delle identità, è necessario creare un dominio SageMaker Studio o modificare un dominio esistente come descritto nella procedura seguente.

1. Apri la console SageMaker AI, vai a Domini ed esegui una delle seguenti operazioni.

- Crea un nuovo dominio SageMaker Studio utilizzando [Setup for organizations](#).

Scegliete Configura per le organizzazioni, quindi effettuate le seguenti operazioni:

- Scegli AWS Identity Center come metodo di autenticazione.
- Seleziona la casella di controllo Abilita la propagazione dell'identità affidabile per tutti gli utenti di questo dominio.
- Modifica un dominio SageMaker Studio esistente.
- Seleziona un dominio esistente che utilizza IAM Identity Center per l'autenticazione.

Important

La propagazione affidabile delle identità è supportata solo nei domini SageMaker Studio che utilizzano IAM Identity Center per l'autenticazione. Se il dominio utilizza

IAM per l'autenticazione, non è possibile modificare il metodo di autenticazione e quindi non è possibile abilitare la propagazione delle identità affidabili.

- [Modifica le impostazioni del dominio](#). Modifica le impostazioni di autenticazione e autorizzazioni per abilitare la propagazione delle identità affidabili.
2. Passare alla [Fase 2: Configurare il ruolo di esecuzione del dominio predefinito](#). Questo ruolo è necessario per gli utenti di un dominio SageMaker Studio per accedere ad altri AWS servizi come Amazon S3.

Passaggio 2: configura il ruolo di esecuzione del dominio e la politica di attendibilità dei ruoli predefiniti

Un ruolo di esecuzione del dominio è un [ruolo IAM](#) che un dominio SageMaker Studio assume per conto di tutti gli utenti del dominio. Le autorizzazioni assegnate a questo ruolo determinano le azioni che SageMaker Studio può eseguire.

1. Per creare o selezionare un ruolo di esecuzione del dominio, effettuate una delle seguenti operazioni:
 - Crea o seleziona un ruolo utilizzando [Configurazione per le organizzazioni](#).
 - Apri la console SageMaker AI e segui le istruzioni riportate nella fase 2: Configurazione dei ruoli e delle attività di machine learning per creare un nuovo ruolo di esecuzione del dominio o selezionare un ruolo esistente.
 - Completa il resto dei passaggi di configurazione per creare il tuo dominio SageMaker Studio.
 - Crea manualmente un ruolo di esecuzione.
 - Apri la console IAM e [crea tu stesso il ruolo di esecuzione](#).
2. [Aggiorna la policy di fiducia](#) allegata al ruolo di esecuzione del dominio in modo che includa le due azioni seguenti: [sts:AssumeRole](#) e [sts:SetContext](#). Per informazioni su come trovare il ruolo di esecuzione per il dominio SageMaker Studio, consulta [Get domain execution role](#).

Una politica di fiducia specifica l'identità che può assumere un ruolo. Questa politica è necessaria per consentire al servizio SageMaker Studio di assumere il ruolo di esecuzione del dominio. Aggiungi queste due azioni in modo che appaiano come segue nella tua politica.

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

```
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "Service": [
            "sagemaker.amazonaws.com"
          ]
        },
        "Action": [
          "sts:AssumeRole",
          "sts:SetContext"
        ]
      }
    ]
  }
}
```

Fase 3: verifica le autorizzazioni richieste di Amazon S3 Access Grant per il ruolo di esecuzione del dominio

Per utilizzare Amazon S3 Access Grants, devi avere una politica di autorizzazioni allegata (come policy in linea o come policy gestita dal cliente) al ruolo di esecuzione del dominio SageMaker Studio che contenga le seguenti autorizzazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
    }
  ]
}
```


Se non disponi di una policy che contenga queste autorizzazioni, segui le istruzioni in [Aggiungere e rimuovere le autorizzazioni di identità IAM](#) nella Guida per l'utente AWS Identity and Access Management

Passaggio 4: Assegna gruppi e utenti al dominio

Assegna gruppi e utenti al dominio SageMaker Studio seguendo la procedura descritta in [Aggiungere gruppi e utenti](#).

Fase 5: configurare Amazon S3 Access Grants

Per configurare Amazon S3 Access Grants, segui i passaggi descritti in Configurazione di [Amazon S3 Access Grants per la propagazione di identità affidabili tramite IAM](#) Identity Center. Utilizza le step-by-step istruzioni per completare le seguenti attività:

1. Crea un'istanza Amazon S3 Access Grants.
2. Registra una posizione in quell'istanza.
3. Crea sovvenzioni per consentire a utenti o gruppi specifici di IAM Identity Center di accedere a posizioni o sottoinsiemi di Amazon S3 designati (ad esempio, prefissi specifici) all'interno di tali sedi.

Fase 6: Invia un lavoro di SageMaker formazione e visualizza i dettagli della sessione in background dell'utente

In SageMaker Studio, avvia un nuovo notebook Jupyter e invia un lavoro di formazione. Mentre il processo è in esecuzione, completa i seguenti passaggi per visualizzare le informazioni sulla sessione e verificare che il contesto della sessione in background dell'utente sia attivo.

1. Apri la console Centro identità IAM.
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 per questo utente.
5. Per cercare le sessioni in base all'Amazon Resource Name (ARN) del processo che utilizza la sessione, nell'elenco Tipo di sessione, scegli Sessioni utente in background, quindi inserisci l'ARN del lavoro nella casella di ricerca.

Di seguito è riportato un esempio di come un processo di formazione che utilizza una sessione utente in background viene visualizzato nella scheda Sessioni attive per un utente.

Active sessions (5)

You can end any of the active sessions in this list. The list shows all active sessions initiated by [wei_zhang](#) [Learn more](#)

Find sessions by client or used by Session type: All

☐	Client	Session type	Used by	IP address
☐	-	User background se...	arn:aws:sagemaker:us-west-2:777788889999:training-job/trustedidprop-trjob-12345a6b	-

Passaggio 7: Visualizza CloudTrail i log per verificare la propagazione dell'identità affidabile in CloudTrail

Quando la propagazione delle identità attendibili è abilitata, le azioni vengono visualizzate nei registri CloudTrail degli eventi sotto l'elemento. `onBehalfOf` `userId` riflette l'ID dell'utente IAM Identity Center che ha avviato il processo di formazione. Il seguente CloudTrail evento cattura il processo di propagazione dell'identità affidabile.

```

      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AR0A123456789EXAMPLE:SageMaker",
        "arn": "arn:aws:sts::111122223333:assumed-role/SageMaker-
ExecutionRole-20250728T125817/SageMaker",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AR0A123456789EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/service-role/SageMaker-
ExecutionRole-20250728T125817",
            "accountId": "111122223333",
            "userName": "SageMaker-ExecutionRole-20250728T125817"
          },
          "attributes": {
            "creationDate": "2025-07-29T17:17:10Z",
            "mfaAuthenticated": "false"
          }
        },
        "onBehalfOf": {
          "userId": "2801d3e0-f0e1-707f-54e8-f558b19f0a10",

```

```
"identityStoreArn": "arn:aws:identitystore::777788889999:identitystore/d-1234567890"
  }
},
```

Considerazioni sul runtime

Se un amministratore imposta processi `MaxRuntimeInSeconds` di formazione o elaborazione di lunga durata inferiori alla durata della sessione utente in background, SageMaker Studio esegue il lavoro per la durata minima della sessione utente in background `MaxRuntimeInSeconds` o per la durata minima della sessione utente in background.

Per ulteriori informazioni in merito `MaxRuntimeInSeconds`, consulta la guida per il `CreateTrainingJob` [StoppingCondition](#) parametro nell'Amazon SageMaker API Reference.

Servizi di autorizzazione

In tutti i [casi d'uso di analisi e data lakehouse](#), puoi ottenere controlli granulari degli accessi utilizzando:

- AWS Lake Formation - per ulteriori informazioni, vedere. [Configurazione AWS Lake Formation con IAM Identity Center](#)
- Amazon S3Access Grants: per indicazioni, consulta. [Configurazione di Amazon S3 Access Grants con IAM Identity Center](#)

Configurazione AWS Lake Formation con IAM Identity Center

[AWS Lake Formation](#) è un servizio gestito che semplifica la creazione e la gestione di data lake su AWS. Automatizza la raccolta, la catalogazione e la sicurezza dei dati, fornendo un repository centralizzato per l'archiviazione e l'analisi di diversi tipi di dati. Lake Formation offre controlli di accesso granulari e si integra con vari servizi di AWS analisi, consentendo alle organizzazioni di configurare, proteggere e ricavare informazioni in modo efficiente dai propri data lake.

Segui questi passaggi per consentire a Lake Formation di concedere le autorizzazioni per i dati in base all'identità dell'utente utilizzando IAM Identity Center e la propagazione affidabile delle identità.

Prerequisiti

Prima di iniziare con questo tutorial, dovrai configurare quanto segue:

- [Abilita IAM Identity Center](#). [L'istanza dell'organizzazione](#) è consigliata. Per ulteriori informazioni, consulta [Prerequisiti e considerazioni](#).

Passaggi per configurare una propagazione affidabile delle identità

1. Integra IAM Identity Center AWS Lake Formation seguendo le indicazioni contenute in [Connecting Lake Formation with IAM Identity Center](#).

Important

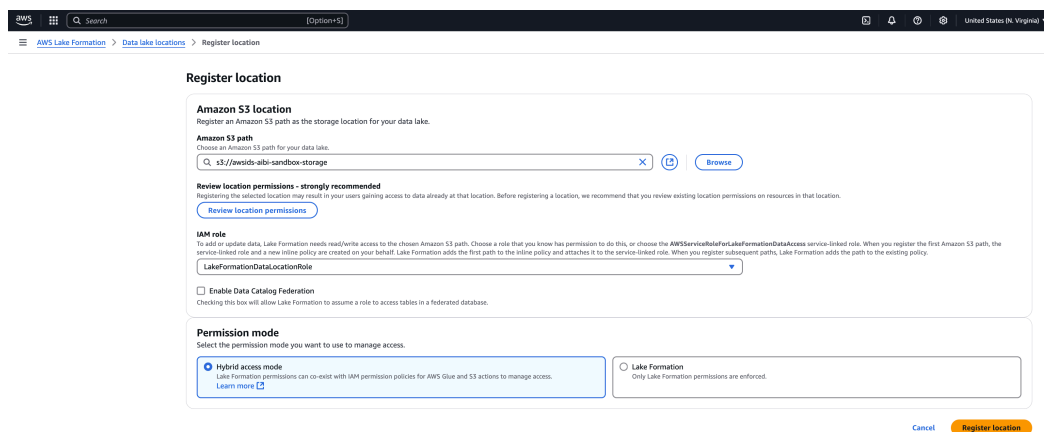
Se non disponi di AWS Glue Data Catalog tabelle, devi crearle per poterle utilizzare AWS Lake Formation per concedere l'accesso agli utenti e ai gruppi di IAM Identity Center. Per ulteriori informazioni, consulta [Creazione AWS Glue Data Catalog di oggetti in](#).

2. Registra le posizioni dei data lake.

[Registra le posizioni S3](#) in cui sono archiviati i dati delle tabelle Glue. In questo modo, Lake Formation fornirà l'accesso temporaneo alle posizioni S3 richieste quando le tabelle vengono interrogate, eliminando la necessità di includere le autorizzazioni S3 nel ruolo di servizio (ad esempio il ruolo di servizio Athena configurato su). WorkGroup

- a. Passa alle posizioni dei Data lake nella sezione Amministrazione del pannello di navigazione della console. AWS Lake Formation Seleziona Registra posizione.

Ciò consentirà a Lake Formation di fornire credenziali IAM temporanee con le autorizzazioni necessarie per accedere alle posizioni dei dati S3.



- b. Inserisci il percorso S3 delle posizioni dei dati delle AWS Glue tabelle nel campo Percorso Amazon S3.
- c. Nella sezione relativa al ruolo IAM, non selezionare il ruolo collegato al servizio se desideri utilizzarlo con una propagazione affidabile delle identità. Crea un ruolo separato con le seguenti autorizzazioni.

Per utilizzare queste politiche, sostituisci la *italicized placeholder text* politica di esempio con le tue informazioni. Per ulteriori indicazioni, consulta [Creare un criterio](#) o [Modificare un criterio](#). La politica di autorizzazione dovrebbe concedere l'accesso alla posizione S3 specificata nel percorso:

- i. Politica di autorizzazione:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LakeFormationDataAccessPermissionsForS3",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket/*"
      ]
    },
    {
      "Sid":
        "LakeFormationDataAccessPermissionsForS3ListBucket",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket"
      ]
    }
  ],
}
```

```

    {
      "Sid": "LakeFormationDataAccessServiceRolePolicy",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    }
  ]
}

```

- ii. Relazione di fiducia: ciò dovrebbe includere `sts:SetContext`, che è necessario per la propagazione di identità affidabili.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "lakeformation.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}

```

Note

Il ruolo IAM creato dalla procedura guidata è un ruolo collegato al servizio e non include `sts:SetContext`

- d. Dopo aver creato il ruolo IAM, seleziona Registra posizione.

Propagazione affidabile dell'identità con Lake Formation in tutto il mondo Account AWS

AWS Lake Formation supporta l'utilizzo di [AWS Resource Access Manager \(RAM\)](#) per condividere le tabelle Account AWS e funziona con la propagazione affidabile delle identità quando l'account del concedente e l'account del beneficiario si trovano nello stesso Regione AWS, nello stesso e condividono la stessa istanza organizzativa di IAM Identity Center. AWS Organizations Per ulteriori informazioni, consulta [Condivisione dei dati tra account in Lake Formation](#).

Configurazione di Amazon S3 Access Grants con IAM Identity Center

[Amazon S3 Access Grants](#) offre la flessibilità necessaria per garantire un controllo granulare degli accessi basato sull'identità alle sedi S3. Puoi usare Amazon S3 Access Grants per concedere l'accesso ai bucket Amazon S3 direttamente ai tuoi utenti e gruppi aziendali. Segui questi passaggi per abilitare S3 Access Grants con IAM Identity Center e ottenere una propagazione affidabile delle identità.

Prerequisiti

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

- [Abilita IAM Identity Center](#). [L'istanza dell'organizzazione](#) è consigliata. Per ulteriori informazioni, consulta [Prerequisiti e considerazioni](#).

Configurazione di S3 Access Grants per la propagazione affidabile delle identità tramite IAM Identity Center

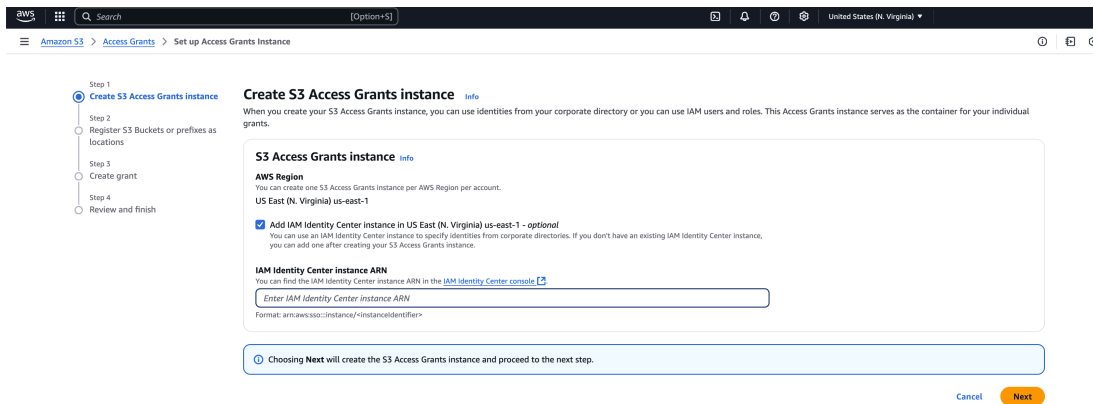
Se hai già un'Access Grantsistanza Amazon S3 con una posizione registrata, segui questi passaggi:

1. [Associa la tua istanza IAM Identity Center](#).
2. [Crea una sovvenzione](#).

Se non hai Access Grants ancora creato un Amazon S3, segui questi passaggi:

1. [Crea un'Access Grantsistanza S3](#): puoi creare un'istanza S3 Access Grants per volta. Regione AWS Quando crei l'Access Grantsistanza S3, assicurati di selezionare la casella Aggiungi istanza IAM Identity Center e di fornire l'ARN della tua istanza IAM Identity Center. Seleziona Avanti.

L'immagine seguente mostra la pagina Crea Access Grants istanza S3 nella console Amazon Access Grants S3:



2. Registra una posizione: dopo aver creato e [creato un'Access Grants istanza Amazon S3](#) Regione AWS in un account, [registri una posizione S3](#) in quell'istanza. Una Access Grants posizione S3 associa la regione S3 predefinita (S3://), un bucket o un prefisso a un ruolo IAM. S3 Access Grants assume questo ruolo di Amazon S3 per fornire credenziali temporanee al beneficiario che accede a quella particolare posizione. Devi prima registrare almeno una posizione nella tua Access Grants istanza S3 prima di poter creare una concessione di accesso.

Per l'ambito Location, specificas3://, che include tutti i bucket in quella regione. Questo è l'ambito di localizzazione consigliato per la maggior parte dei casi d'uso. Se disponi di un caso d'uso avanzato per la gestione degli accessi, puoi impostare l'ambito della posizione su un bucket s3://*bucket* o un prefisso specifico all'interno di un bucket. s3://*bucket/prefix-with-path* Per ulteriori informazioni, consulta [Registrazione una sede](#) nella Guida per l'utente di Amazon Simple Storage Service.

Note

Assicurati che le posizioni S3 delle AWS Glue tabelle a cui desideri concedere l'accesso siano incluse in questo percorso.

La procedura richiede la configurazione di un ruolo IAM per la posizione. Questo ruolo dovrebbe includere le autorizzazioni per accedere all'ambito della posizione. Puoi utilizzare la procedura guidata della console S3 per creare il ruolo. Dovrai specificare l'ARN dell'Access Grants istanza S3 nelle policy per questo ruolo IAM. Il valore predefinito dell'arn:aws:s3:*Your-*

Region:Your-AWS-Account-ID:access-grants/defaultARN dell'Access Grantsistanza S3 è.

Il seguente esempio di policy di autorizzazione fornisce ad Amazon S3 le autorizzazioni per il ruolo IAM che hai creato. E l'esempio di policy di fiducia che segue consente al responsabile del Access Grants servizio S3 di assumere il ruolo IAM.

a. Policy di autorizzazione

Per utilizzare queste politiche, sostituisci la *italicized placeholder text* politica dell'esempio con le tue informazioni. Per ulteriori indicazioni, consulta [Creare un criterio](#) o [Modificare un criterio](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectLevelReadPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts"
      ],
      "Resource": [
        "arn:aws:s3::*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "ArnEquals": {
          "s3:AccessGrantsInstanceArn": [
            "arn:aws:s3:::access-grants/instance-id"
          ]
        }
      }
    }
  ],
}
```

```

{
  "Sid": "ObjectLevelWritePermissions",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:PutObjectVersionAcl",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:AbortMultipartUpload"
  ],
  "Resource": [
    "arn:aws:s3:::*"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "111122223333"
    },
    "ArnEquals": {
      "s3:AccessGrantsInstanceArn": [
        "arn:aws:s3:::access-grants/instance-id"
      ]
    }
  }
},
{
  "Sid": "BucketLevelReadPermissions",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket"
  ],
  "Resource": [
    "arn:aws:s3:::*"
  ],
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "111122223333"
    },
    "ArnEquals": {
      "s3:AccessGrantsInstanceArn": [
        "arn:aws:s3:::access-grants/instance-id"
      ]
    }
  }
}

```

```

    },
    {
      "Sid": "OptionalKMSPermissionsForSSEEncryption",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

b. Policy di trust

Nella policy di attendibilità del ruolo IAM, concedi al principale del servizio S3 Access Grants (access-grants.s3.amazonaws.com) l'accesso al ruolo IAM creato. A tal fine, è possibile creare un file JSON contenente le seguenti istruzioni. Per aggiungere la policy di attendibilità all'account, consulta [Creare un ruolo utilizzando policy di attendibilità personalizzati](#).

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1234567891011",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333",
          "aws:SourceArn": "Your-Custom-Access-Grants-Location-ARN"
        }
      }
    }
  ]
}

```

```

    },
    {
      "Sid": "Stmt1234567891012",
      "Effect": "Allow",
      "Action": "sts:SetContext",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333",
          "aws:SourceArn": "Your-Custom-Access-Grants-Location-
ARN"
        },
        "ForAllValues:ArnEquals": {
          "sts:RequestContextProviders":
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
        }
      }
    }
  ]
}

```

Crea una concessione di accesso per Amazon S3

Se disponi di un'Access Grantsistanza Amazon S3 con una posizione registrata e hai associato la tua istanza IAM Identity Center ad essa, puoi [creare una concessione](#). Nella pagina Create Grant della console S3, completa quanto segue:

Creazione di una concessione

1. Seleziona la posizione creata nel passaggio precedente. È possibile ridurre l'ambito della concessione aggiungendo un prefisso secondario. Il sottoprefisso può essere un bucketbucket/prefix, o un oggetto nel bucket. Per ulteriori informazioni, consulta [Subprefix](#) nella Guida per l'utente di Amazon Simple Storage Service.
2. In Autorizzazioni e accesso, seleziona Leggi o Scrivi a seconda delle tue esigenze.
3. Nel tipo Granter, scegli Directory Identity da IAM Identity Center.
4. Fornisci l'ID utente o di gruppo di IAM Identity Center. Puoi trovare l'utente e il gruppo IDs nella console IAM Identity Center [nelle sezioni Utente e gruppo](#). Seleziona Avanti.

5. Nella pagina Revisione e conclusione, rivedi le impostazioni per S3Access Grant, quindi seleziona **Create Grant**.

L'immagine seguente mostra la pagina **Create Grant** nella console Amazon S3: Access Grants

Create Grant Info

Grant Info
Grant a user or role a specific level of access to your S3 data.

Grant scope
The grant scope is a combination of the location and the subprefix. Choose a registered location or register a new location. To narrow the scope, specify a subprefix. If you use the default "s3://" location, you must specify a subprefix.

Location Info
s3:// Browse locations Register location Location ID Info IAM role Info
[s3accessgrants_role_for_location_for_awsid-wbi-sandbox-storage](#)

Subprefix - optional Info
Further scope the grant to a bucket, prefix, or an individual object.

Don't include any part of the grant already specified in the location.
Format for bucket: "bucket/"
Format for prefix: "bucket/prefix-with-slash/"
Format for object: "bucket/prefix-with-slash/object"

Grant scope Info
s3://
☐ The grant scope is an object

Permissions and access
Grant a user or role a specific level of access to your S3 data.

The S3 console can't be used to access the data specified in the grant scope. To access the data, the grantee must do so through the AWS CLI, the application, or other AWS services.

Permissions
☒ Read
☐ Write

Grantee type Info
☒ Directory identity from IAM Identity Center
☐ IAM principal

Directory identity type Info
☐ User
☒ Group

IAM Identity Center group ID Info
The group that you want to grant this level of access to. You can find the ID in the [IAM Identity Center console](#).

Configurazione della propria applicazione 2.0 OAuth

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. Servizi AWS

Important

Per accedere a un' Servizio AWS applicazione gestita dal cliente deve 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 a Servizi AWS (applicazioni riceventi). 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](#)
- [Utilizzo di applicazioni con un emittente di token affidabile](#)

Configura applicazioni OAuth 2.0 gestite dal cliente per la propagazione affidabile delle identità

Per configurare un'applicazione Customer Managed OAuth 2.0 per la propagazione affidabile delle identità, 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 Centro identità IAM](#).
2. Selezionare Applications (Applicazioni).
3. Scegli la scheda Gestione clienti.
4. Scegli Aggiungi applicazione.
5. Nella pagina Seleziona tipo di applicazione, alla voce Preferenze di impostazione, scegli Applicazione da configurare presente.
6. In Tipo di applicazione, scegli OAuth 2.0.
7. Scegliete 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 scegli 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 [Taggare le 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 la OAuth versione 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 da AWS (applicazioni di ricezione).

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 emittente di token attendibili.
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 Enable refresh token grant. Se selezionata, questa opzione aggiorna il token di accesso per la sessione ogni 60 minuti, fino alla scadenza della sessione o fino alla fine della sessione da parte dell'utente.
4. Scegli Avanti e passa 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. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo.

Questa politica richiede l'azione dell'[CreateTokenWithIAMAPI](#). Per ulteriori informazioni su questa politica e un esempio che è possibile adattare in base alle esigenze del proprio ambiente, consulta [Esempio di policy basato sulle risorse per IAM Identity Center \(IAM Identity Center\)](#).

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 politiche basate sulle risorse e IAM nella Guida per l'utente. ARNs 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 una o più Servizi AWS applicazioni attendibili 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 attendibili per quel servizio.

1. Apri la [console Centro identità IAM](#).
2. Selezionare Applications (Applicazioni).
3. Scegli la scheda Gestione clienti.
4. Nell'elenco Applicazioni gestite dal cliente, selezionare l'applicazione OAuth 2.0 per la quale si desidera avviare le richieste di accesso. Questa è l'applicazione a cui accedono gli utenti.
5. Nella pagina Dettagli, in Applicazioni attendibili per la propagazione dell'identità, scegli Specifica applicazioni attendibili.
6. In Tipo di configurazione, seleziona Applicazioni individuali e specifica l'accesso, quindi scegli Avanti.

7. Nella pagina **Seleziona servizio**, scegli il AWS servizio che include 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 accesso per applicazione** - Seleziona questa opzione per configurare livelli di accesso diversi 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 secondo necessità, quindi scegli **Salva modifiche**.
 - **Applica lo stesso livello di accesso a tutte le applicazioni**: seleziona questa opzione se non è necessario configurare i livelli di accesso per singola applicazione.
10. Scegli **Next (Successivo)**.
11. Nella pagina **Rivedi configurazione**, rivedi le scelte effettuate. Per apportare modifiche, scegli la sezione di configurazione desiderata, scegli **Modifica accesso** e apporta le modifiche richieste.
12. Al termine, scegli **Applicazioni affidabili**.

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 da AWS.

I seguenti argomenti descrivono come funzionano gli emittenti di token affidabili e forniscono indicazioni sulla configurazione.

Argomenti

- [Panoramica degli emittenti di token affidabili](#)
- [Prerequisiti e considerazioni per emittenti di token affidabili](#)
- [Dettagli del reclamo JTI](#)

- [Impostazioni di configurazione dell'emittente di token affidabili](#)
- [Configurazione di un emittente di token affidabile](#)
- [Sessioni di ruolo IAM con identità migliorate](#)

Panoramica degli emittenti di token affidabili

La propagazione affidabile delle identità fornisce un meccanismo che consente alle applicazioni che si autenticano 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 a (applicazioni riceventi). Servizi 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 affidabile del token che a IAM Identity Center.

Servizi AWS coloro che ricevono richieste gestiscono l'autorizzazione dettagliata alle proprie risorse in base agli utenti e all'appartenenza ai gruppi, come indicato nella directory di Identity Center. Servizi AWS non può 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 affidabile di token è una decisione di sicurezza che richiede un'attenta considerazione. Scegliete solo emittenti di token affidabili di cui vi fidate 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 deve essere 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 individuazione di OIDC (URL dell'emittente) nell'emittente di token attendibile.
 - [Soggetto](#) (sub): l'utente autenticato.
 - [Pubblico](#) (aud): il destinatario previsto del token. Questo è l'oggetto Servizio AWS 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.

Note

L'utilizzo di una chiave di firma personalizzata per JWTs from non Microsoft Entra ID è supportato. Per utilizzare token forniti da un emittente Microsoft Entra ID di token affidabile, non è possibile utilizzare una chiave di firma personalizzata.

- Reclami 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.

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 ha esito negativo. 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. OAuth 1 server di autorizzazione 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 \(URL dell'emittente\)](#)
- [Mappatura degli attributi](#)
- [Reclamo Audi](#)

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 dell'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.

L'URL dell'endpoint di rilevamento OIDC deve essere raggiungibile solo tramite le porte 80 e 443.

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 ad avviare richieste per conto dei rispettivi utenti verso un'applicazione ricevente. Servizio 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 eseguono 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.	Amministratore IdP esterno (trusted token issuer)
	Aiuta a configurare la corretta mappatura degli attributi tra IAM Identity Center e l'IdP esterno.	AWS amministratore del servizio
	Notifica all'amministratore del AWS servizio quando l'emittente affidabil	

Ruolo	Esegue queste attività	Si coordina con
	e del token viene aggiunto alla console IAM Identity Center.	
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 la presenza nella console di AWS servizio dell'emittente affidabile e del 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 di IAM Identity Center 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 IAM Identity Center](#) o [APIs](#). 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). L'endpoint di rilevamento deve essere raggiungibile solo tramite le porte 80 e 443.
 - 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 dell'applicazione o dell'applicazione APIs.

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 Centro identità IAM](#).
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.
6. In Attributi della mappa, procedi come segue:
 - 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.
7. In Tag (opzionale), scegli Aggiungi nuovo tag, specifica un valore per Chiave e, facoltativamente, per Valore.

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 [Taggare le risorse AWS IAM Identity Center](#).

8. Scegli Crea emittente di token attendibili.
9. Una volta terminata la creazione dell'emittente di token attendibili, contatta l'amministratore dell'applicazione per comunicargli il nome dell'emittente di token attendibili, in modo che possa confermare che l'emittente di token attendibili 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.

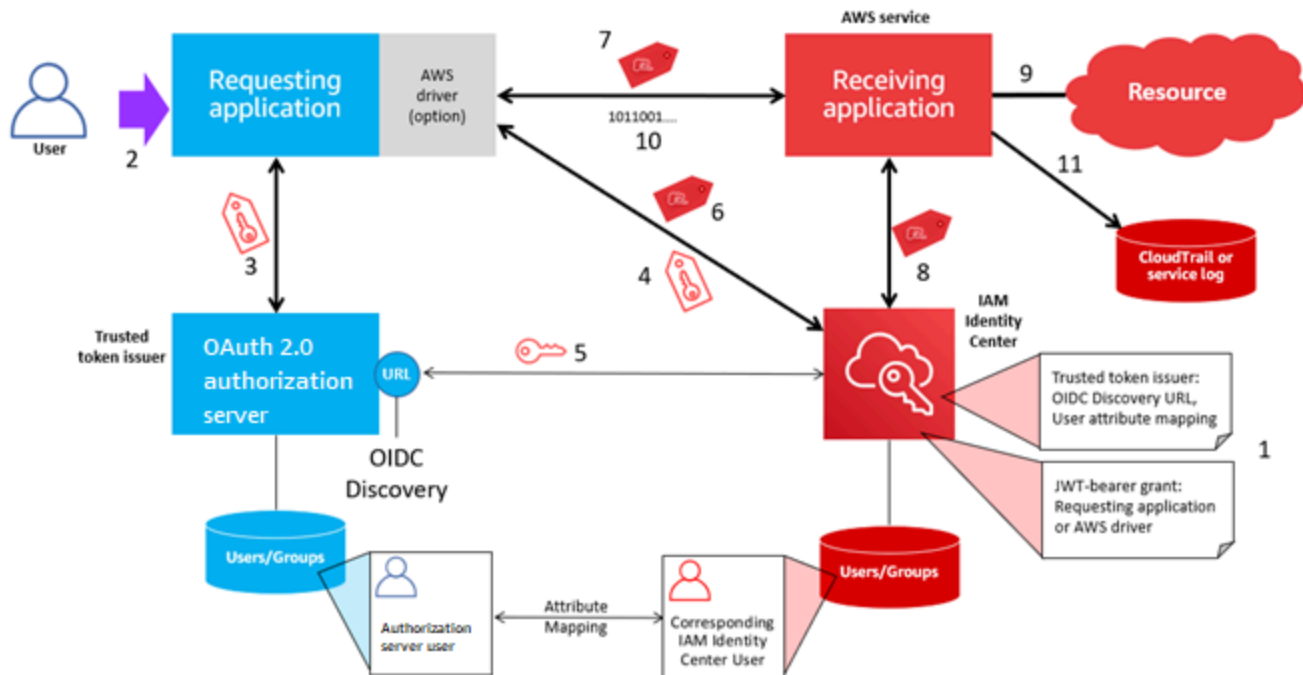
Se prevedi di modificare le impostazioni dell'emittente di token affidabili, tieni presente che così facendo gli utenti potrebbero perdere l'accesso a tutte le applicazioni configurate per utilizzare l'emittente di token affidabili. Per evitare di interrompere l'accesso degli utenti, consigliamo di coordinarsi 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 Centro identità IAM](#).
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. Scegli Save changes (Salva modifiche).
8. Nella finestra di dialogo Modifica l'emittente del token affidabile, viene richiesto di confermare che si desidera 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 vengono registrati nei registri e CloudTrail negli eventi dell'applicazione ricevente. Il modo specifico in cui queste informazioni vengono registrate varia in base all'applicazione.

Sessioni di ruolo IAM con identità migliorate

[AWS Security Token Service](#) (STS) consente a un'applicazione di ottenere una sessione di ruolo IAM con identità migliorata. Le sessioni di ruolo con identità migliorata hanno un contesto di identità aggiunto che associa un identificatore utente a quello che richiamano. Servizio AWS Servizi AWS può cercare le appartenenze ai gruppi e gli attributi dell'utente in IAM Identity Center e utilizzarli per autorizzare l'accesso dell'utente alle risorse.

AWS le applicazioni ottengono sessioni di ruolo con identità migliorata effettuando richieste all'azione AWS STS [AssumeRole](#) API e passando un'asserzione di contesto con l'identificatore dell'utente (`userId`) nel parametro della richiesta `AssumeRole`. L'asserzione di contesto è ottenuta dal `idToken` reclamato ricevuto in risposta a una richiesta inviata a `to`. SSO OIDC [CreateTokenWithIAM](#) Quando un'AWS applicazione utilizza una sessione di ruolo con identità avanzata per accedere a una risorsa, CloudTrail registra la `userId` sessione di avvio e l'azione intrapresa. Per ulteriori informazioni, consulta [Registrazione delle sessioni di ruolo IAM con funzionalità di identità ottimizzate](#).

Argomenti

- [Tipi di sessioni di ruolo IAM con identità migliorata](#)
- [Registrazione delle sessioni di ruolo IAM con funzionalità di identità ottimizzate](#)

Tipi di sessioni di ruolo IAM con identità migliorata

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 Le applicazioni che hanno ottenuto token Id da IAM Identity Center possono essere aggiunte `sts:identity_context` (scelta consigliata) o `sts:audit_context` (supportata per la compatibilità con le versioni precedenti) alle sessioni di ruolo IAM. Una sessione di ruolo IAM con identità migliorata può avere solo una di queste asserzioni di contesto, non entrambe.

Sessioni di ruolo IAM con identità migliorate e create con **sts:identity_context**

Quando una sessione di ruolo con identità migliorata contiene `sts:identity_context` le chiamate Servizio AWS determina se l'autorizzazione delle risorse si basa sull'utente rappresentato nella sessione di ruolo o se è basata sul ruolo. Servizi AWS che supportano l'autorizzazione basata sull'utente forniscono all'amministratore dell'applicazione i controlli per assegnare l'accesso all'utente o ai gruppi di cui l'utente è membro.

Servizi AWS che non supportano l'autorizzazione basata sull'utente ignorano il.

`sts:identity_context` CloudTrail registra l'userID dell'utente IAM Identity Center con tutte le azioni intraprese dal ruolo. Per ulteriori informazioni, consulta [Registrazione delle sessioni di ruolo IAM con funzionalità di identità ottimizzate](#).

Per ottenere questo tipo di sessione di ruolo con identità avanzata da AWS STS, le applicazioni forniscono il valore del `sts:identity_context` campo nella richiesta utilizzando il parametro request. [AssumeRole](#) `ProvidedContexts` Usa `arn:aws:iam::aws:contextProvider/IdentityCenter` come valore per. `ProviderArn`

Per ulteriori informazioni su come si comporta l'autorizzazione, consulta la documentazione per la ricezione Servizio AWS.

Sessioni di ruolo IAM con identità avanzate create con **sts:audit_context**

In passato, `sts:audit_context` veniva utilizzato per consentire di Servizi AWS registrare l'identità dell'utente senza utilizzarla per prendere una decisione di autorizzazione. Servizi AWS sono ora in grado di utilizzare un unico contesto `sts:identity_context` - - per raggiungere questo obiettivo e per prendere decisioni di autorizzazione. Si consiglia di utilizzare `sts:identity_context` in tutte le nuove implementazioni la propagazione affidabile delle identità.

Registrazione delle sessioni di ruolo IAM con funzionalità di identità ottimizzate

Quando viene effettuata una richiesta a una sessione di ruolo IAM basata sull' Servizio AWS utilizzo di un ruolo IAM con identità migliorata, l'IAM Identity Center `userId` dell'utente viene registrato nell'elemento `CloudTrail OnBehalfOf`. Il modo in cui gli eventi vengono registrati varia in base a `CloudTrail` . Servizio AWS Non tutti Servizi AWS registrano l'`onBehalfOf`elemento.

Di seguito è riportato un esempio di come viene registrata una richiesta effettuata a una sessione di Servizio AWS utilizzo di un ruolo con identità avanzata. `CloudTrail`

```
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AROEXAMPLE:MyRole",
  "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
  "accountId": "111111111111",
  "accessKeyId": "ASIAEXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROEXAMPLE",
      "arn": "arn:aws:iam::111111111111:role/MyRole",
      "accountId": "111111111111",
      "userName": "MyRole"
    },
    "attributes": {
      "creationDate": "2023-12-12T13:55:22Z",
      "mfaAuthenticated": "false"
    }
  },
  "onBehalfOf": {
    "userId": "11111111-1111-1111-1111-111111111111",
    "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/d-1111111111"
  }
}
```

Ruota i certificati IAM Identity Center

IAM Identity Center utilizza i certificati per impostare 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.

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 Centro identità IAM](#).
 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 Centro identità IAM](#).
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 domanda. È possibile eliminare solo un certificato che si trova in uno stato Inattivo.

1. Apri la [console Centro identità IAM](#).
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 console IAM Identity Center, la pagina Applicazioni mostra le icone degli indicatori di stato nelle proprietà di ciascuna applicazione. 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 visualizzare 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 di un certificato

1. Apri la [console Centro identità IAM](#).
2. Selezionare Applications (Applicazioni).
3. Nell'elenco delle applicazioni, verifica lo stato dei certificati nell'elenco, come indicato nella colonna Scade il.

Comprendi 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.

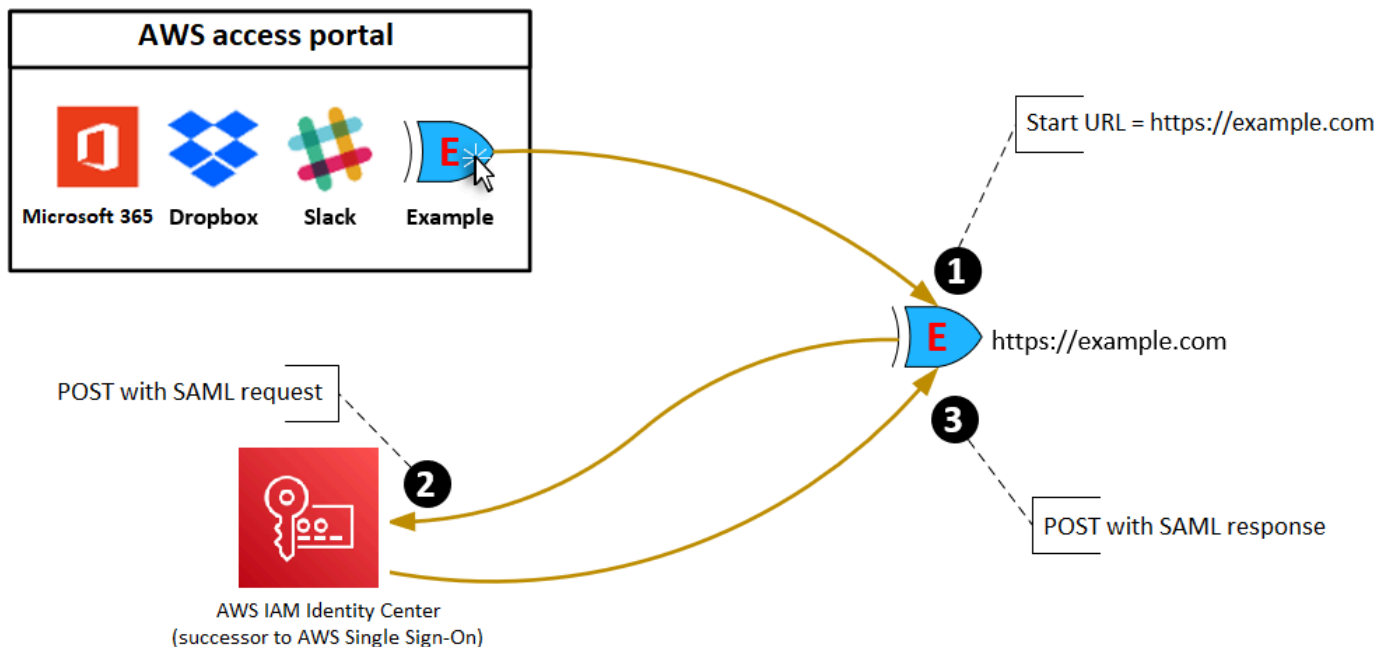
URL di avvio dell'applicazione

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

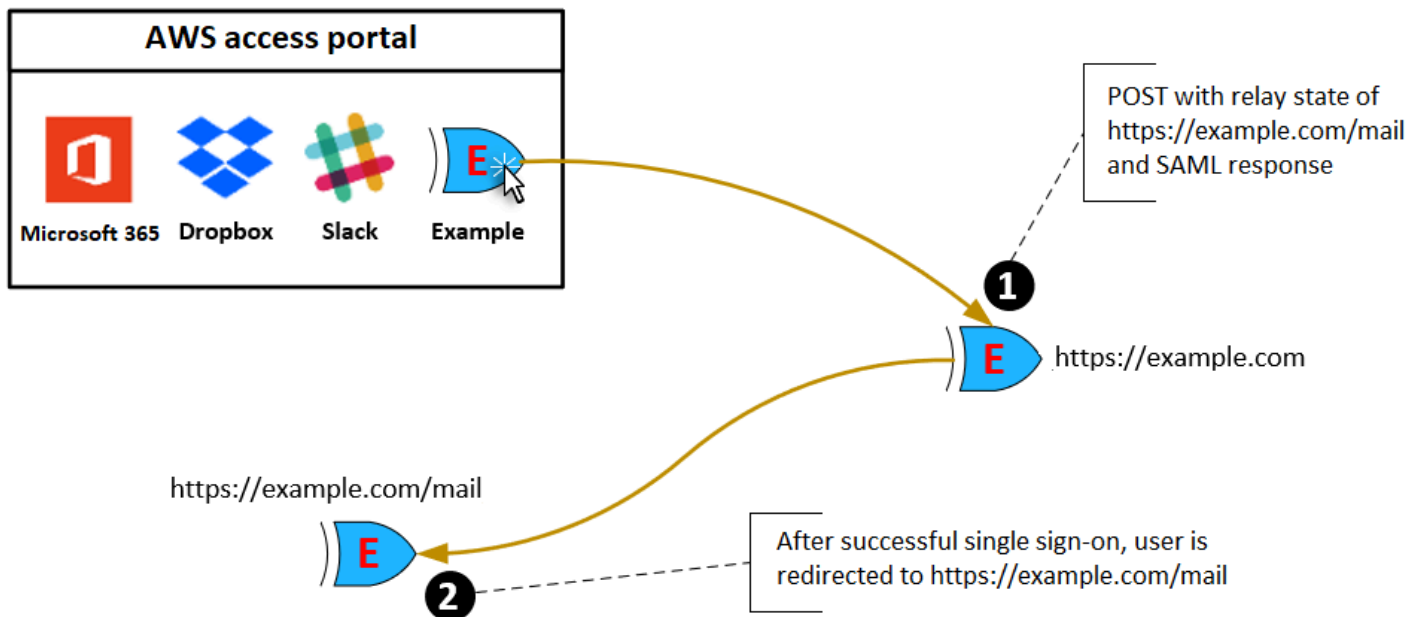
1. Il browser dell'utente reindirizza la richiesta di autenticazione utilizzando il valore dell'URL di avvio dell'applicazione (in questo caso). <https://example.com>
2. L'applicazione invia un HTML POST with SAMLRequest a a IAM Identity Center.

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 inoltra 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 API.

1. Apri la [console Centro identità IAM](#).

 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 visualizzato o un nome di gruppo. È possibile specificare più utenti o gruppi selezionando gli account applicabili così come appaiono nei risultati di ricerca.
6. Scegliere Assign users (Assegna utenti).

Rimuovi l'accesso degli utenti alle applicazioni SAML 2.0

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 ulteriori informazioni sulle sessioni e sulle durate di autenticazione, consulta [Comprendere le sessioni di autenticazione in IAM Identity Center](#)

Per rimuovere l'accesso degli utenti a un'applicazione

1. Apri la [console Centro identità IAM](#).

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 Centro identità IAM](#).
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 in [Mappature degli attributi tra IAM Identity Center e la directory External Identity Provider](#).
8. Nella terza colonna della tabella, scegli il formato appropriato per l'attributo dal menu.
9. Scegli Save changes (Salva modifiche).

Configurare l'accesso a Account AWS

AWS IAM Identity Center è integrato con AWS Organizations, il che ti consente di gestire centralmente le autorizzazioni su più account Account AWS senza configurare manualmente ciascuno dei tuoi account. Puoi definire le autorizzazioni e assegnarle agli utenti della forza lavoro per controllarne l'accesso a risorse specifiche Account AWS utilizzando un'istanza [organizzativa](#) di IAM Identity Center. [Le istanze di account](#) di IAM Identity Center non supportano l'accesso all'account.

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 [Amministratore delegato](#).

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
Crea, modifica o elimina applicazioni gestite dai clienti	⊗ No	✔ Sì	✔ Sì
Creare, modificare o eliminare applicazioni AWS gestite	✔ Sì	✔ 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
Abilita IAM Identity Center	⊗ No	⊗ No	✔ Sì
Elimina la configurazione di IAM Identity Center	⊗ No	⊗ No	✔ Sì

Attività amministrative di IAM Identity Center	Account membro	Account amministratore delegato	Gestione dell'account
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

*Consulta le migliori pratiche per l'amministrazione delegata relative all'assegnazione di utenti e gruppi all'account di gestione.

Assegnazione dell'accesso Account AWS

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 [Creare, gestire ed eliminare set di autorizzazioni](#).

Note

Puoi anche assegnare ai tuoi utenti l'accesso Single Sign-On alle applicazioni. Per informazioni, consulta [Configurare 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 [Console di gestione AWS](#), 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 Console di gestione AWS o recuperare le credenziali temporanee per accedere ai AWS servizi in modo programmatico.

Per aprire Console di gestione AWS 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 Console di gestione AWS.
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. [Configurazione e utilizzo del portale di AWS accesso](#) [Ottenere le credenziali utente di IAM Identity Center per o AWS CLI AWS SDKs](#)

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 del servizio (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 Organizations È necessario assegnare a uno o più utenti l'accesso a un account per utilizzare questo ruolo. Per ulteriori informazioni, consultare [Comprensione dei ruoli collegati ai servizi in IAM Identity Center](#) 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

Per garantire il corretto funzionamento delle applicazioni AWS gestite con il vostro IAM Identity Center, dovreste evitare di applicare questo SCP al Account AWS luogo in cui avete distribuito tali applicazioni. Inoltre, se utilizzi l'amministrazione delegata, dovresti evitare di applicare questo SCP all'account di amministrazione delegato. Per ulteriori informazioni, consulta [Best practice](#).

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

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 [Configurare 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](#)
- [Prerequisiti](#)
- [Registra un account membro](#)
- [Annullamento della registrazione di un account membro](#)
- [Visualizza quale account membro è stato registrato come amministratore delegato](#)

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. Puoi anche prendere in considerazione l'utilizzo di un [accesso temporaneo elevato](#) per concedere questo accesso solo quando necessario.
- Set di autorizzazioni dedicati per l'account di gestione: utilizza set di autorizzazioni dedicati per l'account di gestione. Per motivi di sicurezza, un set di autorizzazioni utilizzato per l'accesso all'account di gestione può essere modificato solo da un amministratore IAM Identity Center dell'account di gestione. L'amministratore delegato non può modificare i set di autorizzazioni forniti nell'account di gestione.
- Assegna solo gli utenti (non i gruppi) ai set di autorizzazioni nell'account di gestione: poiché l'account di gestione dispone di privilegi speciali, è necessario prestare attenzione quando si assegna l'accesso a questo account nella console o (AWS Command Line Interface CLI). Se si assegnano gruppi a set di autorizzazioni con accesso all'account di gestione, chiunque disponga delle autorizzazioni per modificare le appartenenze a tali gruppi può utilizzare tali gruppi e quindi influire sugli add/remove utenti to/from che hanno accesso all'account di gestione. Si tratta di qualsiasi amministratore di gruppo con il controllo sulla fonte di identità, incluso l'amministratore del provider di identità (IdP), l'amministratore del servizio di dominio Microsoft Active Directory (AD DS) o l'amministratore di IAM Identity Center. Pertanto, è necessario assegnare gli utenti direttamente ai set di autorizzazioni che concedono l'accesso nell'account di gestione ed evitare i gruppi. Se utilizzi i gruppi per gestire l'accesso all'account di gestione, assicurati che nell'IdP siano presenti controlli adeguati per limitare chi ha la possibilità di modificare tali gruppi e assicurati che le modifiche a tali gruppi (o le modifiche alle credenziali per gli utenti nell'account di gestione) vengano registrate e riviste, se necessario.

- Considera la tua posizione in Active Directory: se prevedi di utilizzare Active Directory come fonte di identità 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 la fonte di 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 desideri che Active Directory sia presente nell'account di gestione, devi eseguire la configurazione nell'account di gestione poiché l'amministratore delegato non disporrà delle autorizzazioni necessarie per completarla.

Limita le azioni di archiviazione delle identità di IAM Identity Center nell'account di amministrazione delegato con fonti di identità esterne

Se utilizzi una fonte di identità esterna come un IdP o Directory Service, dovresti implementare politiche che limitino le azioni di archiviazione delle identità che un amministratore di IAM Identity Center può eseguire dall'interno dell'account di amministrazione delegato. Le operazioni di scrittura ed eliminazione devono essere considerate con attenzione. In genere, la fonte di identità esterna è la fonte di verità per gli utenti e i relativi attributi e per l'appartenenza ai gruppi. Se li modifichi utilizzando l'archivio di identità APIs o la console, le modifiche verranno sovrascritte durante i normali cicli di sincronizzazione. È meglio lasciare queste operazioni al controllo esclusivo della fonte di verità della propria identità. Ciò impedisce inoltre che un amministratore di IAM Identity Center modifichi le appartenenze ai gruppi per concedere l'accesso a un set di autorizzazioni o a un'applicazione assegnati dal gruppo, anziché lasciare il controllo dell'appartenenza al gruppo all'amministratore IdP. È inoltre necessario evitare chi può creare token SCIM bearer dall'account di amministrazione delegato, in quanto questi potrebbero consentire a un amministratore dell'account membro di modificare gruppi e utenti tramite un client SCIM.

Ci possono essere momenti in cui le operazioni di scrittura o cancellazione dall'account amministratore delegato sono appropriate. Ad esempio, puoi creare un gruppo senza aggiungere membri, quindi assegnare assegnazioni a un set di autorizzazioni senza dover attendere che l'amministratore IdP crei il gruppo. Nessuno avrà accesso a quell'assegnazione finché l'amministratore IdP non provvede al gruppo e il processo di sincronizzazione IdP non stabilisce i membri del gruppo. Potrebbe anche essere opportuno eliminare un utente o un gruppo per impedire l'accesso o l'autorizzazione durante un periodo in cui non è possibile attendere il processo di sincronizzazione IdP per rimuovere l'accesso dell'utente o del gruppo. Tuttavia, l'uso improprio di questa autorizzazione può causare problemi agli utenti. È necessario utilizzare il principio del privilegio minimo quando si assegnano le autorizzazioni dell'archivio di identità. È possibile

controllare quali azioni di archiviazione delle identità sono consentite dagli amministratori degli account di amministrazione delegati utilizzando una policy di controllo del servizio (SCP).

L'esempio SCP riportato di seguito impedisce l'assegnazione di utenti a gruppi tramite l'API Identity Store e la Console di gestione AWS, operazione consigliata quando la fonte di identità è esterna. Ciò non influisce sulla sincronizzazione degli utenti da Directory Service o verso un IdP esterno (tramite SCIM).

Note

È possibile che, sebbene si utilizzi una fonte di identità esterna, l'organizzazione si affidi, in tutto o in parte, all'Identity Store APIs per la fornitura di utenti e gruppi. Pertanto, prima di attivare questo SCP, è necessario confermare che il processo di provisioning degli utenti non utilizzi questa operazione API di Identity Store. Inoltre, fate riferimento alla sezione successiva per informazioni su come limitare la gestione delle appartenenze ai gruppi a gruppi specifici.

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Effect": "Deny",
      "Action": ["identitystore:CreateGroupMembership"],
      "Resource": [ "*" ] }
  ]
}
```

Se desideri evitare di aggiungere utenti solo ai gruppi che concedono l'accesso all'account di gestione, puoi fare riferimento a quei gruppi specifici utilizzando l'ARN del gruppo nel seguente formato: `arn:${Partition}:identitystore:::group/${GroupId}`. Questo e altri tipi di risorse disponibili in Identity Store sono documentati in [Tipi di risorse definiti da AWS Identity Store](#) nel Service Authorization Reference. Puoi anche prendere in considerazione l'inclusione di un Identity Store aggiuntivo APIs in SCP. Per ulteriori informazioni, consulta [Actions](#) in the Identity Store API Reference.

Aggiungendo la seguente dichiarazione politica al tuo SCP, puoi impedire la creazione di token portatori SCIM da parte dell'amministratore delegato. Puoi applicarlo a entrambe le fonti di identità esterne.

 Note

Se l'amministratore delegato deve configurare il provisioning degli utenti con SCIM o eseguire la rotazione periodica del token SCIM bearer, dovrai consentire temporaneamente l'accesso a questa API per consentire all'amministratore delegato di completare tali attività.

```
{ "Effect": "Deny",  
  "Action": ["sso-directory:CreateBearerToken"],  
  "Resource": [ "*" ]  
}
```

Limita le azioni di archiviazione delle identità di IAM Identity Center nell'account di amministrazione delegato per gli utenti gestiti localmente

Se crei utenti e gruppi direttamente in IAM Identity Center, anziché utilizzare un IdP esterno o Directory Service, dovresti prendere precauzioni per chi può creare utenti, reimpostare le password e controllare l'appartenenza ai gruppi. Queste azioni conferiscono all'amministratore ampi poteri su chi può accedere e chi può accedervi tramite l'appartenenza a gruppi. Il modo migliore per implementare queste policy è come policy in linea all'interno dei set di autorizzazioni utilizzate per gli amministratori di IAM Identity Center, piuttosto che come SCPs. L'esempio seguente di politica in linea ha due obiettivi. Innanzitutto, impedisce l'aggiunta di utenti a gruppi specifici. Puoi usarlo per impedire agli amministratori delegati di aggiungere utenti ai gruppi che concedono l'accesso all'account di gestione. In secondo luogo, impedisce l'emissione di token al portatore SCIM.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    { "Effect": "Deny",  
      "Action": ["identitystore:CreateGroupMembership"],  
      "Resource": [ arn:${Partition}:identitystore:::group/${GroupId1},  
                    arn:${Partition}:identitystore:::group/${GroupId2}  
                    ]  
    }  
  ],  
  { "Effect": "Deny",  
    "Action": ["sso-directory:CreateBearerToken"],
```

```
"Resource": [ "*" ] }  
]  
}
```

Separa la gestione della configurazione di IAM Identity Center dalla gestione PermissionSet

Separa le attività amministrative, tra cui la modifica dell'origine dell'identità esterna, la gestione dei token SCIM, la configurazione del timeout della sessione, dalle attività di creazione, modifica e assegnazione dei set di autorizzazioni creando set di autorizzazioni di amministrazione distinti dal tuo account di gestione.

Limita l'emissione di token portatori SCIM

I token portatori SCIM consentono a una fonte di identità esterna di fornire utenti, gruppi e appartenenze ai gruppi tramite il protocollo SCIM quando la fonte di identità del tuo IAM Identity Center è un IdP esterno come Okta o Entra ID. È possibile configurare il seguente SCP per impedire la creazione di token portatori SCIM da parte degli amministratori delegati. Se l'amministratore delegato deve configurare il provisioning degli utenti con SCIM o eseguire la rotazione periodica dei token SCIM bearer, sarà necessario consentire temporaneamente l'accesso a questa API per consentire all'amministratore delegato di completare tali attività.

```
{ "Effect": "Deny",  
  "Action": ["sso-directory:CreateBearerToken"],  
  "Resource": [ "*" ]  
}
```

Utilizzate i tag dei set di autorizzazioni e gli elenchi di account per delegare l'amministrazione di account specifici

Puoi creare set di autorizzazioni da assegnare agli amministratori del tuo IAM Identity Center per delegare chi può creare set di autorizzazioni e chi può assegnare quali set di autorizzazioni in quali account. Questo viene fatto etichettando i set di autorizzazioni e utilizzando le condizioni delle policy nei set di autorizzazioni assegnati agli amministratori. Ad esempio, è possibile creare set di autorizzazioni che consentono a un utente di creare set di autorizzazioni a condizione che venga etichettato in un determinato modo. È inoltre possibile creare politiche che consentano a un

amministratore di assegnare set di autorizzazioni con un tag specifico in determinati account. In questo modo è possibile delegare la gestione degli account senza concedere a un amministratore i privilegi per modificare il proprio accesso e i privilegi sull'account di amministrazione delegato. Ad esempio, etichettando i set di autorizzazioni utilizzati solo nell'account di amministrazione delegato, è possibile specificare una politica che conceda solo a determinate persone le autorizzazioni per modificare i set di autorizzazioni e le assegnazioni che influiscono sull'account di amministrazione delegato. È inoltre possibile concedere ad altre persone le autorizzazioni per gestire un elenco di account esterni all'account di amministrazione delegato. Per ulteriori informazioni, consulta la sezione [Delega della gestione dei set di autorizzazioni e dell'assegnazione degli account AWS IAM Identity Center nel Security Blog](#).AWS

Prerequisiti

Prima di poter registrare un account come amministratore delegato, devi prima aver distribuito il 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 nell' 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 Console di gestione AWS 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 Console di gestione AWS 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 scoprire quale account membro del tuo account AWS Organizations è stato configurato come amministratore delegato per IAM Identity Center.

Per visualizzare il tuo account di membro registrato

1. Apri la [console Centro identità IAM](#).
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 per Account AWS

Ogni accesso al tuo Account AWS implica un certo livello di privilegio. Le operazioni sensibili, come la modifica della configurazione per un ambiente di produzione, richiedono un trattamento speciale a causa della portata e del potenziale impatto. L'accesso temporaneo con privilegi elevati (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.

Note

Per garantire la continuità aziendale, si consiglia di [configurare l'accesso di emergenza a](#). Console di gestione AWS

Per soddisfare una vasta gamma di esigenze dei clienti, AWS IAM Identity Center si integra con le soluzioni dei partner AWS Security Competency. AWS convalida che queste soluzioni soddisfino 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 specifiche, tra cui la tua attività, l'architettura del tuo ambiente cloud e il tuo budget.

Le soluzioni convalidate includono [Apono Access Management Platform](#), [CyberArk Secure Cloud Access](#), [Okta Access Requests](#) e [Tenable](#) (precedentemente Ermetic).

I partner possono proporre soluzioni utilizzando l'applicazione Security Competency disponibile nel AWS Partner Center. Per ulteriori informazioni, consulta [AWS Security Competency Partners](#).

Note

Se utilizzi Amazon Elastic AWS Key Management Service Kubernetes Service basato su risorse [oppure consulta i set di autorizzazioni di riferimento nelle politiche delle risorse, le](#)

[mappe di configurazione AWS KMS dei cluster Amazon EKS e le politiche](#) chiave prima di scegliere la soluzione. just-in-time

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 con privilegi elevati, per ulteriori restrizioni di sicurezza è necessario disporre della politica di [IAMFullaccesso](#) o di autorizzazioni equivalenti prima di poterlo configurare. Queste restrizioni di sicurezza aggiuntive non sono richieste per nessuno degli account membro dell'organizzazione. AWS

Argomenti

- [Assegna l'accesso a utenti o gruppi a Account AWS](#)
- [Rimuovere l'accesso di utenti e gruppi a un Account AWS](#)
- [Revoca le sessioni di ruolo IAM attive create dai set di autorizzazioni](#)
- [Delega chi può assegnare l'accesso Single Sign-On a utenti e gruppi nell'account di gestione](#)

Assegna l'accesso a utenti o gruppi 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. [Visualizzare e modificare un set di autorizzazioni](#)

 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 Centro identità IAM](#).

 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 AWS pagina 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.

 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: Seleziona i 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 indicati [Creare un set di autorizzazioni](#). Dopo aver creato i set di autorizzazioni che desideri applicare, nella console IAM Identity Center, torna Account AWS e 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.

Considerazioni

- 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 con privilegi elevati, per ulteriori restrizioni di sicurezza è necessario disporre della politica di [IAMFullaccesso](#) o di autorizzazioni equivalenti prima di poterlo configurare. Queste restrizioni di sicurezza aggiuntive non sono richieste per nessuno degli account membro dell'organizzazione. AWS

8. 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 utilizzando una AWS Managed Microsoft AD directory o una directory autogestita in Active Directory come origine dell'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.

In alternativa, è possibile utilizzare [AWS CloudFormation](#) per 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 \(AWS CLI\)](#).

Rimuovere l'accesso di utenti e gruppi a un Account AWS

Utilizzare questa procedura per rimuovere l'accesso Single Sign-On a uno Account AWS o più utenti e gruppi nella directory connessa. In alternativa, è possibile utilizzare l'[delete-account-assignment](#) AWS CLI.

 Note

Quando devi rimuovere il provisioning di utenti o gruppi di IAM Identity Center, devi prima [rimuovere qualsiasi assegnazione di set di autorizzazioni](#) dai tuoi utenti e gruppi prima di eliminare gli utenti e i gruppi.

Per rimuovere l'accesso di utenti e gruppi a un Account AWS

1. Apri la [console Centro identità IAM](#).
2. Nel riquadro di navigazione, in Autorizzazioni multiaccount, scegli. Account AWS
3. Nella Account AWS pagina 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 l'automazione per gestire tutti i passaggi tranne le operazioni solo su console.

1. Ottieni l'ID utente della persona a cui devi revocare l'accesso. Puoi utilizzare l'archivio di identità APIs per trovare l'utente in base al suo nome utente.

2. Aggiorna la politica di rifiuto per aggiungere l'ID utente dal passaggio 1 della politica 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.

Dopo aver eliminato una sessione utente, l'utente perderà immediatamente l'accesso al portale di AWS accesso. 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

In alternativa, è possibile utilizzare AWS CLI per creare, allegare politiche e assegnare set di autorizzazioni. Di seguito sono elencati i comandi per ogni passaggio:

- Per creare un set di autorizzazioni: [create-permission-set](#)
- Per allegare AWS Managed Policy a un set di autorizzazioni: [attach-managed-policy-to-permission-set](#)
- [Per allegare una politica gestita dal cliente a un set di autorizzazioni: - attach-customer-managed-policy to-permission-set](#)
- Per assegnare un set di autorizzazioni a un principale: [create-account-assignment](#)

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 [Creare 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.
Console di gestione AWS Esempio:

<https://console.aws.amazon.com/ec2/>

Per ulteriori informazioni, consulta [Imposta lo stato di inoltro per un accesso rapido a Console di gestione AWS](#).

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 [Taggare le risorse AWS IAM Identity Center](#).
 7. Controlla le selezioni effettuate, quindi scegli Crea.
3. Segui i passaggi indicati [Assegna l'accesso a utenti o gruppi 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.

Gestisci Account AWS con set di autorizzazioni

Un set di autorizzazioni è un modello che crei e gestisci e che definisce una raccolta di una o più [policy 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. [Creare, gestire ed eliminare set di autorizzazioni](#)

Creare 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 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 per Account AWS](#).

- 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 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 nuovi o esistenti a tali utenti.

Per informazioni, consulta [Assegna l'accesso a utenti o gruppi a Account AWS](#).

Argomenti

- [Autorizzazioni predefinite per AWS le politiche gestite](#)
- [Autorizzazioni personalizzate per politiche AWS gestite e gestite dai clienti](#)
- [Creare, gestire ed eliminare set di autorizzazioni](#)
- [Configura le proprietà del set di autorizzazioni](#)

Autorizzazioni predefinite per AWS le politiche gestite

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, vedere [Creare, gestire ed eliminare set di autorizzazioni](#).

Autorizzazioni personalizzate per politiche AWS gestite e gestite dai clienti

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. [Creare, gestire ed eliminare 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 il [AWS Policy Generator](#).

Quando distribuisce 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

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 con [Policy 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 con [Policy 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 le 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](#).

Note

Quando una policy gestita dal cliente è allegata a un set di autorizzazioni, il nome della policy non fa distinzione tra maiuscole e minuscole.

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, [AWS politiche gestite](#) non puoi concedere alcuna autorizzazione che superi le [Policy inline](#) 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.

Creare, gestire ed eliminare 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, consulta [Gestisci Account AWS con set di autorizzazioni](#).

Note

Puoi cercare e ordinare i set di autorizzazioni per nome nella console IAM Identity Center.

Tieni a mente le seguenti considerazioni quando crei i set di autorizzazioni:

- Istanza dell'organizzazione

Per utilizzare i set di autorizzazioni, devi utilizzare un'istanza Organization di IAM Identity Center. Per ulteriori informazioni, consulta [Istanze di organizzazione e account di IAM Identity Center](#).

- 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 gestione AWS 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 viene chiesto di accedere nuovamente. Per una sicurezza ottimale, è consigliabile non impostare la durata delle sessioni più del tempo necessario per eseguire 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 per Account AWS](#).

- 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 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 CloudFormation](#) per creare e assegnare set di autorizzazioni e assegnare utenti a tali set di autorizzazioni.

Argomenti

- [Creare un set di autorizzazioni](#)
- [Visualizzare e modificare un set di autorizzazioni](#)
- [Delega l'amministrazione dei set di autorizzazioni](#)
- [Utilizza le politiche IAM nei set di autorizzazioni](#)
- [Rimuovi i set di autorizzazioni in IAM Identity Center](#)
- [Elimina i set di autorizzazioni in IAM Identity Center](#)

Creare 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.

Note

Per utilizzare i set di autorizzazioni, dovrai utilizzare un'istanza Organization di IAM Identity Center. Per ulteriori informazioni, consulta [Istanze di organizzazione e account di IAM Identity Center](#).

Per creare un set di autorizzazioni

1. Apri la [console Centro identità IAM](#).
2. In Autorizzazioni multiaccount, 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. Scegli Next (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 politica 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.

 Note

I nomi dei set di autorizzazioni devono essere univoci all'interno dell'istanza di IAM Identity Center.

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 per Account AWS](#).
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 di inoltro per un accesso rapido a Console di gestione AWS](#).

 Note

L'URL dello stato di inoltro deve trovarsi all'interno di. Console di gestione AWS

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 [Taggare le risorse AWS IAM Identity Center](#).

6. Scegli Next (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 [Assegna l'accesso a utenti o gruppi a Account AWS](#).

Visualizzare e modificare un set di autorizzazioni

Puoi utilizzare i set di autorizzazioni per concedere agli utenti l'accesso a Account AWS. È possibile visualizzare e modificare un set di autorizzazioni con la AWS IAM Identity Center console. Puoi cercare e ordinare i set di autorizzazioni per nome nella console IAM Identity Center. Per ulteriori informazioni sui set di autorizzazioni e su come vengono utilizzati in IAM Identity Center, consulta [the section called "Set di autorizzazioni"](#).

I set di autorizzazioni non sono necessari per gestire l'accesso degli utenti alle applicazioni.

 Note

Per utilizzare i set di autorizzazioni, è necessario utilizzare un'istanza Organization di IAM Identity Center. Per ulteriori informazioni, consulta [Istanze di organizzazione e account di IAM Identity Center](#).

Visualizza le assegnazioni dei set di autorizzazioni

Utilizza questa procedura per visualizzare il set di autorizzazioni applicato nella AWS IAM Identity Center console.

All Account AWS where a permission set is provisioned

Per visualizzare tutte le assegnazioni per un set di autorizzazioni, utilizzare la procedura seguente:

1. Accedere a Console di gestione AWS e aprire la AWS IAM Identity Center console all'indirizzo <https://console.aws.amazon.com/singlesignon/>.
2. In Autorizzazioni per più account, scegli Set di autorizzazioni.
3. Nella pagina Set di autorizzazioni, seleziona il set di autorizzazioni che desideri visualizzare.
4. Una volta nella pagina dei set di autorizzazioni selezionati, nella scheda Account, puoi vedere gli account in cui viene utilizzato il set di autorizzazioni. Puoi selezionare l'account per vedere come viene fornito il set di autorizzazioni all'interno dell'account. È possibile [eliminare](#), modificare e allegare politiche al set di autorizzazioni.

All permission sets for an Account AWS

Per visualizzare tutte le assegnazioni per un set di autorizzazioni, utilizzare la procedura seguente:

1. Accedere a Console di gestione AWS e aprire la AWS IAM Identity Center console all'indirizzo <https://console.aws.amazon.com/singlesignon/>.
2. In Autorizzazioni per più account, scegli. Account AWS Seleziona l'account per il quale desideri visualizzare i set di autorizzazioni predisposti.
3. Una volta nella Account AWS pagina selezionata, nella scheda Set di autorizzazioni, è possibile visualizzare il diverso set di autorizzazioni assegnato al selezionato Account AWS. È possibile selezionare il collegamento ipertestuale del set di autorizzazioni per ulteriori informazioni sul set di autorizzazioni.

All applied permission sets to users and groups

Per visualizzare tutti i set di autorizzazioni assegnati a utenti o gruppi, utilizzare la procedura seguente:

1. Accedere Console di gestione AWS e aprire la AWS IAM Identity Center console all'indirizzo <https://console.aws.amazon.com/singlesignon/>.
2. Seleziona Utenti o Gruppi in Dashboard per visualizzare gli utenti o i gruppi di IAM Identity Center.
 - a. Una volta nella pagina Utenti, seleziona l'utente per il quale desideri visualizzare i set di autorizzazioni applicati. Quindi, seleziona la Account AWS scheda e la Account AWS sezione di accesso all'AWS account. Sarai in grado di visualizzare i set di autorizzazioni applicati e Account AWS quelli relativi all'utente selezionato.
 - b. Una volta nella pagina Gruppi, seleziona il gruppo a cui desideri visualizzare i set di autorizzazioni applicati. Quindi, seleziona la Account AWS scheda e la sezione Account AWS sotto la sezione di Account AWS accesso. Sarai in grado di visualizzare i set di autorizzazioni applicati e Account AWS per il gruppo selezionato.

Modificare un set di autorizzazioni

Utilizza questa procedura per modificare un [set di autorizzazioni](#) con la console IAM Identity Center. Puoi aggiungere o rimuovere set di autorizzazioni da utenti o gruppi.

1. Accedi Console di gestione AWS e apri la AWS IAM Identity Center console all'indirizzo <https://console.aws.amazon.com/singlesignon/>.
2. In Autorizzazioni per più account, scegli. Account AWS
3. Nella Account AWS pagina viene visualizzato un elenco ad albero della tua organizzazione. Seleziona il nome della persona Account AWS da cui desideri modificare il set di autorizzazioni.
4. Nella pagina Panoramica di Account AWS, in Utenti e gruppi assegnati, seleziona il nome utente o il nome del gruppo del set di autorizzazioni che desideri modificare. Quindi scegli Modifica set di autorizzazioni.
5. Apporta le modifiche desiderate al set di autorizzazioni, quindi scegli Salva modifiche.
6. Vai alla scheda Set di autorizzazioni e seleziona il set di autorizzazioni modificato di recente e scegli Aggiorna.
7. Nella pagina Aggiorna le autorizzazioni, scegli Aggiorna.

Delega 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 ad [Amazon Resource Names \(ARNs\) 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.

Note

Per utilizzare i set di autorizzazioni, è necessario utilizzare un'istanza Organization di IAM Identity Center. Per ulteriori informazioni, consulta [Istanze di organizzazione e account di IAM Identity Center](#).

Puoi utilizzare uno dei seguenti metodi per creare questi tipi di policy.

- (Consigliato) Crea [set di autorizzazioni](#) in IAM Identity Center, ciascuno 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

ARNs Le risorse IAM Identity Center distinguono tra maiuscole e minuscole.

Di seguito vengono illustrati i casi appropriati per fare riferimento al set di autorizzazioni e ai tipi di risorse dell'account IAM Identity Center.

Tipi di risorsa	ARN	Chiavi contestuali
PermissionSet	<code>arn:\${Partition}:sso::permissionSet/\${InstanceId}/\${PermissionSetId}</code>	<code>aws:ResourceTag/\${TagKey}</code>
Account	<code>arn:\${Partition}:sso::account/\${AccountId}</code>	Non applicabile

Utilizza le politiche IAM nei set di autorizzazioni

In [Creare 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 AWS È 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.

Considerazioni

- Per utilizzare i set di autorizzazioni, dovrai utilizzare un'istanza Organization di IAM Identity Center. Per ulteriori informazioni, consulta [Istanze di organizzazione e account di IAM Identity Center](#).
- Prima di assegnare il set di autorizzazioni con le politiche IAM, devi preparare il tuo account membro. Il nome di una policy IAM nel tuo account membro deve corrispondere 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.

Note

Quando una policy gestita dal cliente è allegata a un set di autorizzazioni, il nome della policy non fa distinzione tra maiuscole e minuscole.

- Le autorizzazioni concesse dalla politica non devono necessariamente corrispondere esattamente tra gli account.

Assegna 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 [Creare 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.

Rimuovi i set di autorizzazioni in IAM Identity Center

Puoi rimuovere un set di autorizzazioni dagli utenti e dai gruppi di IAM Identity Center nella console IAM Identity Center. Puoi anche rimuovere un set di autorizzazioni da un Account AWS. Per ulteriori informazioni sui set di autorizzazioni e su come vengono utilizzati in IAM Identity Center, consulta [Gestisci Account AWS con set di autorizzazioni](#).

Note

Per utilizzare i set di autorizzazioni, dovrai utilizzare un'istanza Organization di IAM Identity Center. Per ulteriori informazioni, consulta [Istanze di organizzazione e account di IAM Identity Center](#).

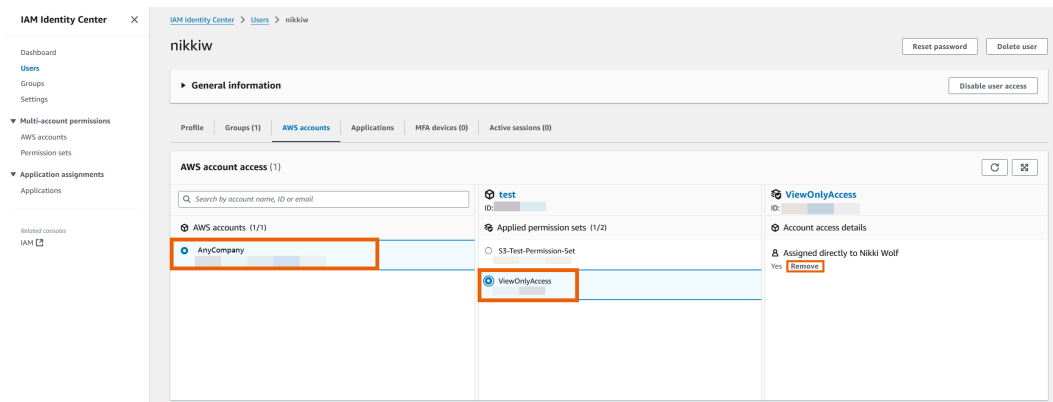
Remove permission set from a user

Rimuovi il set di autorizzazioni da un utente

Utilizza questa procedura per rimuovere un set di autorizzazioni da un utente con la console IAM Identity Center.

1. Accedi Console di gestione AWS e apri la AWS IAM Identity Center console all'indirizzo <https://console.aws.amazon.com/singlesignon/>.
2. In IAM Identity Center, seleziona Utenti.
3. Seleziona il nome utente dell'utente da cui desideri rimuovere un set di autorizzazioni.
4. Nella pagina dei dettagli dell'utente, seleziona la Account AWS scheda. In Account AWS accesso, seleziona il tuo Account AWS.
5. Nel riquadro di destra, vengono visualizzate le autorizzazioni applicate per l'utente selezionato. Seleziona il set di autorizzazioni che desideri rimuovere. In Dettagli di accesso all'account, seleziona Rimuovi.

- Viene visualizzata una finestra di dialogo che ti chiede se desideri rimuovere questo set di autorizzazioni. Selezionare Rimuovi.

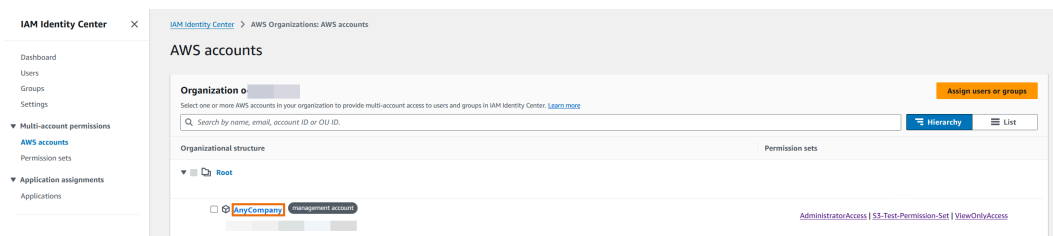


Remove permission set from a group

Rimuovi il set di autorizzazioni da un gruppo

Utilizza questa procedura per rimuovere un set di autorizzazioni da un gruppo con la console IAM Identity Center.

- Accedi Console di gestione AWS e apri la AWS IAM Identity Center console all'indirizzo <https://console.aws.amazon.com/singlesignon/>.
- In Autorizzazioni per più account, seleziona. Account AWS Seleziona il link al tuo account di gestione.



- Nella scheda Utenti e gruppi assegnati, seleziona il gruppo da cui desideri rimuovere il set di autorizzazioni, quindi seleziona Modifica set di autorizzazioni.
- Nella pagina Modifica set di autorizzazioni, deseleziona il set di autorizzazioni che desideri rimuovere, quindi seleziona Salva modifiche.

Remove permission set from an Account AWS

Utilizza questa procedura per rimuovere un set di autorizzazioni dalla Account AWS console IAM Identity Center.

1. Accedi Console di gestione AWS e apri la AWS IAM Identity Center console all'indirizzo <https://console.aws.amazon.com/singlesignon/>.
2. In Autorizzazioni per più account, seleziona. Account AWS Seleziona il nome del file Account AWS da cui desideri rimuovere il set di autorizzazioni.
3. Nella pagina Panoramica di Account AWS, scegli la scheda Set di autorizzazioni. Seleziona il set di autorizzazioni che desideri rimuovere. Quindi seleziona Rimuovi.
4. 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.

Elimina i set di autorizzazioni in IAM Identity Center

Prima di poter eliminare un set di autorizzazioni da IAM Identity Center, è necessario [rimuoverlo](#) da tutti coloro Account AWS che utilizzano il set di autorizzazioni. Per verificare l'accesso esistente di utenti e gruppi, consulta [Visualizzare e modificare un set di autorizzazioni](#).

Considerazioni

- Per utilizzare i set di autorizzazioni, dovrai utilizzare un'istanza Organization di IAM Identity Center. Per ulteriori informazioni, consulta [Istanze di organizzazione e account di IAM Identity Center](#).
- Se desideri revocare una sessione attiva del set di autorizzazioni, consulta. [the section called "Termina le sessioni attive per gli utenti della forza lavoro"](#)
- È necessario rimuovere i set di autorizzazioni e le assegnazioni delle applicazioni dagli utenti o dai gruppi che si desidera eliminare prima di eliminarli. Altrimenti, avrai set di autorizzazioni e applicazioni non assegnati e non utilizzati in IAM Identity Center.

Utilizza la seguente procedura per eliminare uno o più set di autorizzazioni in modo che non possano più essere utilizzati da nessuno Account AWS nell'organizzazione.

Important

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, vedere [Visualizzare e modificare un set di autorizzazioni](#).

Per eliminare un set di autorizzazioni da un Account AWS

1. Apri la [console Centro identità IAM](#).
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, digita 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, gli amministratori possono completare le seguenti attività di configurazione e gestione per controllare l'accesso degli utenti e la durata della sessione.

Operazione	Ulteriori informazioni
Gli amministratori possono impostare la durata massima delle sessioni utente quando accedono alle AWS risorse tramite IAM Identity Center.	Imposta la durata della sessione per Account AWS
Gli amministratori possono personalizzare la pagina di destinazione visualizzata dagli utenti dopo l'autenticazione corretta tramite IAM Identity Center.	Imposta lo stato di inoltro per un accesso rapido a Console di gestione AWS
Assicurati che gli utenti non abbiano più accesso alle AWS risorse quando le loro autorizzazioni vengono revocate.	Utilizza una politica Deny per revocare le autorizzazioni utente attive

Imposta la durata della sessione per Account AWS

Per ogni [set di autorizzazioni](#), è possibile 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 Centro identità IAM](#).
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 in cui Account AWS riassegnare automaticamente il set di autorizzazioni. 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. Scegli **Save changes** (Salva modifiche).
8. Nella parte superiore della Account AWS pagina, 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 di inoltro per un accesso rapido a Console di gestione AWS

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 Console di gestione AWS. È 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`**

Configura lo stato del relè

Utilizzare la procedura seguente per configurare l'URL dello stato di inoltro per un set di autorizzazioni.

1. Apri la [console Centro identità IAM](#).
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. Esempio:

`https://console.aws.amazon.com/ec2/`

Note

L'URL dello stato di inoltro deve trovarsi all'interno di. Console di gestione AWS

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. Scegli Save changes (Salva 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, consulta:

- 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-admin](#) sezione 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 utilizzando 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. [the section called “Termina le sessioni attive per gli utenti della forza lavoro”](#)

Politica di negazione

Puoi utilizzare una policy Deny con una condizione che User:ID 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.

JSON

```
{
  "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. È possibile automatizzare il processo di creazione di una politica di rifiuto ottenendo l'ID utente tramite una query nell'archivio di identità. APIs

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 SCPs, 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, nelle mappe di configurazione dei cluster Amazon EKS e AWS KMS nelle politiche chiave

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_ <i>permission-set-name_unique-suffix</i>	arn:aws:iam:: <i>aws-account-ID</i> :role/aws-reserved/sso.amazonaws.com/ <i>aws-region</i> /AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>

Se la tua fonte di identità in IAM Identity Center è ospitata su us-east-1, non è presente *aws-region* nell'ARN. Il nome completo e l'ARN del ruolo utilizzano il formato seguente:

Nome	ARN
AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>	arn:aws:iam:: <i>aws-account-ID</i> :role/aws-reserved/sso.amazonaws.com/AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>

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
<code>AWSReservedSSO_DatabaseAdministrator_ abcdef0123456789</code>	<code>arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_ abcdef0123456789</code>

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 i cluster Amazon Elastic Kubernetes Service (Amazon EKS) quando utilizzi per l'accesso al cluster. `aws-auth ConfigMap`
- In una politica basata sulle risorse per una chiave (`.`). AWS Key Management Service AWS KMS Questa politica viene anche definita politica chiave.

Note

Ti consigliamo di utilizzare le [voci di accesso di Amazon EKS](#) per gestire l'accesso ai tuoi cluster Amazon EKS. Ciò consente di utilizzare le autorizzazioni IAM per gestire i principali che hanno accesso a un cluster Amazon EKS. Utilizzando le voci di accesso di Amazon EKS, puoi utilizzare un principale IAM con autorizzazioni Amazon EKS per riottenere l'accesso a un cluster senza contattare. Supporto

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 con le

autorizzazioni per aggiornare la policy `aws-auth ConfigMap` o la policy AWS KMS chiave, contatta Supporto per riottenere l'accesso a tali risorse.

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 i cluster Amazon EKS che utilizzano **`aws-auth ConfigMap`** e AWS KMS: includono un ruolo creato in IAM.

Se fai riferimento al ruolo ARNs 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 che crei 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'Conditionelemento 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.

JSON

```
{  
  "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 tiene 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 IAM Identity Center APIs, consulta la Guida di riferimento [CreateInstanceAccessControlAttributeConfiguration](#) all'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	Operazione	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	• Manage your identity source

Fase	Operazione	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 <code>Optional</code> sezioni del tutorial relative al tuo IdP specifico.	• Tutorial sulle fonti di identità di IAM Identity Center
	• 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.	• Esegui il provisioning di utenti e gruppi da un provider di identità esterno utilizzando SCIM • Attributi del provider di identità esterno supportati

Fase	Operazione	Documentazione di riferimento
	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 tra IAM Identity Center e Microsoft AD
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 <code>aws:PrincipalTag/key</code> condizione.	Crea politiche di autorizzazione per ABAC in IAM Identity Center

Fase	Operazione	Documentazione di riferimento
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 a utenti o gruppi 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, vedere [Controllo 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 AWS pagina 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 tra IAM Identity Center e Microsoft AD](#)

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 SCIM 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 sulle fonti di identità di IAM Identity Center](#) 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, consulta [Attributi 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 il controllo degli accessi basato sugli attributi \(ABAC\), devi prima abilitarlo nella pagina Impostazioni della console IAM Identity Center o nell'API IAM Identity Center.](#) Indipendentemente dall'origine dell'identità, puoi sempre configurare gli attributi utente dall'Identity Store per utilizzarli in ABAC. Nella console, puoi farlo accedendo alla scheda Attributi per il controllo degli accessi nella pagina Impostazioni. Se utilizzi un provider di identità esterno (IdP) come origine dell'identità, hai anche la possibilità di ricevere gli attributi dall'IdP esterno nelle asserzioni SAML. In questo caso, è necessario configurare l'IdP esterno per inviare gli attributi desiderati. Se un attributo di un'asserzione SAML è definito anche come attributo ABAC in IAM Identity Center, IAM Identity Center invierà il valore dal suo Identity Store come [tag di sessione](#) al momento dell'accesso a un Account AWS.

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.

Argomenti

- [Abilita gli attributi per il controllo degli accessi](#)
- [Seleziona gli attributi per il controllo degli accessi](#)
- [Disabilitazione di attributi per il controllo degli accessi](#)

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.

Se la tua istanza IAM Identity Center è stata creata prima di dicembre 2020 e prevedi di abilitare ABAC al suo interno, devi disporre della `iam:UpdateAssumeRolePolicy` policy associata al ruolo amministrativo di IAM Identity Center, indipendentemente dal fatto che nel tuo account siano stati creati set di autorizzazioni.

Per abilitare gli attributi per il controllo degli accessi

1. Apri la [console Centro identità IAM](#).
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 gli attributi per il controllo degli accessi

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 Centro identità IAM](#).
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.

Key ⓘ	Value (optional) ⓘ	Remove
Department	\${path:enterprise.department}	✕
CostCenter	\${path:enterprise.costCenter}	✕
Add new key	Add new value	

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 CostCentera 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 in [Mappature degli attributi tra IAM Identity Center e la directory External Identity Provider](#). 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. Scegli Save changes (Salva 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 and/or di autorizzazioni, 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 Centro identità IAM](#).
2. Seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli la scheda Attributi per il controllo dell'accesso, quindi scegli Gestisci attributi.
4. Nella pagina Gestisci gli attributi per il controllo degli accessi, scegli Disabilita.
5. Nella finestra di dialogo Disabilita gli attributi per il controllo degli accessi, rivedi le informazioni e, quando sei pronto **DISABLE**, inserisci, quindi scegli Conferma.

 Important

Questo passaggio elimina tutti gli attributi e interrompe l'uso degli attributi per il controllo degli accessi durante la federazione, Account AWS indipendentemente dalla presenza di attributi nelle asserzioni SAML di un provider di origini di identità esterno.

Crea politiche di autorizzazione per ABAC in IAM Identity Center

È possibile creare politiche di autorizzazione che determinano chi può accedere alle AWS risorse in base al valore dell'attributo configurato. Quando abiliti ABAC e specifichi gli attributi, IAM Identity Center passa 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 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 durante la 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.

JSON

```
{
  "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:PrincipalTag 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](#).

Comprensione dei ruoli collegati ai servizi in IAM Identity Center

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 la sezione [Ruoli collegati ai AWS Organizations 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 [Configurare 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](#).

 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.

Configurazione e utilizzo del portale di AWS accesso

Il portale di AWS accesso collega la forza lavoro Account AWS e le applicazioni cloud tramite IAM Identity Center. Gli amministratori configurano il portale e gestiscono l'accesso degli utenti, mentre gli utenti finali effettuano l'accesso una sola volta per accedere senza problemi a tutte le risorse autorizzate.

Il portale di AWS accesso fornisce l'accesso Single Sign-On a:

- Account AWS nella tua organizzazione.
- AWS applicazioni gestite come Amazon Quick e Kiro.
- applicazioni cloud come Office 365, Concur, Salesforce e altre.

Quando gli utenti accedono al portale, trovano le applicazioni Account AWS e le applicazioni a cui sono autorizzati ad accedere senza ulteriori accessi.

Guida introduttiva al portale di AWS accesso

Per gli amministratori:

È necessario l'accesso amministrativo all'[istanza dell'organizzazione o all'istanza dell'account](#) di IAM Identity Center per configurare il portale di AWS accesso e gestire l'accesso degli utenti.

1. Facoltativamente, personalizza l'URL del portale di AWS accesso.
2. Assegna l'accesso utente alle applicazioni Account AWS e agli utenti. AWS Le risorse assegnate vengono visualizzate nel portale.

Per gli utenti finali:

L'amministratore deve aver completato la configurazione del portale di AWS accesso e fornito all'utente l'URL del portale e le credenziali di accesso.

1. Richiedete l'URL del portale all'amministratore (in genere `https://your-company.awsapps.com/start`).
2. Accedi utilizzando le credenziali fornite dall'amministratore.

3. Accedi alle tue risorse nel tuo portale.

Configura il portale di AWS accesso

In qualità di amministratore, puoi personalizzare il portale di AWS accesso per soddisfare le esigenze della tua organizzazione e garantire che gli utenti possano accedere facilmente alle risorse autorizzate.

Cosa puoi configurare

AWS attivazione del portale di accesso: configura l'accesso iniziale degli utenti al portale di AWS accesso, inclusa l'attivazione delle credenziali utente e i processi di accesso per la prima volta.

URL del portale di AWS accesso personalizzato (opzionale): Personalizza l'URL del portale di AWS accesso dell'organizzazione dal formato predefinito (`d-xxxxxxxxx.awsapps.com/start`) a un sottodominio più riconoscibile (`. your-company.awsapps.com/start`).

Prima di iniziare

Assicurati di avere accesso amministrativo a IAM Identity Center, verifica che IAM Identity Center sia configurato come [istanza dell'organizzazione o come istanza](#) di [account](#) e pianifica il nome di sottodominio personalizzato (si tratta di una configurazione unica che non può essere modificata in seguito).

Una volta configurato, gli utenti possono accedere al portale di AWS accesso utilizzando l'URL personalizzato e seguire il processo di attivazione che hai stabilito per la tua organizzazione.

Argomenti

- [Attivazione del portale di AWS accesso per gli utenti di IAM Identity Center per la prima volta](#)
- [Personalizzazione dell'URL del portale di AWS accesso](#)
- [Conferma che gli utenti possano accedere al portale di AWS accesso](#)

Attivazione del portale di AWS accesso per gli utenti di IAM Identity Center per la prima volta

Se è la prima volta che tenti di accedere al portale di AWS accesso, controlla la tua e-mail per ricevere 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, 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 in [Accedere al portale di AWS accesso](#).

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 si modifica l'URL del portale di AWS accesso, non è possibile modificarlo in un secondo momento.

Per personalizzare l'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 di sottodominio desiderato e scegli Salva.

Ora puoi accedere alla AWS Console tramite il tuo portale di AWS accesso con il tuo URL personalizzato.

Conferma che gli utenti possano accedere al portale di AWS accesso

I seguenti passaggi consentono all'amministratore di IAM Identity Center di confermare che l'utente IAM Identity Center possa accedere al portale di AWS accesso e accedere a Account AWS.

Accedi al portale di AWS accesso

1. Effettua una delle seguenti operazioni per accedere a Console di gestione AWS.
 - Nuovo utente AWS (utente root): accedi come proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS e-mail. 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 Centro identità IAM](#).
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.

6. Nella scheda Account, individua il tuo Account AWS ed espandilo.
7. Vengono visualizzati i ruoli a tua disposizione. Ad esempio, se all'utente 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.
8. 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 AWS nell'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, consulta [Assegna l'accesso a utenti o gruppi 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 Console di gestione AWS 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. Conserva le credenziali dell'utente root e utilizzale 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.

Utilizza il portale di accesso AWS

È possibile avviare più applicazioni scegliendo la scheda Account AWS o l'applicazione nel portale. La presenza di icone delle applicazioni nel portale di AWS accesso indica 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.

Come utilizzare il portale di accesso AWS

Per utilizzare il portale di AWS accesso:

1. Richiedi l'URL del portale all'amministratore (in genere si presenta così `https://your-company.awsapps.com/start`).
2. Accedi utilizzando le credenziali fornite dall'amministratore.
3. Scegliete gli account e le applicazioni del portale a cui desiderate accedere.

L'amministratore controlla ciò che vedi nel portale in base al tuo ruolo e alle tue autorizzazioni. Contatta il tuo 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

- [Accedere al portale di AWS accesso](#)
- [Reimpostazione della password utente del portale di AWS accesso](#)
- [Ottenere le credenziali utente di IAM Identity Center per o AWS CLI AWS SDKs](#)
- [Creazione di collegamenti rapidi alle destinazioni Console di gestione AWS](#)
- [Registrazione del dispositivo per l'MFA](#)
- [Visualizzazione e fine della sessione attiva](#)

Accedere al portale di AWS accesso

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. Di seguito vengono descritti come accedere al portale di AWS accesso, suggerimenti per l'accesso e come disconnettersi dal AWS portale di accesso.

Prerequisiti

IAM Identity Center deve essere abilitato per utilizzare il portale di AWS accesso. Per ulteriori informazioni, consulta [Abilita IAM Identity Center](#).

 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.

Accedi al portale di AWS accesso

Per accedere al portale di AWS accesso

1. Nella finestra del browser, incolla l'URL di accesso che ti è stato fornito e scegli Invio. L'URL è simile a `d-xxxxxxxxx.awsapps.com/start` *o* `your_subdomain.awsapps.com/start`. Consigliamo di inserire subito nei segnalibri questo link al portale in modo da potervi accedere rapidamente in un secondo momento.
2. Accedi utilizzando le credenziali di accesso aziendali standard.

 Note

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

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

 Note

I codici di verifica di solito vengono inviati via e-mail, ma il metodo di consegna può variare. Consulta l'amministratore per i dettagli.

3. Una volta effettuato l'accesso, puoi accedere a qualsiasi Account AWS applicazione visualizzata nel portale.

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 finché si utilizza 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 del portale di AWS accesso

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 [Console di gestione AWS](#), 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 AD](#) come 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 essere connesso Active Directory.

- Se la fonte dell'identità è una directory di IAM Identity Center, consulta [Requisiti 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 tua 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 o AWS CLI AWS SDKs

Puoi accedere ai AWS servizi in modo programmatico utilizzando AWS Command Line Interface o i AWS Software Development Kit (SDKs) 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, in AWS CLI o AWS SDKs 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 descritte in questo argomento per avviare l'accesso a. AWS CLI [Per informazioni su AWS CLI, consulta la Guida per l'AWS Command Line Interface utente.](#)

Se si utilizza AWS SDKs per accedere ai AWS servizi a livello di programmazione, seguendo le procedure riportate in questo argomento viene inoltre stabilita direttamente l'autenticazione per. AWS SDKs Per informazioni su AWS SDKs, consulta la [AWS SDKs and Tools](#) Reference Guide.

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 effettui l'accesso.

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, consulta [Nozioni di base sul Centro identità IAM](#).
- 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 a utenti o gruppi 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 per Account AWS](#).

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 `aws configure sso`. AWS CLI È possibile utilizzare questo comando per accedere automaticamente a qualsiasi ruolo associato a qualsiasi set di autorizzazioni a cui si è assegnati 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 AWS nell'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 a utenti o gruppi 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 `PowerUserAccess` autorizzazioni 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 PowerShell oppure, 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, è necessario copiare e incollare 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 AWS nell'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 a utenti o gruppi a Account AWS](#).

3. Nella finestra di dialogo Ottieni credenziali, scegli macOS e Linux, Windows PowerShell, o la 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 strumenti AWS SDKs 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 per creare in 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 Console di gestione AWS

I collegamenti di scelta rapida creati nel portale di AWS accesso indirizzano gli utenti di IAM Identity Center verso una destinazione specifica nel Console di gestione AWS, 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 Console di gestione AWS (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 contenuto nel collegamento di scelta rapida Console di gestione AWS specificato. 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 di inoltro per un accesso rapido a Console di gestione AWS](#)
- Console di gestione AWS 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 account IDs e i nomi 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 è possibile concedere un nuovo accesso con collegamenti di scelta rapida. I collegamenti 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 Console di gestione AWS 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:

IPv4 punto finale:

```
https://[your_subdomain].awsapps.com/start/#/console?  
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination]
```

Endpoint dual-stack

```
https://[identity_center_instance_id].portal.[region].app.aws/#/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:

- IPv4 endpoint: `https://example.awsapps.com/start/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- Endpoint dual-stack: `https://ssoins-1234567890abcdef.portal.us-east-1.app.aws/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- () punto finale:AWS GovCloud (US) Region IPv4 `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`
- (AWS GovCloud (US) Region) Endpoint dual-stack: `https://ssoins-1234567890abcdef.portal.us-gov-west-1.app.aws/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`

Registrazione del dispositivo per l'MFA

Per gli utenti della directory Identity Center, utilizzare la seguente procedura all'interno del portale di AWS accesso per registrare il nuovo dispositivo per l'autenticazione a più fattori (MFA).

Important

L'MFA in IAM Identity Center non è attualmente supportata per i provider di [identità esterni](#).

Prima di iniziare

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](#)

Registra il tuo dispositivo

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 di autenticazione MFA. 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.

Visualizzazione e fine della sessione attiva

È possibile utilizzare il portale di AWS accesso per visualizzare l'elenco delle sessioni attive e, se necessario, terminare una o più sessioni.

Termina la sessione attiva utilizzando il portale di AWS accesso

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 Sicurezza.
3. Nella pagina Sicurezza, il numero tra parentesi accanto a Sessioni attive indica quante sessioni attive hai. Seleziona la casella di controllo accanto a ogni sessione che desideri terminare, quindi scegli Termina sessioni.

Tip

Per la sessione utente in background, puoi cercare le sessioni in base all'Amazon Resource Name (ARN) del processo che utilizza la sessione. Nell'elenco Tipo di sessione, scegli Sessioni utente in background, quindi inserisci l'ARN del lavoro nella casella di ricerca.

È possibile terminare solo le sessioni attive caricate. Se hai molte sessioni, scegli Carica altre sessioni attive per visualizzare sessioni aggiuntive.

4. Seleziona la casella di controllo accanto a ogni sessione che desideri terminare, quindi scegli Termina sessioni.
5. Viene visualizzata una finestra di dialogo che conferma che state terminando le sessioni attive. Esamina le informazioni e, se vuoi continuare, digita `confirm`, quindi scegli Termina sessioni.
6. Verrai reindirizzato all'elenco delle sessioni attive. Viene visualizzato un messaggio di notifica verde per indicare che le sessioni selezionate sono state terminate correttamente.

Utilizzo di IAM Identity Center su più Regioni AWS

Questo argomento spiega come utilizzarlo AWS IAM Identity Center su più piattaforme Regioni AWS. Scopri come replicare l'istanza in altre regioni, gestire l'accesso e le sessioni della forza lavoro, distribuire applicazioni e mantenere l'accesso all'account durante le interruzioni del servizio.

Quando abiliti un'istanza organizzativa di IAM Identity Center, scegli una singola regione Regione AWS (principale). Puoi replicare questa istanza in altre Regioni AWS se soddisfa determinati prerequisiti. IAM Identity Center replica automaticamente le identità della forza lavoro, i set di autorizzazioni, le assegnazioni di utenti e gruppi, le sessioni e altri metadati dalla regione principale alle regioni aggiuntive scelte.

Vantaggi del supporto multiregionale

La replica di IAM Identity Center ad altri Regioni AWS offre due vantaggi chiave:

- Maggiore resilienza di Account AWS accesso: la tua forza lavoro può accedere ai propri Account AWS servizi anche se l'istanza IAM Identity Center subisce un'interruzione del servizio nella sua regione principale. Questo vale per l'accesso con le autorizzazioni fornite prima dell'interruzione.
- Maggiore flessibilità nella scelta delle regioni di distribuzione per le applicazioni AWS gestite: è possibile distribuire applicazioni AWS gestite nelle regioni preferite per soddisfare i requisiti di residenza dei dati delle applicazioni e migliorare le prestazioni grazie alla vicinanza agli utenti. Le applicazioni distribuite in altre regioni accedono alle identità della forza lavoro replicate localmente per prestazioni e affidabilità ottimali.

Prerequisiti e considerazioni

Prima di replicare l'istanza di IAM Identity Center, assicurati che siano soddisfatti i seguenti requisiti:

- Tipo di istanza: l'istanza IAM Identity Center deve essere un'[istanza dell'organizzazione](#). Il supporto multiregionale non è disponibile nelle [istanze degli account](#).
- Origine dell'identità: l'istanza di IAM Identity Center deve essere connessa a un provider di identità esterno (IdP), ad esempio. [Okta](#) Il supporto multiregionale non è disponibile per le istanze che utilizzano [Active Directory o la directory Identity Center come origine dell'identità](#).
- AWS Regioni: il supporto multiregionale è disponibile nelle [regioni commerciali abilitate per impostazione predefinita](#) in. Account AWS Le regioni opt-in non sono attualmente supportate.

- Tipo di chiave KMS per la crittografia a riposo: l'istanza di IAM Identity Center deve essere configurata con una chiave KMS multiregionale [gestita dal cliente](#). La chiave KMS deve trovarsi nello stesso AWS account di IAM Identity Center. Per ulteriori informazioni, consulta [Implementazione di chiavi KMS gestite dal cliente in AWS IAM Identity Center](#).
- AWS compatibilità gestita delle applicazioni: consulta la tabella delle applicazioni [the section called “Applicazioni che è possibile utilizzare con IAM Identity Center”](#) per confermare i seguenti due requisiti applicativi:
 - Tutte le applicazioni AWS gestite utilizzate dall'organizzazione devono supportare IAM Identity Center, configurato con una chiave KMS gestita dal cliente.
 - Le applicazioni AWS gestite che desideri distribuire in regioni aggiuntive devono supportare questo tipo di implementazione.
- Compatibilità con IdP esterni: per sfruttare appieno il supporto multiregionale, l'IdP esterno deve supportare il Multiple Assertion Consumer Service (ACS). URLS Si tratta di una funzionalità SAML supportata da,, IdPs , eOkta. Microsoft Entra ID PingFederate PingOne JumpCloud

Se utilizzi un IdP che non supporta più ACS URLs, ad esempio, ti consigliamo di collaborare con il fornitore del tuo IdP per abilitare questa funzionalità. Google Workspace Per le opzioni disponibili senza più URLs ACS, consulta e. [the section called “Utilizzo di applicazioni AWS gestite senza più ACS URLs”](#) [the section called “Account AWS resilienza di accesso senza più ACS URLs”](#)

Scelta di una regione aggiuntiva

Quando scegli una regione aggiuntiva tra le regioni commerciali abilitate per impostazione predefinita, considera questi fattori:

- Requisiti di conformità: se devi eseguire applicazioni AWS gestite che accedono a set di dati limitati a una regione specifica per motivi di conformità, scegli la regione in cui risiedono i set di dati.
- Ottimizzazione delle prestazioni: se la residenza dei dati non è un fattore, seleziona la regione più vicina agli utenti dell'applicazione per ottimizzare la loro esperienza.
- Supporto per le applicazioni: verifica che le AWS applicazioni richieste siano disponibili nella regione prescelta.
- Account AWS resilienza di accesso: per garantire la continuità dell'accesso a Account AWS s, scegli una regione geograficamente distante dalla regione principale dell'istanza di IAM Identity Center.

 Note

IAM Identity Center ha una quota sul numero di Regioni AWS. Per ulteriori informazioni, consulta [the section called "Quote aggiuntive"](#).

Replica IAM Identity Center in un'altra regione

Se il tuo ambiente soddisfa i [prerequisiti](#), ad esempio la configurazione di IAM Identity Center con una chiave KMS gestita dal cliente in più regioni, completa i seguenti passaggi per replicare l'istanza di IAM Identity Center in una regione aggiuntiva. La regione principale continua a funzionare normalmente durante e dopo questi passaggi.

Passaggio 1: creare una chiave di replica nella regione aggiuntiva

Prima di replicare IAM Identity Center in una regione, devi prima creare una chiave di replica della chiave KMS gestita dal cliente in quella regione e configurare la chiave di replica con le autorizzazioni richieste per le operazioni di IAM Identity Center. [Per istruzioni sulla creazione di chiavi di replica multiregionali, consulta Creazione di chiavi di replica multiregionali.](#)

L'approccio consigliato per le autorizzazioni delle chiavi KMS consiste nel copiare la policy chiave dalla chiave primaria, che concede le stesse autorizzazioni già stabilite per IAM Identity Center nella regione primaria. In alternativa, è possibile definire politiche chiave specifiche per regione, sebbene questo approccio aumenti la complessità della gestione delle autorizzazioni tra le regioni e possa richiedere un ulteriore coordinamento per l'aggiornamento delle politiche in futuro.

 Note

AWS KMS non sincronizza la politica delle chiavi KMS tra le regioni della chiave KMS multiregionale. Per mantenere sincronizzata la politica delle chiavi KMS tra le regioni chiave KMS, dovrai applicare le modifiche in ciascuna regione singolarmente.

Passaggio 2: aggiungi la regione in IAM Identity Center

L'aggiunta di una regione in IAM Identity Center attiva la replica automatica dei dati di IAM Identity Center in quella regione. La replica è asincrona con eventuale coerenza. Le seguenti schede

forniscono istruzioni per eseguire questa operazione nella modalità e. Console di gestione AWS AWS CLI

Console

Per aggiungere una regione

1. Apri la [console Centro identità IAM](#).
2. Nel pannello di navigazione scegli Impostazioni.
3. Scegliere la scheda Management (Gestione),
4. Nella sezione Regioni per IAM Identity Center, scegli Aggiungi regione.
5. Nella sezione Regioni AWS Disponibile per la replica, scegli la tua preferita Regione AWS. Se la regione non appare nell'elenco, non è disponibile per la replica perché la chiave KMS non è stata replicata lì. Per ulteriori informazioni, consulta [the section called "Implementazione di chiavi KMS gestite dal cliente"](#).
6. Scegli Aggiungi regione.
7. Nella sezione Regioni per IAM Identity Center, monitora lo stato della regione. Utilizza il pulsante Aggiorna (freccia circolare) per verificare lo stato più recente della regione, se necessario. Una volta completata la replica, procedi al passaggio 2.

AWS CLI

Per aggiungere una regione

```
aws sso-admin add-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

Per verificare lo stato attuale della regione

```
aws sso-admin describe-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

Quando lo stato della regione è ATTIVO, puoi procedere al passaggio 2.

La durata della replica iniziale in una regione aggiuntiva dipende dalla quantità di dati nell'istanza di IAM Identity Center. Le modifiche incrementali successive vengono replicate in pochi secondi nella maggior parte dei casi.

Fase 3: Aggiornare la configurazione dell'IdP esterno

Segui il tutorial per il tuo IdP esterno [Tutorial sulle fonti di identità](#) per i seguenti passaggi:

Fase 3.a: Aggiungi l'Assertion Consumer Service (ACS) URLs al tuo IdP esterno

Questo passaggio consente l'accesso diretto a ciascuna regione aggiuntiva ed è necessario per abilitare l'accesso alle applicazioni AWS gestite distribuite in tali regioni e per l'accesso a noi tramite tali regioni. Account AWS Per sapere dove trovare l'URLsACS, vedi. [Endpoint ACS primari e aggiuntivi Regioni AWS](#)

Fase 3.b (facoltativo): rendere Portale di accesso AWS disponibile il file nel portale IdP esterno

Rendila disponibile Portale di accesso AWS nella regione aggiuntiva come app per segnalibri nel portale IdP esterno. Le app per i segnalibri contengono solo un link (URL) alla destinazione desiderata e sono simili ai segnalibri del browser. Puoi trovarle Portale di accesso AWS URLs nella console selezionando Visualizza tutto Portale di accesso AWS URLs nella sezione Regioni per IAM Identity Center. Per ulteriori informazioni, consulta [the section called “AWS accedere agli endpoint del portale primari e aggiuntivi Regioni AWS”](#).

IAM Identity Center supporta l'SSO SAML avviato da IdP in ogni regione aggiuntiva, ma l'esterno in IdPs genere lo supporta con un solo URL ACS. Per garantire la continuità, consigliamo di mantenere l'URL ACS della regione principale in uso per l'SSO SAML avviato dall'IdP e di affidarsi alle app di segnalibri e ai segnalibri del browser per accedere a regioni aggiuntive.

Fase 4: Conferma gli elenchi di indirizzi consentiti per firewall e gateway

[Esamina gli elenchi di domini consentiti nei firewall o nei gateway e aggiornali in base agli elenchi di consentiti documentati.](#)

Fase 5: Fornisci informazioni ai tuoi utenti

Fornisci agli utenti informazioni sulla nuova configurazione, incluso l' Portale di accesso AWS URL nella regione aggiuntiva e su come utilizzare le aree aggiuntive. Consulta le seguenti sezioni per i dettagli pertinenti:

- [the section called “Accesso alla forza lavoro tramite una regione aggiuntiva”](#)
- [the section called “Failover verso un'altra regione per l'accesso Account AWS ”](#)
- [the section called “Distribuzione e gestione di applicazioni su più Regioni AWS”](#)

Modifiche alla regione oltre all'aggiunta della prima regione

Puoi aggiungere e rimuovere altre regioni. La regione primaria può essere rimossa solo eliminando l'intera istanza di IAM Identity Center. Per ulteriori informazioni sulla rimozione di una regione, consulta [the section called “Rimuovi una regione da IAM Identity Center”](#).

Non è possibile promuovere una regione aggiuntiva come principale o retrocedere la regione principale come aggiuntiva.

Quali dati vengono replicati?

IAM Identity Center replica i seguenti dati:

Dati	Origine e destinazione della replica
Identità della forza lavoro (utenti, gruppi, appartenenze ai gruppi)	Dalla regione principale alle regioni aggiuntive
Set di autorizzazioni e relative assegnazioni a utenti e gruppi	Dalla regione principale alle regioni aggiuntive
Configurazione (ad esempio impostazioni SAML IdP esterne)	Dalla regione principale alle regioni aggiuntive
Metadati dell'applicazione e assegnazioni delle applicazioni a utenti e gruppi	Dalla regione IAM Identity Center connessa di un'applicazione alle altre regioni abilitate
Emittenti di token affidabili	Dalla regione principale alle regioni aggiuntive
Sessioni	Dalla regione di origine della sessione alle altre regioni abilitate

 Note

IAM Identity Center non replica i dati archiviati nelle applicazioni AWS gestite. Inoltre, non modifica l'impronta regionale della distribuzione di un'applicazione. Ad esempio, se la tua istanza IAM Identity Center si trova negli Stati Uniti orientali (Virginia settentrionale) e Amazon Redshift è distribuito nella stessa regione, la replica di IAM Identity Center negli Stati Uniti occidentali (Oregon) non influisce sulla regione di distribuzione di Amazon Redshift e sui dati che archivia.

Considerazioni:

- Identificatori di risorse globali nelle regioni abilitate: utenti, gruppi, set di autorizzazioni e altre risorse hanno gli stessi identificatori in tutte le regioni abilitate.
- La replica non influisce sui ruoli IAM assegnati: i ruoli IAM esistenti forniti in base alle assegnazioni dei set di autorizzazioni vengono utilizzati durante l'accesso all'account da qualsiasi regione abilitata.

Accesso alla forza lavoro tramite una regione aggiuntiva

Questa sezione spiega come la forza lavoro può accedere a Portale di accesso AWS, Account AWS e alle applicazioni dopo aver abilitato IAM Identity Center in più regioni.

Portale di accesso AWS In una regione aggiuntiva vengono visualizzati Account AWS i messaggi e le applicazioni a cui la forza lavoro ha accesso nello stesso modo in cui nella regione principale. La tua forza lavoro può accedere Portale di accesso AWS in un'altra regione tramite un collegamento diretto all'endpoint del portale regionale (ad esempio <https://ssoins-111111h2222j33pp.eu-west-1.portal.amazonaws.com>) o tramite un'app [di segnalibri](#) configurata nell'IdP esterno.

Puoi utilizzare l' Portale di accesso AWS endpoint in una regione aggiuntiva per autorizzarne l'accesso APIs come utente AWS CLI IAM Identity Center. Questa funzionalità funziona allo stesso modo della regione principale. Tuttavia, le autorizzazioni CLI non vengono replicate tra le regioni abilitate. Pertanto, è necessario autorizzare la CLI in ciascuna regione singolarmente.

Sessioni utente su più sessioni Regioni AWS

IAM Identity Center replica le sessioni utente dalla regione di origine alle altre regioni abilitate. La revoca della sessione e la disconnessione in una regione vengono replicate anche nelle altre regioni.

Revoca della sessione da parte degli amministratori di IAM Identity Center

Gli amministratori di IAM Identity Center possono revocare le sessioni utente in regioni aggiuntive. Poiché le sessioni vengono replicate tra le regioni, in condizioni normali è sufficiente revocare una sessione in una singola regione e consentire a IAM Identity Center di replicare la modifica nelle altre regioni abilitate. Se la regione principale di IAM Identity Center presenta un'interruzione, gli amministratori possono eseguire questa operazione in regioni aggiuntive.

Portale di accesso AWS endpoint primari e aggiuntivi Regioni AWS

Se devi cercare il portale di AWS accesso URLs per le regioni abilitate, procedi nel seguente modo:

1. Apri la [console Centro identità IAM](#).
2. Nel pannello di navigazione scegli Impostazioni.
3. Scegliere la scheda Management (Gestione),
4. Nella sezione Regioni per IAM Identity Center, scegli Visualizza tutto il portale di AWS accesso URLs.

La tabella seguente specifica gli Portale di accesso AWS endpoint nelle regioni primarie e aggiuntive di un'istanza di IAM Identity Center.

Portale di accesso AWS endpoint	Regione principale	Regione aggiuntiva	Modello ed esempio di URL
Classico IPv4 solo ¹	Sì	No	Pattern: <code>https://[Identity Store ID].awsapps.com/start</code> Esempio: <code>https://d-12345678.awsapps.com/start</code>
Alias personalizzato solo 1 IPv4	Sì (facoltativo)	No	Pattern: <code>https://[custom alias].awsapps.com/start</code>

Portale di accesso AWS endpoint	Regione principale	Regione aggiuntiva	Modello ed esempio di URL
			Esempio: <code>https://mycompany.awsapps.com/start</code>
Alternativa solo 2 IPv4	Sì	Sì	Pattern: <code>https://[Identity Center instance ID].[Region].portal.amazonaws.com</code> Esempio: <code>https://soins-11111h2222j33pp.eu-west-1.portal.amazonaws.com</code>
Dual-stack 2	Sì	Sì	Pattern: <code>https://[Identity Center instance ID].portal.[Region].app.aws</code> Esempio: <code>https://soins-11111h2222j33pp.portal.eu-west-1.app.aws</code>

¹ In altre regioni, l'alias personalizzato non è supportato e il dominio `awsapps.com` principale non è disponibile.

² IPv4 Solo gli endpoint alternativi e dual-stack del portale non hanno la parte finale nell'URL. `/start`

Endpoint Assertion Consumer Service (ACS) negli endpoint primari e aggiuntivi Regioni AWS

Se devi cercare gli ACS URLs o scaricarli come parte dei metadati SAML, segui questi passaggi:

1. Apri la [console Centro identità IAM](#).

2. Nel pannello di navigazione scegli Impostazioni.
3. Scegli la scheda Identity source.
4. Nel menu a discesa Azioni, scegli Gestisci l'autenticazione.
5. La sezione dei metadati del fornitore di servizi mostra l'URL Portale di accesso AWS e l'URL ACS per ogni regione abilitata. IPv4-only e dual-stack URLs vengono visualizzati in schede separate. Se il tuo IdP supporta il caricamento di un file di metadati SAML, puoi scegliere Scarica il file di metadati per scaricare il file di metadati SAML con tutti gli ACS. URLs Se il tuo IdP non supporta il caricamento di un file di metadati o preferisci aggiungere ACS URLs singolarmente, puoi copiare un singolo elemento URLs dalla tabella nella console oppure scegliere Visualizza URLs ACS e quindi Copia tutto. URLs Conserva l'URL ACS già configurato per la regione principale per garantire che il single sign-on SAML avviato dal provider di servizi dalla regione principale rimanga funzionante.

La tabella seguente specifica gli endpoint SAML Assertion Consumer Service (ACS) nelle regioni primarie e aggiuntive di un'istanza di IAM Identity Center:

Endpoint ACS	Regione principale	Regione aggiuntiva	Modello di URL ed esempio
IPv4 solo	Sì	Sì	Pattern: https://[Region].signin.aws/platform/saml/acs/ [Tenant ID] Esempio: https://us-west-2.signin.aws/platform/saml/acs/1111111111111111-aaee-ffff-dddd-111111111111
IPv4 Solo alternativi*	Sì	No	Pattern: https://[Region].signin.aws.amazon.com/platform/saml/acs/ [Tenant ID] Esempio: https://us-west-2.signin.aws.amazon.com/platform/saml/acs/1111111111111111

Endpoint ACS	Regione principale	Regione aggiuntiva	Modello di URL ed esempio
			11-aaee-ffff-dddd-111111111111
Dual-stack	Sì	Sì	Pattern: <code>https://[Region].sso.signin.aws/platform/saml/acs/[Tenant ID]</code> Esempio: <code>https://us-west-2.sso.signin.aws/platform/saml/acs/1111111111111111-aaee-ffff-dddd-111111111111</code>

* Per le istanze abilitate prima di febbraio 2026, conservate questo endpoint perché è necessario il single sign-on SAML avviato dal provider di servizi per la regione primaria. IAM Identity Center non utilizza questo endpoint per le istanze abilitate a febbraio 2026 o successivamente.

Utilizzo di applicazioni AWS gestite senza più ACS URLs

Alcuni provider di identità esterni (IdPs) non supportano Multiple Assertion Consumer Service (ACS) URLs nella loro applicazione IAM Identity Center. Gli ACS multipli URLs sono una funzionalità SAML necessaria per l'accesso diretto a una regione specifica in un IAM Identity Center multiregionale.

Ad esempio, se avvii un'applicazione AWS gestita tramite un collegamento all'applicazione, il sistema attiva l'accesso tramite la regione IAM Identity Center connessa all'applicazione. Tuttavia, se l'URL ACS per quella regione non è configurato nell'IdP esterno, l'accesso non riesce.

Per risolvere questo problema, collabora con il tuo fornitore IdP per abilitare il supporto per più ACS. URLs Nel frattempo, puoi comunque utilizzare le applicazioni AWS gestite in altre regioni. Innanzitutto, accedi alla regione il cui URL ACS è configurato nell'IdP esterno (la regione principale per impostazione predefinita). Dopo una sessione attiva in IAM Identity Center, puoi avviare l'applicazione dal portale di AWS accesso in qualsiasi regione abilitata o tramite un collegamento all'applicazione.

Failover verso una regione aggiuntiva per l'accesso Account AWS

L'argomento dell' Account AWS accesso tramite IAM Identity Center è ampiamente trattato in.

[Account AWS accesso](#) Questa sezione fornisce dettagli aggiuntivi relativi al mantenimento dell' Account AWS accesso tra più utenti Regioni AWS in caso di interruzione del servizio nella regione principale.

Se l'istanza di IAM Identity Center subisce un'interruzione nella regione principale (ad esempio, il portale di AWS accesso nella regione principale non è disponibile), la forza lavoro può passare a un'altra regione per continuare ad accedere a Account AWS e alle applicazioni non interessate. Per ulteriori informazioni, consulta [the section called "Accesso alla forza lavoro tramite una regione aggiuntiva"](#).

Ti consigliamo di comunicare gli Portale di accesso AWS endpoint in altre regioni e la configurazione dell'IdP esterno (ad esempio le app per aggiungere segnalibri alle regioni aggiuntive) alla tua forza lavoro non appena completi la configurazione in. [the section called "Replica IAM Identity Center in un'altra regione"](#) Ciò consentirà loro di essere pronti per il failover in un'altra regione, se necessario.

Allo stesso modo, consigliamo AWS CLI agli utenti di creare [AWS CLI profili](#) per regioni aggiuntive per ciascuno dei profili che hanno per la regione principale. Quindi, possono passare a quel profilo in caso di interruzione del servizio nella regione principale.

Note

La continuità dell'accesso a Account AWS dipende anche dallo stato dell'IdP esterno e dalle autorizzazioni, come l'assegnazione di set di autorizzazioni e l'appartenenza ai gruppi, che vengono fornite e replicate prima di un'interruzione del servizio. Consigliamo alla tua organizzazione di configurare anche l'accesso [AWS break-glass per mantenere l' AWS accesso](#) a un piccolo gruppo di utenti privilegiati in caso di interruzione del servizio da parte dell'IdP esterno. [L'accesso di emergenza](#) è un'opzione simile che evita l'utilizzo di utenti IAM, ma dipende anch'essa dall'IdP esterno.

Account AWS resilienza di accesso senza più ACS URLs

Alcuni provider di identità esterni (IdPs) non supportano Multiple Assertion Consumer Service (ACS) URLs nella loro applicazione IAM Identity Center. Gli ACS multipli URLs sono una funzionalità SAML necessaria per l'accesso diretto a una regione specifica in un IAM Identity Center multiregionale.

Per consentire agli utenti di accedere alle proprie regioni Account AWS tramite più IAM Identity Center, è necessario configurare il rispettivo ACS regionale URLs nell'IdP esterno. Tuttavia, se l'IdP esterno supporta solo un singolo URL ACS nella propria applicazione IAM Identity Center, gli utenti possono accedere direttamente a una singola regione IAM Identity Center.

Per risolvere questo problema, collabora con il tuo fornitore IdP per abilitare il supporto per più ACS. URLs Nel frattempo, puoi utilizzare regioni aggiuntive come backup per l'accesso a Account AWS

Se si verifica un'interruzione del servizio IAM Identity Center nella regione principale, è necessario aggiornare l'URL ACS nell'IdP esterno con un URL ACS della regione aggiuntivo. Dopo questo aggiornamento, i tuoi utenti possono accedere al portale di AWS accesso nella regione aggiuntiva utilizzando l'applicazione IAM Identity Center esistente nel portale IdP esterno o tramite un link diretto che condividi con loro.

Ti consigliamo di testare questa configurazione periodicamente per assicurarti che funzioni quando necessario e di comunicare questo processo di failover alla tua organizzazione.

Note

Quando si utilizza una regione aggiuntiva per l'accesso Account AWS in questa configurazione, gli utenti potrebbero non essere in grado di accedere alle applicazioni AWS gestite connesse alla regione principale. Pertanto, consigliamo questa operazione solo come misura temporanea per mantenere l'accesso a Account AWS.

Distribuzione e gestione di applicazioni in più AWS regioni

L'argomento dell'accesso alle applicazioni tramite IAM Identity Center è ampiamente trattato in [Accesso alle applicazioni](#). Questa sezione fornisce dettagli aggiuntivi relativi alla distribuzione e alla gestione delle applicazioni su più piattaforme. Regioni AWS

Distribuzione e gestione di applicazioni AWS gestite su più piattaforme Regioni AWS

Con un'istanza IAM Identity Center a regione singola, puoi distribuire applicazioni AWS gestite nella stessa regione dell'istanza. Alcune applicazioni come Amazon Q Business supportano una connessione interregionale a IAM Identity Center, che ne consente la distribuzione al di fuori della regione dell'IAM Identity Center se l'applicazione di interesse è disponibile lì. Tuttavia, le chiamate

interregionali possono rallentare le prestazioni delle applicazioni e la maggior parte delle applicazioni AWS gestite non supporta questo tipo di connessione.

Un'istanza multiregionale di IAM Identity Center consente di distribuire applicazioni AWS gestite in qualsiasi regione abilitata con una connessione a IAM Identity Center nella stessa regione («connessione locale a livello regionale»). L'implementazione nella regione principale è supportata da tutte le applicazioni gestite integrate. AWS Per confermare quali applicazioni AWS gestite supportano l'implementazione in regioni aggiuntive di IAM Identity Center, consulta la tabella delle applicazioni [in the section called “Applicazioni che è possibile utilizzare con IAM Identity Center”](#). In ogni caso, l'applicazione AWS gestita deve essere disponibile nella regione in cui desideri distribuirla.

Con una connessione locale a IAM Identity Center, le applicazioni AWS gestite accedono alle identità della forza lavoro nella stessa regione per prestazioni e affidabilità ottimali. [Consigliamo di scegliere una connessione regionale locale quando si distribuisce un'applicazione AWS gestita ogni volta che vengono soddisfatti i prerequisiti.](#)

Per distribuire un'applicazione AWS gestita in un'altra regione di IAM Identity Center, avvia la distribuzione in quella regione tramite la console dell'applicazione o l'API nello stesso modo in cui la distribuisce nella regione principale.

Considerazioni:

- Se non hai ancora replicato il tuo IAM Identity Center in quella regione, ti consigliamo di farlo prima in modo che la distribuzione dell'applicazione possa essere completata immediatamente.
- AWS le applicazioni gestite, in molti casi, stabiliranno automaticamente una connessione locale a livello regionale se hai già replicato IAM Identity Center nella regione.
- [Se un'applicazione AWS gestita offre una connessione interregionale a IAM Identity Center, ti consigliamo di scegliere una connessione locale a livello regionale a condizione che siano soddisfatti i prerequisiti.](#)
- Se l'applicazione non supporta la distribuzione in regioni aggiuntive, puoi distribuirla nella regione principale a condizione che l'applicazione sia disponibile in quella regione.

Important

Se l'istanza di IAM Identity Center è multiregionale, tutte le applicazioni AWS gestite utilizzate dall'organizzazione devono supportare IAM Identity Center configurato con una chiave KMS gestita dal cliente indipendentemente dalla regione di distribuzione dell'applicazione. Confermalo [the section called “Applicazioni che è possibile utilizzare con IAM Identity Center”](#)

prima di distribuire un'applicazione e prima di configurare una chiave KMS gestita dal cliente nel tuo IAM Identity Center.

Regione di gestione di un'applicazione

Dopo aver distribuito un'applicazione AWS gestita in una regione aggiuntiva di IAM Identity Center utilizzando una connessione locale a livello regionale, gestisci l'applicazione e le relative assegnazioni a utenti e gruppi nella stessa regione. IAM Identity Center replica i metadati dell'applicazione, comprese le assegnazioni a utenti e gruppi, in altre regioni abilitate in modo che la forza lavoro possa avviare applicazioni da qualsiasi regione abilitata.

Se l'applicazione AWS gestita utilizza una connessione interregionale a IAM Identity Center, puoi gestire i dettagli dell'applicazione, come nome e descrizione, e le assegnazioni delle applicazioni a utenti e gruppi tramite la console e l'API di IAM Identity Center nella regione connessa. Indipendentemente dal tipo di connessione, puoi gestire l'applicazione tramite la relativa console nella relativa regione di distribuzione.

Propagazione attendibile delle identità

Puoi utilizzare la propagazione affidabile delle identità con applicazioni AWS gestite che la supportano in qualsiasi regione abilitata dell'istanza di IAM Identity Center.

Tutte le applicazioni che propagano il contesto dell'identità tra loro devono trovarsi nella stessa regione.

La dipendenza di un'applicazione dalla regione IAM Identity Center connessa

Ogni applicazione AWS gestita si connette a una regione specifica di IAM Identity Center durante la distribuzione. L'applicazione dipende quindi da quella regione per l'accesso dell'utente, anche se l'IAM Identity Center è abilitato in più regioni. Se il tuo IAM Identity Center sta riscontrando un'interruzione in quella regione, gli utenti potrebbero non essere in grado di accedere alle applicazioni AWS gestite connesse alla regione.

Implementazione e gestione di applicazioni gestite dai clienti su più applicazioni Regioni AWS

IAM Identity Center supporta SAML e applicazioni [gestite OAuth2 dai clienti](#). Puoi scegliere di crearle in qualsiasi regione abilitata della tua istanza IAM Identity Center. Dopo averne creata una, gestisci l'applicazione e le sue assegnazioni a utenti e gruppi nella stessa regione.

Rimuovi una regione da IAM Identity Center

Per rimuovere una regione aggiuntiva dall'istanza di IAM Identity Center, segui questi passaggi:

Fase 1: Aggiornamento della configurazione IdP esterna

Puoi scegliere di rimuovere l'URL ACS per questa regione dal tuo IdP esterno o conservarlo nel caso in cui desideri aggiungere nuovamente questa regione in un secondo momento. Ti consigliamo di rimuovere o nascondere l'app per i segnalibri che potresti aver creato per questa Portale di accesso AWS regione.

Passaggio 2: rimuovere la regione

Console

Per aggiungere una regione

1. Apri la [console Centro identità IAM](#).
2. Nel pannello di navigazione scegli Impostazioni.
3. Scegliere la scheda Management (Gestione),
4. Nella sezione Regioni per IAM Identity Center, scegli la regione aggiuntiva che desideri rimuovere.
5. Scegli Rimuovi.
6. Prima di confermare la rimozione selezionando Rimuovi regione, presta attenzione all'avviso relativo alla potenziale perdita di accesso alle applicazioni create in questa regione di IAM Identity Center. Se non sei sicuro di disporre di tali applicazioni, scegli Applicazioni nel pannello di navigazione e conferma la regione connessa nella colonna Creato da per ogni applicazione AWS gestita e gestita dal cliente.

Note

Potresti continuare a incorrere in costi per le distribuzioni di applicazioni AWS gestite che sono ancora connesse alla regione rimossa anche se perdi l'accesso a tali applicazioni. Per evitare ciò, è necessario rimuovere queste distribuzioni di applicazioni AWS gestite tramite la console dell'applicazione o l'API prima di rimuovere la regione in IAM Identity Center. Se hai già rimosso la regione IAM Identity

Center, puoi ripristinare l'accesso alle applicazioni aggiungendo nuovamente la regione.

7. Nella sezione Regions for IAM Identity Center, monitora lo stato della regione. Utilizza il pulsante Aggiorna (freccia circolare) per visualizzare lo stato più recente della regione, se necessario. Una volta rimossa, la regione non viene più visualizzata nell'elenco delle regioni.

AWS CLI

Per rimuovere una regione

```
aws sso-admin remove-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

Per verificare lo stato attuale della regione

```
aws sso-admin describe-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

Quando la regione viene rimossa, procedi al passaggio 2.

Passaggio 3: Eliminare la chiave di replica

Puoi scegliere di rimuovere la chiave di replica da questa regione per evitare di incorrere in costi di archiviazione KMS. [Per ulteriori informazioni, vedere Eliminazione di una chiave. AWS KMS](#)

Important

Assicurati di eliminare solo la chiave di replica in questa regione specifica. Le altre regioni IAM Identity Center continuano a fare affidamento sulla chiave KMS nelle altre regioni abilitate per le normali operazioni.

Il servizio IAM Identity Center è APIs supportato in regioni aggiuntive AWS

"Hello, World!"	Funzionalità in altre regioni
API Identity Center	Supportato: • read/write Operazioni di gestione delle applicazioni • Operazioni di lettura delle istanze Non supportato: • Qualsiasi operazione di scrittura diversa da quella relativa all'applicazione • Operazioni di lettura relative al set di autorizzazioni e all'assegnazione degli account
API Identity Store	Operazioni di lettura
API OIDC	Tutte le operazioni sono supportate
Accedi all'API del portale	Tutte le operazioni sono supportate
API SCIM	Nessuna operazione è supportata

AWS CloudTrail eventi di IAM Identity Center nella regione principale e aggiuntiva

In AWS CloudTrail, puoi controllare le azioni intraprese dagli utenti e dagli amministratori di IAM Identity Center su tutte le istanze IAM Identity Center abilitate Regioni AWS . Gli AWS CloudTrail eventi vengono emessi e registrati nella regione in cui si svolge l'azione. Per ulteriori informazioni, consulta [the section called “Registrazione di log e monitoraggio”](#).

Disponibilità di casi d'uso di IAM Identity Center nelle regioni primarie e aggiuntive

Funzionalità	Disponibilità regionale
Directory della forza lavoro con un portale per gli utenti	
Accesso utente all'accesso al portale e alle sessioni globali, Portale di accesso AWS inclusi (un unico accesso per tutte le regioni)	Tutte le regioni abilitate
Visualizzazione di tutti gli account assegnati	Tutte le regioni abilitate
Visualizzazione di tutte le applicazioni assegnate (indipendentemente da dove sono state create le applicazioni)	Tutte le regioni abilitate
Accesso in lettura a utenti, gruppi e appartenenze nella AWS console o tramite Identity Store APIs	Tutte le regioni abilitate
Revoca le sessioni utente	Tutte le regioni abilitate
Sincronizzazione automatica di utenti e gruppi da una fonte di identità esterna, ad esempio IdP esterna, tramite l'API SCIM o l'API Identity Store	Solo regione primaria
Configura il provisioning automatico delle identità con SCIM	Solo regione primaria
Configurare SAML SSO con un IdP esterno	Solo regione primaria: accesso alla lettura tramite la console in tutte le regioni abilitate
Create/update/delete operazioni su utenti, gruppi e appartenenze ai gruppi tramite la console o Identity Store APIs.	Regione primaria: disponibile tramite l'API Identity Store ma bloccata nella console IAM Identity Center quando l'API SCIM viene utilizzata per il provisioning (tranne disable/enable

Funzionalità	Disponibilità regionale
	l'accesso utente e l'eliminazione degli utenti, che sono sempre disponibili). Regioni aggiuntive: non disponibili
Accesso multiaccount	
Accedi agli account assegnati tramite i collegamenti Portale di accesso AWS AWS CLI, e di scelta rapida	Tutte le regioni abilitate
Gestisci i set di autorizzazioni per più account e le relative assegnazioni nella console e APIs (incluso l'accesso temporaneo con privilegi elevati)	Solo regione principale
Accesso ad applicazioni e AWS servizi	
AWS Implementa applicazioni gestite tramite la console delle applicazioni e APIs	Tutte le regioni abilitate, in base alla disponibilità regionale delle applicazioni e al supporto per la distribuzione in aree aggiuntive
Crea applicazioni gestite dai clienti tramite la console Identity Center e APIs	Tutte le regioni abilitate
Gestisci i metadati e le assegnazioni delle applicazioni nella console e APIs	Regione IAM Identity Center connessa all'applicazione
Avvia le applicazioni da Portale di accesso AWS o direttamente tramite un link all'applicazione o un segnalibro	Tutte le regioni abilitate
Istanze da SSO a Amazon EC2	Tutte le regioni abilitate
Propagazione affidabile delle identità	
Creazione di un emittente del token affidabile	Solo regione principale

Funzionalità	Disponibilità regionale
Propagazione affidabile delle identità con applicazioni AWS gestite	Tutte le regioni abilitate: le applicazioni che propagano il contesto di identità tra loro devono trovarsi nella stessa regione
Altre funzionalità amministrative	
Tutte le altre funzionalità amministrative come la gestione delle regioni, la gestione delle chiavi KMS, la gestione delle istanze e la gestione delle sessioni (tranne la revoca della sessione)	Solo regione principale: accesso alla lettura disponibile in tutte le aree abilitate per alcuni dati (escluse le assegnazioni dei set di autorizzazioni)

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. Puoi replicare l'istanza di IAM Identity Center in altre regioni per mantenere l'accesso all'account con le autorizzazioni già assegnate in caso di interruzione regionale. Per ulteriori informazioni, consulta [Utilizzo di IAM Identity Center su più Regioni AWS](#).

Abilita IAM Identity Center nel tuo account di gestione. AWS Organizations Ciò è necessario per consentire a IAM Identity Center di effettuare il provisioning, il deprovisioning e l'aggiornamento dei ruoli in tutti i tuoi Account AWS. Quando abiliti IAM Identity Center, Regione AWS questo viene distribuito nella regione attualmente selezionata, denominata «regione primaria». Se desideri eseguire la distribuzione in una regione specifica Regione AWS, modifica la selezione della regione prima di abilitare IAM Identity Center, poiché la regione primaria non può essere modificata dopo l'attivazione di IAM Identity Center.

IAM Identity Center supporta la maggior parte delle funzioni amministrative solo dalla regione principale. Ciò include la connessione a un provider di identità esterno, la sincronizzazione di utenti e gruppi e la creazione e l'assegnazione di set di autorizzazioni a utenti e gruppi. Al contrario, la gestione delle applicazioni e delle relative assegnazioni deve avvenire nella regione IAM Identity Center in cui è stata creata l'applicazione.

Note

Anche se il tuo IAM Identity Center viene replicato in altre regioni, ti consigliamo di configurare un accesso [AWS break-glass](#). Ciò consente di mantenere AWS l'accesso per un piccolo gruppo di utenti privilegiati durante eventi come un'interruzione del servizio nell'IdP esterno. [L'accesso di emergenza](#) è un'altra opzione che utilizza le identità di un IdP esterno anziché di utenti IAM; tuttavia, non protegge da un'interruzione dell'IdP esterno.

Sebbene IAM Identity Center determini l'accesso dalla regione in cui si abilita il servizio, sono globali. Account AWS 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 AI, tuttavia, devono essere installate in una regione dell'istanza IAM Identity Center affinché gli utenti possano 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 relativa all'applicazione e [the section called “Distribuzione e gestione di applicazioni AWS gestite su più piattaforme Regioni AWS”](#)

Puoi anche utilizzare IAM Identity Center per autenticare e autorizzare l'accesso alle applicazioni gestite dai clienti basate su SAML e raggiungibili tramite un URL pubblico, indipendentemente dalla piattaforma o dal cloud su cui è costruita l'applicazione.

Non è consigliabile utilizzarle [Istanze account del Centro identità IAM](#) come mezzo per implementare la resilienza perché non supportano l'accesso all' AWS account e creano un secondo punto di controllo isolato che non è collegato all'istanza dell'organizzazione.

Progettato per la disponibilità

La tabella seguente fornisce la disponibilità che IAM Identity Center è progettato per raggiungere in una singola AWS regione. Questi valori non rappresentano un accordo o una garanzia sul livello di servizio, ma forniscono piuttosto informazioni sugli obiettivi di progettazione. Le percentuali di disponibilità si riferiscono all'accesso a dati o funzioni e non si riferiscono alla durabilità (ad esempio, la conservazione a lungo termine dei dati).

Componente di servizio	Obiettivo di progettazione della disponibilità
Piano dati (incluso l'accesso)	99.95%
Piano di controllo	99.90%

Configurare l'accesso di emergenza al Console di gestione AWS

IAM Identity Center è costruito su un' AWS infrastruttura 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 AWS interruzione, ti consigliamo di configurare una configurazione che possa essere utilizzata per fornire un accesso temporaneo a. Console di gestione AWS

AWS ti 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 Console di gestione AWS 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). [Se preferisci non dipendere dall'IdP esterno, valuta la possibilità di configurare AWS un accesso break-glass](#)

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.

Argomenti

- [Riepilogo della configurazione dell'accesso di emergenza](#)
- [Come progettare i ruoli operativi critici](#)
- [Come pianificare il tuo modello di accesso](#)
- [Come progettare una mappatura di emergenza di ruoli, account e gruppi](#)
- [Come creare la configurazione di accesso di emergenza](#)
- [Attività di preparazione alle emergenze](#)
- [Processo di failover di emergenza](#)
- [Ritorno alle normali operazioni](#)
- [Configurazione una tantum di un'applicazione federativa IAM diretta in Okta](#)
- [Configurazione una tantum di un'applicazione federativa IAM diretta con ADFS](#)

Riepilogo della configurazione dell'accesso di emergenza

Per configurare l'accesso di emergenza, è necessario completare le seguenti attività:

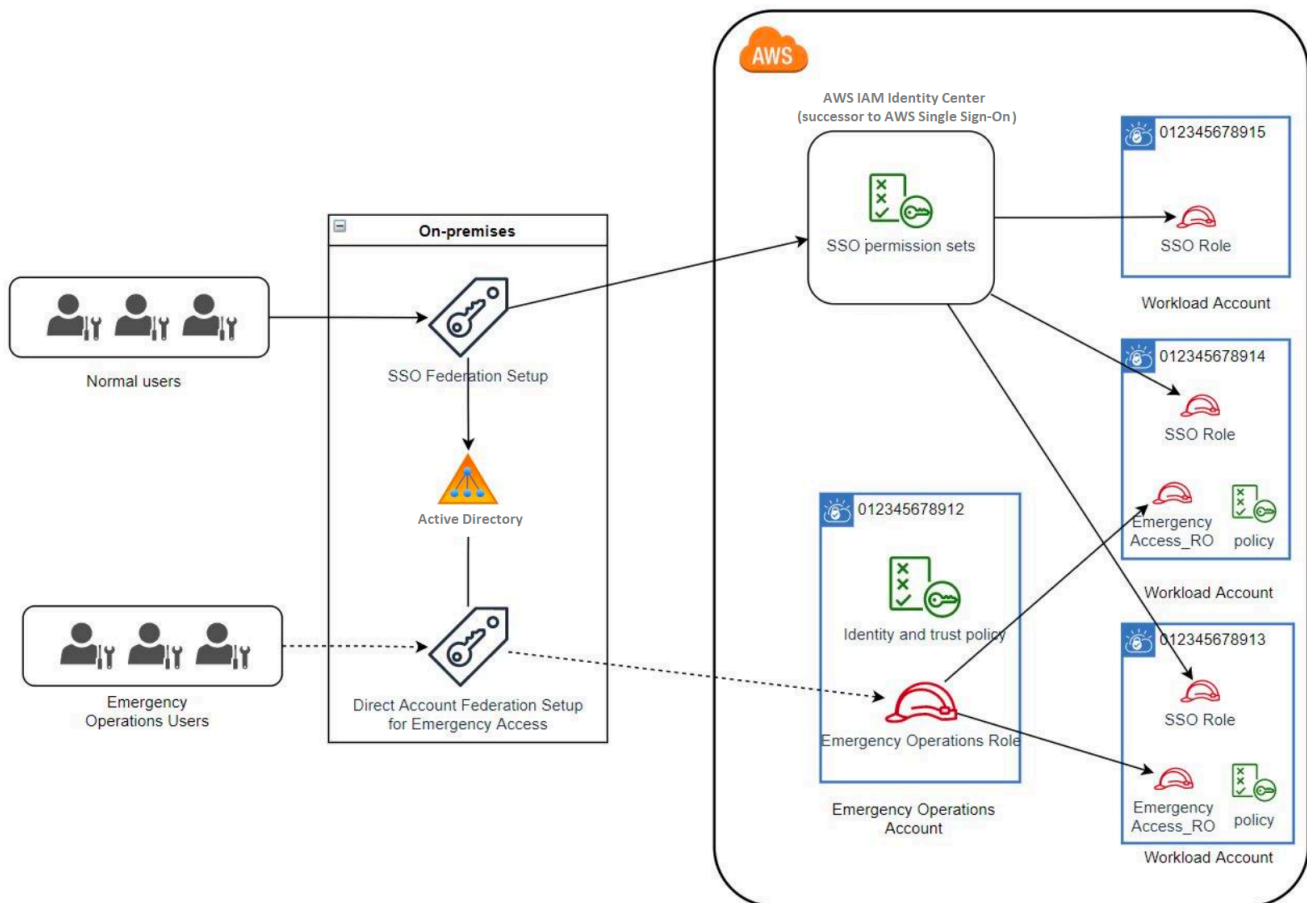
1. [Crea un account per le operazioni di emergenza nella tua organizzazione in AWS Organizations](#). Questo account diventerà il tuo account per le operazioni di emergenza.
2. Connect il tuo IdP all'account per le operazioni di emergenza utilizzando la federazione basata su [SAML 2.0](#).
3. Nell'account 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 Console di gestione AWS

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 Console di gestione AWS 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 tuo modello di accesso

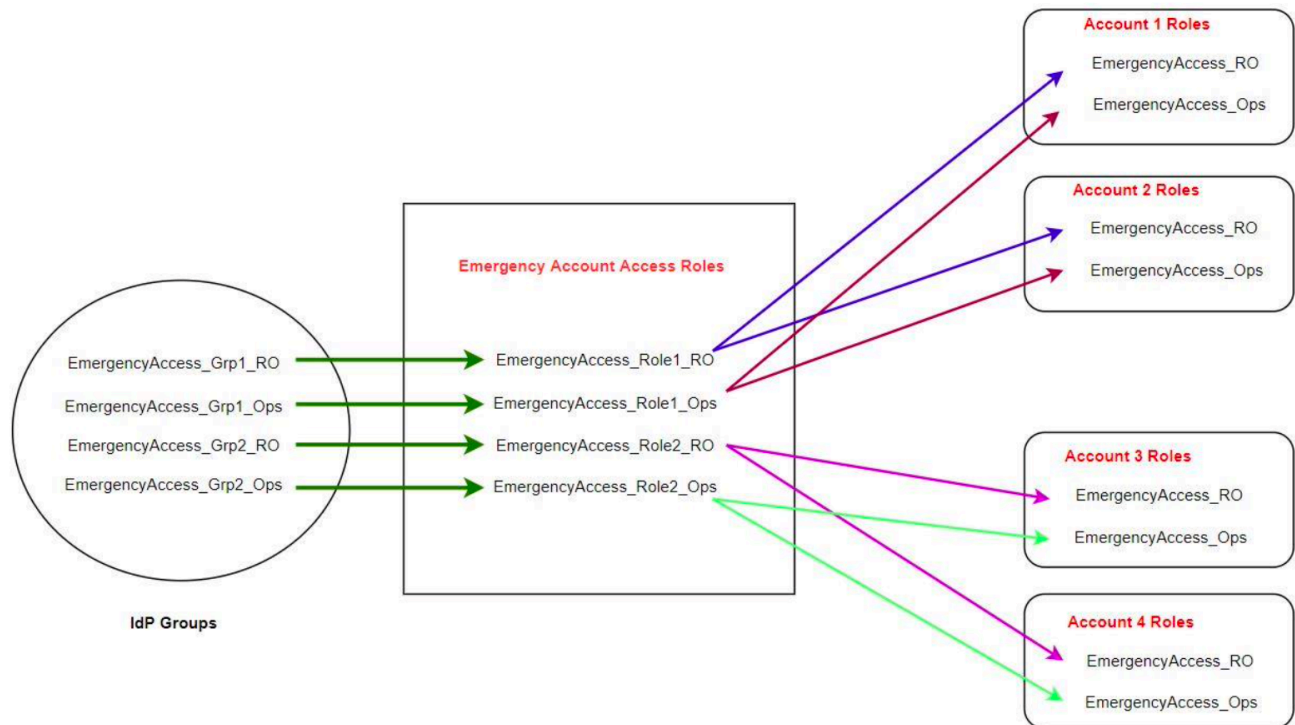
Prima di configurare l'accesso di emergenza, crea un piano per il funzionamento del modello di accesso. Utilizza la procedura seguente per creare questo piano.

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
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_R0 ruolo si affida al EmergencyAccess_Role1_R0 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. Se utilizzi Okta o un'altra fonte esterna IdPs come fonte di identità, consulta [Configurazione una tantum di un'applicazione federativa IAM diretta in Okta](#). Se utilizzi Active Directory come fonte di identità, vedi [Configurazione una tantum di un'applicazione federativa IAM diretta con ADFS](#).
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'[AWS Health 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 AWS Account 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](#). Per gestire gli scenari di errore regionali, quando configuri l'endpoint di accesso, ti consigliamo di abilitare sia l'endpoint non regionale che gli endpoint regionali multipli per tutte le regioni in cui operi per migliorare la resilienza della federazione. Quando configuri l'URL ACS per questo accesso di emergenza, ti consigliamo di utilizzare l'endpoint regionale di una regione diversa da quella in cui è distribuito il tuo IAM Identity Center.

Per l'elenco degli endpoint regionali, consulta gli [endpoint di accesso](#) nel riferimento AWS generale.

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.

Group Filter	<code>^aws\#\S+\#(?({role}}[\w\-\+])\#(?({accountid}}\d+)\\$</code>
Role Value Pattern	<code>arn:aws:iam::\${accountid}:saml-provider/Okta,arn:aws:iam::\${accountid}:role/\${role}</code>

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_R0` ruolo. Per un'illustrazione, vedi l'account di emergenza nel diagramma seguente. [Come progettare una mappatura di emergenza di ruoli, account e gruppi](#) Sostituisci l'ARN del provider SAML di esempio con quello corretto che hai creato nell'account di accesso di emergenza. Sostituisci gli endpoint regionali dell'esempio con le regioni di tua scelta.

JSON

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



```

    "Principal":{
      "Federated":"arn:aws:iam::123456789012:saml-provider/[SAML
PROVIDER NAME]"
    },
    "Action":[
      "sts:AssumeRoleWithSAML",
      "sts:TagSession"
    ],
    "Condition":{"
      "StringEquals":{"
        "SAML:aud": [
          "https://signin.aws.amazon.com/saml",
          "https://us-west-2.signin.aws.amazon.com/saml",
          "https://us-west-1.signin.aws.amazon.com/saml",
          "https://us-east-2.signin.aws.amazon.com/saml"
        ]
      }
    }
  },
  {
    "Effect":"Allow",
    "Principal":{
      "Federated":"arn:aws:iam::123456789012:saml-provider/Okta"
    },
    "Action":"sts:SetSourceIdentity"
  }
]
}

```

8. Di seguito è riportato un esempio di dichiarazione per una politica di autorizzazioni associata al EmergencyAccess_Role1_R0 ruolo. Per un'illustrazione, vedi l'account di emergenza nel diagramma seguente. [Come progettare una mappatura di emergenza di ruoli, account e gruppi](#)

JSON

```

{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",

```

```

        "Resource": [
            "arn:aws:iam::111122223333:role/EmergencyAccess_R0",
            "arn:aws:iam::444455556666:role/EmergencyAccess_R0"
        ]
    }
}

```

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](#)

JSON

```

{
  "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.

Configurazione una tantum di un'applicazione federativa IAM diretta con ADFS

Questa guida descrive il processo di configurazione, una tantum, per configurare la federazione diretta IAM con lo scopo di ADFS abilitare l'accesso di emergenza Account AWS quando IAM Identity Center non è disponibile.

Prerequisiti

Se prevedi di eseguire la configurazione ADFS con AWS Managed Microsoft AD, ti consigliamo di [configurare prima la replica multiregione](#) e di continuare con i passaggi seguenti nella regione aggiuntiva e non nella regione principale per la resilienza.

Pianifica la convenzione di denominazione dei gruppi di Active Directory

Crea gruppi AD utilizzando uno schema di denominazione specifico che consente la corrispondenza automatica tra i nomi dei gruppi e i ruoli AWS IAM.

Formato di denominazione dei gruppi: AWS-<AccountNumber>-<RoleName>

Per un'illustrazione, vedi l'account di emergenza nel diagramma seguente. [Come progettare una mappatura di emergenza di ruoli, account e gruppi](#) Quando un utente viene assegnato a questo gruppo, gli viene concesso l'accesso al EmergencyAccess_Role1_R0 ruolo nell'account. 123456789012 Se un utente è associato a più gruppi, visualizza un elenco di ruoli disponibili Account AWS e può scegliere quale ruolo assumere.

AWS configurazione

La configurazione completa include le configurazioni in un account di accesso di emergenza e negli account del carico di lavoro. Per un'illustrazione della configurazione generale, vedere. [Come progettare una mappatura di emergenza di ruoli, account e gruppi](#)

1. [Creare un provider di identità SAML](#)
2. [Crea ruoli di accesso di emergenza](#)
3. [Configura i ruoli degli account del carico di lavoro](#)

Creare un provider di identità SAML

Nell'account di accesso di emergenza, crea un provider di identità SAML in IAM seguendo i passaggi in [Creare un provider di identità SAML](#) in IAM. Scarica i metadati richiesti dal tuo server: ADFS

`https://<yourADFSserverFQDN>/FederationMetadata/2007-06/
FederationMetadata.xml`

Crea ruoli di accesso di emergenza

[Crea ruoli di accesso](#) di emergenza nell'account di emergenza utilizzando SAML 2.0 Federation come tipo di entità affidabile. Seleziona il provider SAML 2.0 che hai creato nel passaggio precedente.

Considerazioni:

- Includi tutte le regioni in cui operi: seleziona ogni regione in cui hai carichi di lavoro attivi per garantire che la federazione rimanga disponibile durante un'interruzione regionale.
- Configura almeno un endpoint regionale aggiuntivo, anche se operi in una singola regione: ad esempio, se operi solo in us-east-1, aggiungilo us-west-2 come endpoint secondario. Puoi eseguire il failover del tuo IdP sull'endpoint di accesso us-west-2 SAML e continuare ad accedere alle tue us-east-1 risorse, anche senza carichi di lavoro. us-west-2
- Abilita sia l'endpoint non regionale che gli endpoint regionali: sebbene l'endpoint non regionale (`https://signin.aws.amazon.com/saml`) sia altamente disponibile, è ospitato in un unico Regione AWS us-east-1, mentre gli endpoint regionali (`https://<region>.signin.aws.amazon.com/saml`) migliorano la resilienza riducendo la dipendenza da un singolo endpoint globale.

Configura la politica di fiducia

[Configurazione una tantum di un'applicazione federativa IAM diretta in Okta](#) Per un esempio, consulta la politica di fiducia con più endpoint regionali di accesso. Sostituisci gli endpoint regionali e il provider SAML di esempio con i tuoi. ARNs

Configura le politiche di autorizzazione

[Configurazione una tantum di un'applicazione federativa IAM diretta in Okta](#) Per un esempio, fai riferimento alla politica di autorizzazione che alleggi ai ruoli di accesso di emergenza.

Configura i ruoli degli account del carico di lavoro

Per i ruoli degli account di carico di lavoro, configura una politica di attendibilità personalizzata che consenta ai ruoli di accesso di emergenza nell'account di accesso di emergenza di assumerli.

[Configurazione una tantum di un'applicazione federativa IAM diretta in Okta](#) Per un esempio, consulta la policy di fiducia, dove account 123456789012 è l'account per l'accesso di emergenza.

Configurazione di Active Directory

I passaggi seguenti descrivono come configurare Active Directory e ADFS per l'accesso di emergenza.

1. [Creare gruppi](#)
2. [Crea un relying party](#)
3. [Crea regole per i reclami](#)

Creare gruppi

Crea gruppi di emergenza in Active Directory secondo la convenzione di denominazione descritta in precedenza (ad esempio, AWS-123456789012-EmergencyAccess_Role1_R0). Assegna gli utenti a questi gruppi tramite i meccanismi di provisioning esistenti.

Crea un relying party

ADFS la federazione richiede una configurazione di relying party. Il relying party è AWS Security Token Service (AWS STS), che esternalizza l'autenticazione ADFS come provider di identità.

1. Nella console di ADFS gestione, utilizza il menu Azione e seleziona Aggiungi Relying Party Trust. Seleziona Claims aware quando aggiungi un relying party.
2. Per i metadati di federazione, inserisci l'URL dei metadati dalle informazioni sui metadati del provider di identità sulla console IAM. Esempio:

```
https://signin.aws.amazon.com/static/saml/SAMLSPXXXXXX/saml-metadata.xml
```

3. Imposta il nome visualizzato per il relying party (ad esempio, AWS Account Access), quindi scegli Avanti.
4. Seleziona a chi vuoi consentire l'accesso AWS. Puoi selezionare gruppi specifici e definire requisiti come la MFA.
5. Scegli Chiudi nella pagina Fine per completare la procedura guidata Add Relying Party Trust. AWS è ora configurato come relying party.

Crea regole per i reclami

ADFS utilizza Claims Rule Language per emettere e trasformare i reclami tra i fornitori di reclami e le parti affidatarie. Devi creare quattro regole di reclamo: `NameId`, `RoleSessionName`, `Get AD Groups` e `Roles for AWS Access`.

Fai clic con il pulsante destro del mouse sulla parte affidante, quindi scegli **Modifica politica di emissione dei reclami**. Scegli **Aggiungi regola** per aggiungere regole.

1. `NameId`.

- a. Seleziona **Trasforma un reclamo in entrata**, quindi scegli **Avanti**.
- b. Utilizzare le seguenti impostazioni:
 - Nome della regola di richiesta: `NameId`
 - Tipo di reclamo in entrata: `Windows Account Name`
 - Tipo di reclamo in uscita: `Name ID`
 - Formato identificativo del nome in uscita: `Persistent Identifier`
 - Esamina tutti i valori del reclamo: **selezionato**
- c. Scegli **OK**.

2. `RoleSessionName`

- a. Selezionare **Add Rule (Aggiungi regola)**.
- b. Nell'elenco dei modelli di regole di reclamo, seleziona **Invia attributi LDAP come attestazioni**.
- c. Utilizzare le seguenti impostazioni:
 - Nome della regola di rivendicazione: `RoleSessionName`
 - Archivio attributi: `Active Directory`
 - Attributo LDAP: `E-Mail-Addresses`
 - Tipo di reclamo in uscita: `https://aws.amazon.com/SAML/Attributes/RoleSessionName`
- d. Scegli **OK**.

3. Ottieni gruppi AD

- a. Selezionare **Add Rule (Aggiungi regola)**.

- b. Nell'elenco dei modelli di regole di reclamo, seleziona Invia reclami utilizzando una regola personalizzata, quindi scegli Avanti.
- c. Per il nome della regola di reclamo Get AD Groups, inserisci, quindi in Regola personalizzata, inserisci quanto segue:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
=> add(store = "Active Directory", types = ("http://temp/variable"), query =
";tokenGroups;{0}", param = c.Value);
```

Questa regola personalizzata utilizza uno script nel linguaggio delle regole di attestazione che recupera tutti i gruppi di cui l'utente autenticato è membro e li inserisce in un'attestazione temporanea denominata. `http://temp/variable`

Note

Assicurati che non vi siano spazi bianchi finali per evitare risultati imprevisti.

4. Attributi del ruolo

- a. Selezionare Add Rule (Aggiungi regola).
- b. Nell'elenco dei modelli di regole di reclamo, seleziona Invia reclami utilizzando una regola personalizzata, quindi scegli Avanti.
- c. Per il nome della regola di reclamo Roles, inserisci, quindi in Regola personalizzata, inserisci quanto segue:

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-(\d{12})"]
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
  RegExReplace(c.Value, "AWS-(\d{12})-", "arn:aws:iam::$1:saml-provider/
<ADFS>,arn:aws:iam::$1:role/"));
```

Questa regola personalizzata utilizza espressioni regolari per trasformare ogni appartenenza al gruppo del modulo `AWS-<Account Number>-<Role Name>` nel modulo ARN del ruolo IAM e nel modulo ARN del provider federativo IAM previsto. `AWS`

 Note

Nel linguaggio delle regole di esempio riportato sopra, ADFS rappresenta il nome logico assegnato al provider di identità SAML nella configurazione del provider di identità. AWS Modificalo in base al nome logico che hai scelto nella console IAM per il tuo provider di identità.

Test della configurazione

Verifica che la soluzione funzioni autenticandoti su. <https://<yourADFSserverFQDN>/adfs/ls/IdpInitiatedSignOn.aspx> Seleziona il nome del relying party che hai creato dall'elenco a discesa dei siti.

Aggiorna l'endpoint di asserzione SAML predefinito in ADFS

 Important

Quando si configura il relying party trust in ADFS, per impostazione predefinita viene utilizzato l'endpoint SAML Assertion, <https://signin.aws.amazon.com/> che non è un endpoint globale e si trova in. `us-east-1` Ti consigliamo di modificare l'endpoint predefinito con un endpoint regionale diverso da quello in cui il tuo IAM Identity Center è configurato per la resilienza. Ad esempio, se il tuo IAM Identity Center è distribuito in `us-east-1` e anche tu operi in `us-west-2`, modifica l'endpoint consumer SAML Assertion predefinito in. <https://us-west-2.signin.aws.amazon.com/saml>

1. Scegli Proprietà sul relying party trust e vai alla scheda Monitoraggio. Deseleziona la casella di controllo Aggiorna automaticamente il relying party.
2. Vai alla scheda Endpoints, seleziona l'endpoint di accesso preferito e scegli Modifica.
3. Seleziona la casella di controllo Imposta l'URL affidabile come predefinito. Scegli OK e Applica per rendere effettiva l'impostazione.

 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 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 conformità AWS](#). 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. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria 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](#)
- [Console IAM Identity Center e autorizzazione API](#)
- [AWS STS chiavi contestuali di condizione per IAM Identity Center](#)
- [Registrazione e monitoraggio in IAM Identity Center](#)
- [Convalida della conformità per IAM Identity Center](#)
- [Resilienza in IAM Identity Center](#)
- [Sicurezza dell'infrastruttura in IAM Identity Center](#)

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 [Creare, gestire ed eliminare 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.

Note

Se la tua istanza IAM Identity Center è configurata con una chiave KMS gestita dal cliente, gli amministratori del tuo IAM Identity Center e gli altri attori che devono accedere alla chiave

KMS avranno bisogno di autorizzazioni aggiuntive. Fai riferimento a [Implementazione di chiavi KMS gestite dal cliente in AWS 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](#)
- [Esempio di policy basato sulle risorse per IAM Identity Center \(IAM Identity Center\)](#)
- [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](#)
- [Specifiche 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 sulle 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.

JSON

```
{
  "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 sulle 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 (vedi [Risorse e operazioni di IAM Identity Center](#)), il servizio definisce una serie 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, `iam:DescribePermissionsPolicies` autorizza l'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. Se l'accesso a una risorsa non viene esplicitamente autorizzato (consentito), di fatto è 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 le 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 del tuo IAM Identity Center. Per ulteriori informazioni, consulta [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. Al contrario, si allega 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 ruoli. and/or 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.

JSON

```
{
  "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:ListDelegatedAdministrators",
        "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 necessarie per consentire a un utente di creare, gestire e distribuire set di autorizzazioni per: Account AWS

JSON

```

{
  "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": "AccessToSSOProvisionedRoles" 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.

JSON

```

{
  "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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:ListGroupForUser",
        "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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:DescribeAccountAssignmentCreationStatus",
        "sso:DescribeAccountAssignmentDeletionStatus",
        "sso:DescribePermissionSet",
        "sso:DescribePermissionSetProvisioningStatus",
        "sso:DescribeRegisteredRegions",
        "sso:GetApplicationInstance",
        "sso:GetApplicationTemplate",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetManagedApplicationInstance",
        "sso:GetMfaDeviceManagementForDirectory",
        "sso:GetPermissionSet",
        "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": "*"
}
}
}

```

Esempio di policy basato sulle risorse per IAM Identity Center (IAM Identity Center)

Ogni applicazione che funziona con IAM Identity Center e utilizza la [OAuth versione 2.0](#) richiede una policy basata sulle risorse. L'applicazione può essere gestita o gestita dal cliente. AWS La policy basata sulle risorse richiesta, denominata policy dell'applicazione (o [ActorPolicy](#) nella APIs), definisce quali [presidi IAM sono autorizzati a richiamare azioni](#) API del metodo di autenticazione IAM come. [CreateTokenWithIAM](#) Il metodo di autenticazione IAM consente a un principale IAM, ad esempio un ruolo o un AWS servizio IAM, di autenticarsi al servizio OIDC di IAM Identity Center presentando le credenziali IAM per richiedere o gestire i token di accesso su `/token? endpoint aws_iam=t`.

La politica dell'applicazione regola le operazioni per l'emissione di token (`()`). `CreateTokenWithIAM` La policy regola anche le azioni basate sui soli permessi che vengono utilizzate solo dalle applicazioni AWS gestite per convalidare i token (`()`) e revocare i token (`()`). `IntrospectTokenWithIAM` `RevokeTokenWithIAM` Per un'applicazione gestita dal cliente, è possibile configurare questa policy specificando quali presidi IAM sono autorizzati a chiamare.

`CreateTokenWithIAM` Quando un preside autorizzato richiama questa azione API, riceve i token di accesso e aggiornamento per l'applicazione.

Se stai utilizzando la console IAM Identity Center per configurare un'applicazione gestita dal cliente per la [propagazione dell'identità affidabile](#), consulta il Passaggio 4 in [Configurazione delle applicazioni gestite dal cliente OAuth 2.0](#) per informazioni su come configurare la politica dell'applicazione. Per un esempio di policy, vedi [Politica di esempio: consenti a un ruolo IAM di creare token di accesso e aggiornamento](#) più avanti in questo argomento.

Requisiti delle politiche

La politica deve soddisfare i seguenti requisiti:

- La politica deve includere un `Version` elemento impostato su «2012-10-17».
- La politica deve includere almeno un elemento. `Statement`
- Ogni politica `Statement` deve includere i seguenti elementi: `EffectPrincipal`, `Action`, `eResource`.

Elementi delle policy

La politica deve includere i seguenti elementi:

Versione

Specifica la versione del documento di policy. Impostare la versione su 2012-10-17 (la versione più recente).

Dichiarazione

Contiene la politica `Statements`. La politica deve contenerne almeno una `Statement`.

Ogni politica `Statement` è composta dai seguenti elementi.

Effetto

(Obbligatorio) Specifica se concedere o negare le autorizzazioni nell'istruzione di policy. I valori validi sono `Allow` e `Deny`.

Principale

(Obbligatorio) Il [principale](#) è l'identità che ottiene le autorizzazioni specificate nell'istruzione di policy. Puoi specificare i ruoli o i responsabili AWS del servizio IAM.

Azione

(Obbligatorio) Le operazioni dell'API del servizio IAM Identity Center OIDC da consentire o negare. Le azioni valide includono:

- `sso-oauth:CreateTokenWithIAM`: Questa azione, che corrisponde al funzionamento dell'[CreateTokenWithIAM](#) API, concede l'autorizzazione a creare e restituire token di accesso e aggiornamento per le applicazioni client autorizzate autenticate utilizzando qualsiasi entità IAM, come un ruolo di AWS servizio o un utente. Questi token possono contenere ambiti definiti che specificano autorizzazioni come `o. read:profile` e `write:data`.
- `sso-oauth:IntrospectTokenWithIAM` [solo autorizzazione]: concede l'autorizzazione a convalidare e recuperare informazioni sui token di accesso e sui token di aggiornamento attivi OAuth 2.0, inclusi gli ambiti e le autorizzazioni associati. Questa autorizzazione viene utilizzata solo dalle applicazioni AWS gestite e non è documentata nell'IAM Identity Center OIDC API Reference.
- `RevokeTokenWithIAM` [solo autorizzazione]: concede l'autorizzazione a revocare i token di accesso OAuth 2.0 e aggiornare i token, invalidandoli prima della loro normale scadenza. Questa autorizzazione viene utilizzata solo dalle applicazioni AWS gestite e non è documentata nello IAM Identity Center OIDC API Reference.

Risorsa

(Obbligatorio) In questa policy, il valore dell'`Resource` elemento è `"*"`, che significa «questa applicazione».

Per ulteriori informazioni sulla sintassi delle AWS policy, consulta [AWS IAM Policy Reference](#) nella IAM User Guide.

Politica di esempio: consenti a un ruolo IAM di creare token di accesso e aggiornamento

La seguente politica di autorizzazione concede le autorizzazioni a `ExampleAppClientRole`, un ruolo IAM assunto da un carico di lavoro, per creare e restituire token di accesso e aggiornamento.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
    "Sid": "AllowRoleToCreateTokens",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/ExampleAppClientRole"
    },
    "Action": "sso-oauth:CreateTokenWithIAM",
    "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, consultare [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, consultare 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: AWSSSOMaster AccountAdministrator

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.

Questa policy include anche AWS Key Management Service le autorizzazioni necessarie per le istanze IAM Identity Center che utilizzano chiavi gestite dal cliente per la crittografia.

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 [Configurare 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: AWSSSOMember AccountAdministrator](#).
- AWSSSOManageDelegatedAdministrator— Consente a IAM Identity Center di registrare e annullare la registrazione di un amministratore delegato dell'organizzazione.
- AllowKMSKeyUseViaService AllowKMSKeyDiscovery — Consente l' AWS Key Management Service operatività delle chiavi gestite dai clienti utilizzate dalle istanze IAM Identity Center.

Per visualizzare le autorizzazioni per questa policy, consulta AWS Managed Policy [AWSSSOMasterAccountAdministrator](#) Reference.

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` e `iam:PassRole`.

AWS politica gestita: AWSSSOMember AccountAdministrator

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 in qualità di 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.

Questa policy include anche AWS Key Management Service le autorizzazioni necessarie per le istanze IAM Identity Center che utilizzano chiavi gestite dal cliente per la crittografia.

Per visualizzare le autorizzazioni per questa policy, consulta AWS Managed Policy [AWSSSOMemberAccountAdministrator](#) Reference.

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 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 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 [Amministratore delegato](#). Per ulteriori informazioni su come vengono utilizzate queste autorizzazioni AWS Organizations, consulta [Utilizzo AWS Organizations con altri AWS servizi](#).

AWS politica gestita: amministratore AWSSSODirectory

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. Questa policy include anche AWS Key Management Service le autorizzazioni necessarie per le istanze IAM Identity Center che utilizzano chiavi gestite dal cliente per la crittografia.

Questa policy include le seguenti autorizzazioni:

- IAM Identity Center Directory: accesso amministrativo completo alle operazioni di directory di IAM Identity Center.

- Identity Store: accesso amministrativo completo alle operazioni e all'autenticazione dell'archivio di identità.
- IAM Identity Center: autorizzazione a elencare le associazioni di directory.
- AWS Key Management Service- Autorizzazioni per decrittografare, descrivere le chiavi e generare chiavi dati per le chiavi gestite dai clienti utilizzate dalle istanze IAM Identity Center.

Per visualizzare le autorizzazioni per questa policy, consulta [AWSSSODirectoryAdministrator](#) in Managed Policy Reference.AWS

AWS politica gestita: Solo AWSSSORRead

È possibile allegare la policy AWSSSORReadOnly 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.

Questa policy include anche AWS Key Management Service le autorizzazioni necessarie per le istanze IAM Identity Center che utilizzano chiavi gestite dal cliente per la crittografia.

Per visualizzare le autorizzazioni per questa policy, consulta [AWSSSORReadSolo](#) nel riferimento alle policy AWS gestite.

AWS politica gestita: AWSSSODirectory ReadOnly

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 associata 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.

Questa policy include anche AWS Key Management Service le autorizzazioni necessarie per le istanze IAM Identity Center che utilizzano chiavi gestite dal cliente per la crittografia.

Per visualizzare le autorizzazioni per questa policy, consulta [AWS Managed Policy AWSSSODirectoryReadOnly](#) Reference.

AWS politica gestita: AWSIdentity SyncFullAccess

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 dell'autorizzazione

Per visualizzare le autorizzazioni relative a questa politica, consulta [Managed Policy Reference AWSIdentitySyncFullAccess](#).AWS

AWS politica gestita: AWSIdentity SyncReadOnlyAccess

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 associata questa politica non possono aggiornare le 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, vedere [Managed Policy Reference AWSIdentitySyncReadOnlyAccess](#).AWS

AWS politica gestita: AWSSSOService RolePolicy

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 dispongono dell'accesso Single Sign-On a specifici in. Account 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 [AWSIAMIdentityCenterAllowListForIdentityContext](#) in AWS Managed Policy Reference.

AWS politica gestita: `AWSIdentityCenterExternalManagementPolicy`

È possibile allegare la policy `AWSIdentityCenterExternalManagementPolicy` alle identità IAM.

Questa policy fornisce l'accesso alla gestione degli utenti di IAM Identity Center da un provider esterno.

Per visualizzare le autorizzazioni per questa policy, consulta [AWSIdentityCenterExternalManagementPolicy](#) in 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
AWSIdentityCenterExternalManagementPolicy	Politica gestita aggiornata per modificare l'ARN per il tenant di provisioning.	5 dicembre 2025

Modifica	Descrizione	Data
AWSIdentityCenterExternalManagementPolicy	Questa policy fornisce l'accesso alla gestione degli utenti di IAM Identity Center da un provider esterno.	21 novembre 2025
AWSSSOMasterAccountAdministrator , AWSSSOMemberAccountAdministrator , AWSSSOReadSolo , AWSSSODirectoryAdministrator , AWSSSODirectoryReadOnly	Policy gestite aggiornate per includere le AWS KMS autorizzazioni necessarie per le istanze IAM Identity Center che utilizzano chiavi gestite dal cliente per la crittografia.	17 settembre 2025
AWSSSOServiceRolePolicy	Questa politica ora include le autorizzazioni per chiamare. <code>identity-sync:DeleteSyncProfile</code>	11 febbraio 2025
AWSIAMIdentityCenterAllowListForIdentityContext	Questa politica ora include <code>qapps:ExportQAppSessionData</code> le azioni <code>qapps:ListQAppSessionData</code> e le azioni per supportare sessioni di console con identità migliorata per le applicazioni AWS gestite che supportano queste sessioni.	2 ottobre 2024

Modifica	Descrizione	Data
AWSSSOMasterAccountAdministrator	IAM Identity Center ha aggiunto una nuova azione per concedere DeleteSyncProfile le autorizzazioni per consentire di utilizzare questa policy per eliminare i profili di sincronizzazione. Questa azione è associata all' DeleteInstance API.	26 settembre 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Questa politica ora include l's3:ListCallerAccessGrants azione per supportare sessioni di console con identità migliorata per le applicazioni AWS gestite che supportano queste sessioni.	4 settembre 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Questa politica ora include aoss:APIAccessAll , es:ESHttpHead es:ESHttpPost es:ESHttpGet es:ESHttpPatch es:ESHttpDelete , e es:ESHttpPut le azioni per supportare sessioni di console con identità migliorata per le applicazioni AWS gestite che supportano queste sessioni.	12 luglio 2024

Modifica	Descrizione	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Questa politica ora include <code>qapps:PredictQApp</code> , <code>qapps:ImportDocument</code> , <code>qapps:AssociateLibraryItemReview</code> , <code>qapps:DisassociateLibraryItemReview</code> , <code>qapps:GetQAppSession</code> , <code>qapps:UpdateQAppSession</code> , <code>qapps:GetQAppSessionMetadata</code> , <code>qapps:UpdateQAppSessionMetadata</code> , e <code>qapps:TagResource</code> azioni per supportare sessioni di console con identità migliorate per le applicazioni AWS gestite che supportano queste sessioni.	27 giugno 2024

Modifica	Descrizione	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Questa policy ora includeelasticmapreduce:AddJobFlowSteps ,elasticmapreduce:DescribeCluster elasticmapreduce:CancelSteps elasticmapreduce:DescribeStep ,e elasticmapreduce:ListSteps azioni per supportare la propagazione affidabile delle identità in Amazon EMR.	17 maggio 2024

Modifica	Descrizione	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Questa politica ora include <code>qapps:CreateQApp</code> , <code>qapps:PredictProblemStatementFromConversation</code> , <code>qapps:PredictQAppFromProblemStatement</code> , <code>qapps:CopyQApp</code> , <code>qapps:GetQApp</code> , <code>qapps:ListQApps</code> , <code>qapps:UpdateQApp</code> , <code>qapps>DeleteQApp</code> , <code>qapps:AssociateQAppWithUser</code> , <code>qapps:DisassociateQAppFromUser</code> , <code>qapps:ImportDocumentToQAppSession</code> , <code>qapps:CreateLibraryItem</code> , <code>qapps:GetLibraryItem</code> , <code>qapps:UpdateLibraryItem</code> , <code>qapps:CreateLibraryItemReview</code> , <code>qapps:ListLibraryItems</code> , <code>qapps:CreateSubscriptionToken</code> , <code>qapps:StartQAppSession</code> , e <code>qapps:StopQAppSession</code> azioni per supportare sessioni console	30 aprile 2024

Modifica	Descrizione	Data
	con identità avanzata per le applicazioni AWS gestite che supportano queste sessioni.	
AWSSSOMasterAccountAdministrator	Questa politica ora include <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> le azioni <code>signin:CreateTrustedIdentityPropagationApplicationForConsole</code> e le azioni per supportare sessioni di console con identità avanzata per le applicazioni AWS gestite che supportano queste sessioni.	26 aprile 2024
AWSSSOMemberAccountAdministrator	Questa politica ora include <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> le azioni <code>signin:CreateTrustedIdentityPropagationApplicationForConsole</code> e le azioni per supportare sessioni di console con identità avanzata per le applicazioni AWS gestite che supportano queste sessioni.	26 aprile 2024

Modifica	Descrizione	Data
<u>AWSSSOReadSolo</u>	Questa politica ora include l' <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> azione per supportar e sessioni di console con identità avanzata per le applicazioni AWS gestite che supportano tali sessioni.	26 aprile 2024
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	Questa politica ora include l' <code>qbusiness:PutFeedback</code> azione per supportar e sessioni di console con identità avanzata per le applicazioni AWS gestite che supportano queste sessioni.	26 aprile 2024

Modifica	Descrizione	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Questa politica ora include <code>q:StartConversation</code> , <code>q:SendMessage</code> , <code>q:ListConversations</code> , <code>q:GetConversations</code> , <code>q:StartTroubleshootingAnalysis</code> , <code>q:GetTroubleshootingResults</code> , <code>q:StartTroubleshootingResolutionExplanation</code> , e <code>q:UpdateTroubleshootingCommandResult</code> . Le azioni per supportare sessioni di console con identità migliorata per le applicazioni AWS gestite che supportano queste sessioni.	24 aprile 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Questa politica ora include <code>sts:SetContext</code> azione per supportare sessioni di console con identità avanzata per le applicazioni AWS gestite che supportano queste sessioni.	19 aprile 2024

Modifica	Descrizione	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Questa politica ora include <code>qbusiness:Chat</code> , <code>qbusiness:ChatSync</code> , <code>qbusiness:ListConversations</code> , <code>qbusiness:ListMessages</code> , e <code>qbusiness>DeleteConversation</code> le azioni per supportare sessioni di console con identità migliorata per le applicazioni AWS gestite che supportano queste sessioni.	11 aprile 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Questa politica ora include le azioni <code>es3:GetAccessGrantsInstanceForPrefix</code> , <code>s3:GetDataAccess</code>	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 <code>identitystore-auth</code> 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 <code>identitystore-auth</code> 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 <code>identitystore-auth</code> 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 <code>identitystore-auth</code> con nuove autorizzazioni per consentire all'amministratore di elencare ed eliminare le sessioni per un utente.	20 ottobre 2022

Modifica	Descrizione	Data
<u>AWSSSOMasterAccountAdministrator</u>	Questa politica ora include nuove autorizzazioni per le chiamate. <u>ListDelegatedAdministrators</u> _ AWS Organizations Questa politica ora include anche un sottoinsieme di autorizzazioni AWSSSOManageDelegatedAdministrator che include le autorizzazioni per chiamare e. <u>RegisterDelegatedAdministrator</u> <u>DeregisterDelegatedAdministrator</u>	16 agosto 2022
<u>AWSSSOMemberAccountAdministrator</u>	Questa politica ora include nuove autorizzazioni per chiamare. <u>ListDelegatedAdministrators</u> _ AWS Organizations Questa politica ora include anche un sottoinsieme di autorizzazioni AWSSSOManageDelegatedAdministrator che include le autorizzazioni per chiamare e. <u>RegisterDelegatedAdministrator</u> <u>DeregisterDelegatedAdministrator</u>	16 agosto 2022

Modifica	Descrizione	Data
AWSSSOReadSolo	Questa politica ora include nuove autorizzazioni per effettuare chiamate ListDelegatedAdministrators . AWS Organizations	11 agosto 2022
AWSSSOServiceRolePolicy	Questa politica ora include nuove autorizzazioni per chiamare DeleteRolePermissionsBoundary e PutRolePermissionsBoundary .	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 AWSSSOReadSolo	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
AWSSSOReadSolo	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 [Comprensione dei ruoli collegati ai servizi in IAM Identity Center](#).

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 la sezione [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 `AWSServiceRoleForSSO` per concedere a IAM Identity Center le autorizzazioni per gestire le AWS risorse, inclusi ruoli IAM, policy e IdP SAML per tuo conto.

Il ruolo collegato al servizio `AWSService RoleFor SSO` prevede che i seguenti servizi assumano il ruolo:

- IAM Identity Center (prefisso del servizio:) `sso`

La politica di autorizzazione dei ruoli `AWSSSOService RolePolicy` 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 `«SSO_»: AWSReserved`

- `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 `AWSSSOService RolePolicy` 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 `AWSSSOService RolePolicy` 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 `AWSSSOService RolePolicy` 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 `AWSSSOService RolePolicy` collegati al servizio consente a IAM Identity Center di completare quanto segue su «arn:aws:iam: *:»: `role/aws-service-role/ssso.amazonaws.com/AWSServiceRoleForSSO`

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam>DeleteServiceLinkedRole`

La policy di autorizzazione dei ruoli `AWSSSOService RolePolicy` collegati ai servizi consente a IAM Identity Center di completare quanto segue su «arn:aws:identity-sync: *:profile/*»:

- `identity-sync>DeleteSyncProfile`

Per ulteriori informazioni [Aggiornamenti di IAM Identity Center alle policy AWS gestite](#) sugli aggiornamenti `AWSSSOService RolePolicy` alla politica di autorizzazione dei ruoli collegati al servizio, consulta.

JSON

```
{
```

```

"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": [
        "*"
      ]
    },
    {
      "Sid": "AllowDeleteSyncProfile",
      "Effect": "Allow",
      "Action": [
        "identity-sync:DeleteSyncProfile"
      ],
      "Resource": [
        "arn:aws:identity-sync:*:*:profile/*"
      ]
    }
  ]
}

```

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio è necessario configurare le relative autorizzazioni. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

Creazione di un ruolo collegato al servizio per IAM Identity Center

Non è necessario 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 ruolo `AWSServiceRoleForSSO` 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 servizio `AWSServiceRoleForSSO`. Dopo avere creato un ruolo collegato al servizio, non sarà possibile 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 al servizio](#) 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 `SSO`. `AWSServiceRoleForSSO` Quando un Account AWS 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 dall' `AWSServiceRoleForSSO`

1. [Rimuovere l'accesso di utenti e gruppi a un Account AWS](#) per tutti gli utenti e i gruppi che hanno accesso a. Account AWS
2. [Rimuovi i set di autorizzazioni in IAM Identity Center](#) che 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 servizio `AWSServiceRoleForSSO`. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

Console IAM Identity Center e autorizzazione API

La console IAM Identity Center esistente APIs supporta la doppia autorizzazione, che consente di mantenere l'uso delle operazioni API esistenti quando APIs sono disponibili nuove. 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 si mappano a nuove operazioni API rilasciate dopo tali date.

Argomenti

- [Azioni API dopo novembre 2023](#)
- [Azioni API successive a ottobre 2020](#)

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
GetManagedApplicationInstance	DescribeApplication
GetSharedSsoConfiguration	DescribeInstance
ListApplicationInstances	ListApplications
ListApplicationTemplates	ListApplicationProviders
ListDirectoryAssociations	DescribeInstance
ListProfileAssociations	ListApplicationAssignments

Nome operativo della console utilizzato prima del 15 novembre 2023	Azione API utilizzata dopo il 15 novembre 2023
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
DeleteApplicationProfileForAWSAccount	DeleteProfile	DeleteAccountAssignment
DeletePermissionsPolicy	DeletePermissionsPolicy	DeleteInlinePolicyFromPermissionSet
DeletePermissionSet	DeletePermissionSet	DeletePermissionSet
DescribePermissionsPolicies	DescribePermissionsPolicies	ListManagedPoliciesInPermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
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
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile CreateProfile UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust CreateTrust UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
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 `AssumeRoleAPI`.
- 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 `AssumeRoleAPI`.
- 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

Una buona pratica è monitorare la tua organizzazione per garantire che le modifiche vengano registrate. Il monitoraggio consente di verificare eventuali modifiche impreviste e ripristinare le modifiche indesiderate. IAM Identity Center attualmente supporta due AWS servizi che ti aiutano a monitorare la tua organizzazione e le attività che si svolgono al suo interno: AWS CloudTrail e Amazon EventBridge.

Argomenti

- [Registrazione delle chiamate API IAM Identity Center con AWS CloudTrail](#)
- [Registrazione delle chiamate API SCIM di IAM Identity Center con AWS CloudTrail](#)
- [Connect i componenti delle applicazioni con Amazon EventBridge](#)
- [Registrazione degli errori di sincronizzazione AD configurabili](#)

Registrazione delle chiamate API 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, è possibile determinare la richiesta 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 ulteriori dettagli.

Per ulteriori informazioni CloudTrail, consulta la [Guida AWS CloudTrail per l'utente](#).

La tabella seguente riassume gli CloudTrail eventi di IAM Identity Center, le relative fonti di CloudTrail eventi e le APIs corrispondenze. Consulta i [riferimenti alle API di IAM Identity Center](#) per ulteriori informazioni su. APIs

Note

Esiste un gruppo aggiuntivo di CloudTrail eventi, denominato Sign-in, che viene AWS emesso per l'accesso AWS come utente IAM Identity Center. Questi eventi non hanno un pubblico APIs corrispondente e pertanto non sono elencati nei riferimenti API.

CloudTrail eventi	Pubblico APIs	Description	CloudTrail fonti di eventi
Centro identità IAM	Centro identità IAM	L'IAM Identity Center APIs consente la gestione di set di autorizzazioni, applicazioni, emittenti di token affidabili, assegnazioni di account e applicazioni, istanze IAM Identity Center e tag.	sso.amazonaws.com
Identity Store	Archivio di identità	L'Identity Store APIs consente la gestione del ciclo di vita degli utenti e dei gruppi della forza lavoro e delle appartenenze ai gruppi degli utenti. Inoltre, supportano la gestione dei dispositivi MFA degli utenti.	sso-directory.amazonaws.com, identitystore.amazonaws.com
OIDC	OIDC	L'OIDC APIs supporta la propagazione affidabile delle identità, l'accesso e i toolkit IDE come	sso.amazonaws.com, sso-oidc.amazonaws.com

CloudTrail eventi	Pubblico APIs	Description	CloudTrail fonti di eventi
		utente AWS CLI IAM Identity Center già autenticato.	
AWS portale di accesso	AWS portale di accesso	Il portale di AWS accesso APIs supporta le operazioni del portale di AWS accesso e gli utenti ottengono le credenziali dell' AWS CLI account tramite.	sso.amazonaws.com
SCIM	SCIM	SCIM APIs supporta la fornitura di utenti, gruppi e appartenenze ai gruppi tramite il protocollo SCIM. Per ulteriori informazioni, consulta Registrazione delle chiamate API SCIM di IAM Identity Center con AWS CloudTrail .	identitystore-scim.amazonaws.com
Accedi ad AWS	Nessuna API pubblica	AWS emette CloudTrail eventi di accesso per l'autenticazione degli utenti e i flussi di federazione in IAM Identity Center.	signin.amazonaws.com

Argomenti

- [CloudTrail casi d'uso per IAM Identity Center](#)

- [Informazioni su IAM Identity Center in CloudTrail](#)

CloudTrail casi d'uso per IAM Identity Center

Gli CloudTrail eventi emessi da IAM Identity Center possono essere utili per una varietà di casi d'uso. Le organizzazioni possono utilizzare questi registri eventi per monitorare e controllare l'accesso e l'attività degli utenti all'interno del proprio AWS ambiente. Questo può aiutare i casi d'uso relativi alla conformità, in quanto i log raccolgono dettagli su chi accede a quali risorse e quando. È inoltre possibile utilizzare CloudTrail i dati per le indagini sugli incidenti, consentendo ai team di analizzare le azioni degli utenti e tenere traccia dei comportamenti sospetti. Inoltre, la cronologia degli eventi può supportare le attività di risoluzione dei problemi, fornendo visibilità sulle modifiche apportate alle autorizzazioni e alle configurazioni degli utenti nel tempo.

Le sezioni seguenti descrivono i casi d'uso fondamentali che informano i flussi di lavoro, come il controllo, l'indagine sugli incidenti e la risoluzione dei problemi.

Identificazione dell'utente negli eventi avviati dall'utente di IAM Identity Center CloudTrail

IAM Identity Center emette due CloudTrail campi che consentono di identificare l'utente IAM Identity Center responsabile degli CloudTrail eventi, ad esempio l'accesso a IAM Identity Center o AWS CLI l'utilizzo del portale di AWS accesso, inclusa la gestione dei dispositivi MFA:

- **userId**— L'identificatore utente unico e immutabile proveniente dall'Identity Store di un'istanza di IAM Identity Center.
- **identityStoreArn**— L'Amazon Resource Name (ARN) dell'Identity Store che contiene l'utente.

I **identityStoreArn** campi **userId** e vengono visualizzati nell'**onBehalfOf** elemento annidato all'interno dell'**userIdentity** elemento, come illustrato nel registro CloudTrail eventi di esempio seguente. Questo registro eventi mostra questi due campi relativi a un evento il cui **userIdentity** tipo è "IdentityCenterUser». Puoi anche trovare questi campi sugli eventi per gli utenti autenticati di IAM Identity Center il cui **userIdentity** tipo è "Unknown». I tuoi flussi di lavoro devono accettare entrambi i valori di tipo.

```
"userIdentity":{
  "type":"IdentityCenterUser",
  "accountId":"111122223333",
  "onBehalfOf": {
    "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
```

```
"identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
},
"credentialId" : "90e292de-5eb8-446e-9602-90f7c45044f7"
}
```

Tip

Ti consigliamo di utilizzare `userId` e `identityStoreArn` per identificare l'utente responsabile degli CloudTrail eventi IAM Identity Center. I principali campi `userName` e sotto l'elemento `userIdentity` non sono più disponibili. Se i flussi di lavoro, come l'audit o la risposta agli incidenti, dipendono dall'accesso a `username`, hai due opzioni:

- Recupera il nome utente dalla directory IAM Identity Center come spiegato in [Nome utente negli eventi di accesso CloudTrail](#)
- Ottieni il codice `UserName` emesso da IAM Identity Center sotto l'elemento `additionalEventData` in Sign-in. Questa opzione non richiede l'accesso alla directory IAM Identity Center. Per ulteriori informazioni, consulta [Nome utente negli eventi di accesso CloudTrail](#).

Per recuperare i dettagli di un utente, incluso il `username` campo, esegui una query su Identity Store con ID utente e ID Identity Store come parametri. È possibile eseguire questa azione tramite la richiesta [DescribeUser](#) API o tramite la CLI. Di seguito è riportato un esempio di comando CLI. Puoi omettere il `region` parametro se l'istanza di IAM Identity Center si trova nella regione CLI predefinita.

```
aws identitystore describe-user \
--identity-store-id d-1234567890 \
--user-id 544894e8-80c1-707f-60e3-3ba6510dfac1 \
--region your-region-id
```

Per determinare il valore Identity Store ID per il comando CLI nell'esempio precedente, è possibile estrarre l'ID Identity Store dal `identityStoreArn` valore. Nell'esempio `ARNarn:aws:identitystore::111122223333:identitystore/d-1234567890`, l'ID Identity Store è `d-1234567890`. In alternativa, puoi individuare l'ID Identity Store accedendo alla scheda Identity Store nella sezione Impostazioni della console IAM Identity Center.

Se stai automatizzando la ricerca degli utenti nella directory IAM Identity Center, ti consigliamo di stimare la frequenza delle ricerche degli utenti e di prendere in considerazione il [limite di](#)

[accelerazione di IAM Identity Center sull'API Identity Store](#). La memorizzazione nella cache degli attributi utente recuperati può aiutarti a rimanere entro il limite di accelerazione.

Correlazione degli eventi utente all'interno della stessa sessione utente

Il [AuthWorkflowID](#) campo emesso negli eventi di accesso consente di tenere traccia di tutti CloudTrail gli eventi associati a una sequenza di accesso prima dell'inizio di una sessione utente di IAM Identity Center.

Per le azioni dell'utente all'interno del portale di AWS accesso, il `credentialId` valore è impostato sull'ID della sessione dell'utente di IAM Identity Center utilizzata per richiedere l'azione. Puoi utilizzare questo valore per identificare CloudTrail gli eventi iniziati all'interno della stessa sessione utente autenticata di IAM Identity Center nel portale di AWS accesso.

Note

Non è possibile utilizzare `credentialId` per correlare gli eventi di accesso agli eventi successivi, come l'uso del portale di accesso. AWS Il valore del `credentialId` campo emesso negli eventi di accesso ha un uso interno e ti consigliamo di non fare affidamento su di esso. Il valore del `credentialId` campo emesso per [gli eventi del portale di AWS accesso](#) richiamati con OIDC è uguale all'ID del token di accesso.

Identificazione dei dettagli della sessione in background dell'utente negli eventi avviati dall'utente di IAM Identity Center CloudTrail

Il seguente CloudTrail evento cattura il processo di scambio di token OAuth 2.0, in cui un token di accesso esistente (`theSubjectToken`) che rappresenta la sessione interattiva dell'utente viene scambiato con un token di aggiornamento (`the`). `requestedTokenType` Il token di aggiornamento consente a qualsiasi processo di lunga durata avviato dall'utente di continuare a funzionare con le autorizzazioni dell'utente, anche dopo la disconnessione dell'utente.

Per le [sessioni in background degli utenti](#) di IAM Identity Center, l' CloudTrail evento include un elemento aggiuntivo chiamato `resource` nell'elemento. `requestParameters` Il `resource` parametro contiene l'Amazon Resource Name (ARN) del processo in esecuzione in background. Questo elemento è presente solo nei record CloudTrail degli eventi e non è incluso nelle risposte dell'API IAM o dell'SDK di [CreateTokenWithIAM](#) Identity Center.

```
{  
  "clientId": "EXAMPLE-CLIENT-ID",
```

```
"grantType": "urn:ietf:params:oauth:grant-type:token-exchange",
"code": "HIDDEN_DUE_TO_SECURITY_REASONS",
"redirectUri": "https://example.com/callback",
"assertion": "HIDDEN_DUE_TO_SECURITY_REASONS",
"subjectToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
"subjectTokenType": "urn:ietf:params:oauth:token-type:access_token",
"requestedTokenType": "urn:ietf:params:oauth:token-type:refresh_token",
"resource": "arn:aws:sagemaker:us-west-2:123456789012:training-job/my-job"
}
```

Correlazione degli utenti tra IAM Identity Center e directory esterne

IAM Identity Center fornisce due attributi utente che puoi utilizzare per correlare un utente nella sua directory allo stesso utente in una directory esterna (ad esempio, Microsoft Active Directory e Okta Universal Directory).

- **externalId**— L'identificatore esterno di un utente IAM Identity Center. Ti consigliamo di mappare questo identificatore a un identificatore utente immutabile nella directory esterna. Tieni presente che IAM Identity Center non emette questo valore in CloudTrail
- **username**— Un valore fornito dal cliente con cui gli utenti di solito accedono. Il valore può cambiare (ad esempio, con un aggiornamento SCIM). Tieni presente che quando l'origine dell'identità è Directory Service, il nome utente emesso da IAM Identity Center CloudTrail corrisponde al nome utente che inserisci per l'autenticazione. Il nome utente non deve necessariamente corrispondere esattamente al nome utente nella directory IAM Identity Center.

Se hai accesso agli CloudTrail eventi ma non alla directory IAM Identity Center, puoi utilizzare il nome utente emesso sotto l'`additionalEventData` elemento al momento dell'accesso. Per maggiori dettagli sul nome utente in `additionalEventData`, consulta [Nome utente negli eventi di accesso CloudTrail](#)

La mappatura di questi due attributi utente agli attributi utente corrispondenti in una directory esterna è definita in IAM Identity Center quando l'origine dell'identità è Directory Service. Per informazioni, consulta [Mappature degli attributi tra IAM Identity Center e la directory External Identity Provider](#). Gli utenti esterni di IdPs tale provisioning con SCIM dispongono di una propria mappatura. Anche se utilizzi la directory IAM Identity Center come origine dell'identità, puoi utilizzare l'`externalId` attributo per incrociare i principi di sicurezza con la tua directory esterna.

La sezione seguente spiega come cercare un utente di IAM Identity Center in base al nome dell'`username` utente e `externalId`

Visualizzazione di un utente IAM Identity Center tramite nome utente ed ExternalID

Puoi recuperare gli attributi utente dalla directory IAM Identity Center per un nome utente noto richiedendo prima un nome utente corrispondente `userId` utilizzando la richiesta [GetUserId](#) API, quindi emettendo una richiesta [DescribeUser](#) API, come mostrato nell'esempio precedente. L'esempio seguente mostra come recuperare un nome utente `userId` dall'Identity Store. Puoi omettere il `region` parametro se l'istanza di IAM Identity Center si trova nella regione predefinita con la CLI.

```
aws identitystore get-user-id \
  --identity-store d-9876543210 \
  --alternate-identifier '{
    "UniqueAttribute": {
      "AttributePath": "username",
      "AttributeValue": "anyuser@example.com"
    }
  }' \
  --region your-region-id
```

Allo stesso modo, puoi utilizzare lo stesso meccanismo quando conosci il `externalId`. Aggiorna il percorso dell'attributo nell'esempio precedente con il `externalId` valore e il valore dell'attributo con quello specifico `externalId` che stai cercando.

Visualizzazione del Secure Identifier (SID) di un utente in Microsoft Active Directory (AD) ed ExternalID

In alcuni casi, IAM Identity Center emette il SID di un utente nel `principalId` campo degli CloudTrail eventi, come quelli emessi dal portale di AWS accesso e dall'OIDC. APIs Questi casi vengono gradualmente eliminati. Consigliamo ai tuoi flussi di lavoro di utilizzare l'attributo AD `objectguid` quando hai bisogno di un identificatore utente univoco di AD. Puoi trovare questo valore nell'`externalId` attributo nella directory IAM Identity Center. Tuttavia, se i flussi di lavoro richiedono l'uso del SID, recupera il valore da AD in quanto non è disponibile tramite IAM Identity Center. APIs

[Correlazione degli eventi utente all'interno della stessa sessione utente](#) descrive come utilizzare i `username` campi `externalId` and per correlare un utente IAM Identity Center a un utente corrispondente in una directory esterna. Per impostazione predefinita, IAM Identity Center esegue il mapping `externalId` all'`objectguid` attributo in AD e questa mappatura è fissa. IAM Identity Center offre agli amministratori la flessibilità di mappare `username` in modo diverso rispetto alla mappatura predefinita in `ADUserprincipalname`.

Puoi visualizzare queste mappature nella console IAM Identity Center. Vai alla scheda Identity Source delle Impostazioni e scegli Gestisci sincronizzazione nel menu Azioni. Nella sezione Gestisci sincronizzazione, scegli il pulsante Visualizza mappature degli attributi.

Sebbene sia possibile utilizzare qualsiasi identificatore utente AD univoco disponibile in IAM Identity Center per cercare un utente in AD, consigliamo di utilizzarlo `objectguid` nelle query perché è un identificatore immutabile. L'esempio seguente mostra come interrogare Microsoft AD con Powershell per recuperare un utente utilizzando il `objectguid` valore dell'utente di `16809ecc-7225-4c20-ad98-30094aefdbca`. Una risposta corretta a questa query include il SID dell'utente.

```
Install-WindowsFeature -Name RSAT-AD-PowerShell
```

```
Get-ADUser `
-Filter {objectGUID -eq [GUID]::Parse("16809ecc-7225-4c20-ad98-30094aefdbca")} `
-Properties *
```

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](#).

Note

Per ulteriori informazioni sull'evoluzione dell'identificazione degli utenti e del tracciamento delle azioni degli utenti negli CloudTrail eventi, consulta [Importanti modifiche agli CloudTrail eventi per IAM Identity Center](#) nel AWS Security Blog.

Per una registrazione continua degli eventi che si verificano nel tuo sito 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 nella Guida per l'utente di AWS CloudTrail :

- [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.

CloudTrail eventi per IAM Identity Center supportato APIs

Le seguenti sezioni forniscono informazioni sugli CloudTrail eventi associati ai seguenti elementi APIs supportati da IAM Identity Center:

- [API IAM Identity Center](#)
- [API Identity Store](#)
- [API OIDC](#)
- [AWS accedere all'API del portale](#)
- [API SCIM](#)

CloudTrail eventi delle operazioni dell'API IAM Identity Center

L'elenco seguente contiene CloudTrail gli eventi che le operazioni pubbliche di IAM Identity Center emettono con l'origine dell'sso .amazonaws . comevento. Per ulteriori informazioni sulle operazioni pubbliche dell'API IAM Identity Center, consulta l'[IAM Identity Center API Reference](#).

Potresti trovare eventi aggiuntivi nelle CloudTrail operazioni dell'API della console IAM Identity Center su cui si basa la console. Per ulteriori informazioni su queste console APIs, consulta il [Service Authorization Reference](#).

- [AttachCustomerManagedPolicyReferenceToPermissionSet](#)
-

[AttachManagedPolicyToPermissionSet](#)

-

[CreateAccountAssignment](#)

- [CreateApplication](#)

-

[CreateApplicationAssignment](#)

-

[CreateInstance](#)

-

[CreateInstanceAccessControlAttributeConfiguration](#)

- [CreatePermissionSet](#)

- [CreateTrustedTokenIssuer](#)

- [DeleteAccountAssignment](#)

- [DeleteApplication](#)

- [DeleteApplicationAccessScope](#)

- [DeleteApplicationAssignment](#)

- [DeleteApplicationAuthenticationMethod](#)

-

[DeleteApplicationGrant](#)

-

[DeleteInlinePolicyFromPermissionSet](#)

-

[DeleteInstance](#)

-

[DeleteInstanceAccessControlAttributeConfiguration](#)

-

[DeletePermissionsBoundaryFromPermissionSet](#)

-

[DeletePermissionSet](#)

-

[DeleteTrustedTokenIssuer](#)

- [DescribeAccountAssignmentCreationStatuss](#)

-

[DescribeAccountAssignmentDeletionStatus](#)

-

[DescribeApplication](#)

-

[DescribeApplicationAssignment](#)

-

[DescribeApplicationProvider](#)

-

[DescribeInstance](#)

-

[DescribeInstanceAccessControlAttributeConfiguration](#)

-

[DescribePermissionSet](#)

-

[DescribePermissionSetProvisioningStatus](#)

-

[DescribeTrustedTokenIssuer](#)

-

[DetachCustomerManagedPolicyReferenceFromPermissionSet](#)

-

[DetachManagedPolicyFromPermissionSet](#)

-

[GetApplicationAccessScope](#)

-

[GetApplicationAssignmentConfiguration](#)

-

[GetApplicationAuthenticationMethod](#)

-

[GetApplicationGrant](#)

-

[GetInlinePolicyForPermissionSet](#)

-

[GetPermissionsBoundaryForPermissionSet](#)

-

[ListAccountAssignmentCreationStatus](#)

-

[ListAccountAssignmentDeletionStatus](#)

-

[ListAccountAssignments](#)

-

[ListAccountAssignmentsForPrincipal](#)

-

[ListAccountsForProvisionedPermissionSet](#)

-

[ListApplicationAccessScopes](#)

-

[ListApplicationAssignments](#)

-

[ListApplicationAssignmentsForPrincipal](#)

-

[ListApplicationAuthenticationMethods](#)

-

[ListApplicationGrants](#)

-

[ListApplicationProviders](#)

-

[ListApplications](#)

- [ListCustomerManagedPolicyReferencesInPermissionSet](#)
- [ListInstances](#)
- [ListManagedPoliciesInPermissionSet](#)
- [ListPermissionSetProvisioningStatus](#)
- [ListPermissionSets](#)
- [ListPermissionSetsProvisionedToAccount](#)
- [ListTagsForResource](#)
- [ListTrustedTokenIssuers](#)
- [ProvisionPermissionSet](#)
- [PutApplicationAccessScope](#)
- [PutApplicationAssignmentConfiguration](#)
- [PutApplicationAuthenticationMethod](#)
- [PutApplicationGrant](#)
- [PutInlinePolicyToPermissionSet](#)
- [PutPermissionsBoundaryToPermissionSet](#)

- [TagResource](#)
- [UntagResource](#)
- [UpdateApplication](#)
- [UpdateInstance](#)
- [UpdateInstanceAccessControlAttributeConfiguration](#)
- [UpdatePermissionSet](#)
- [UpdateTrustedTokenIssuer](#)

CloudTrail eventi delle operazioni dell'API Identity Store

L'elenco seguente contiene CloudTrail gli eventi che le operazioni pubbliche di Identity Store emettono con l'origine dell'`identitystore.amazonaws.com` evento. Per ulteriori informazioni sulle operazioni pubbliche dell'API Identity Store, consulta l'[Identity Store API Reference](#).

È possibile trovare eventi aggiuntivi nelle CloudTrail operazioni dell'API della console di Identity Store con l'origine `sso-directory.amazonaws.com` dell'evento. Questi APIs supportano la console e il portale di AWS accesso. Se hai bisogno di rilevare il verificarsi di una particolare operazione, ad esempio l'aggiunta di un membro a un gruppo, ti consigliamo di prendere in considerazione sia le operazioni API pubbliche che quelle della console. Per ulteriori informazioni su queste console APIs, consulta il [Service Authorization Reference](#).

- [CreateGroup](#)
- [CreateGroupMembership](#)
- [CreateUser](#)
- [DeleteGroup](#)
- [DeleteGroupMembership](#)
- [DeleteUser](#)

- [DescribeGroup](#)
- [DescribeGroupMembership](#)
- [DescribeUser](#)
- [GetGroupId](#)
- [GetGroupMembershipId](#)
- [GetUserId](#)
- [IsMemberInGroups](#)
- [ListGroupMemberships](#)
- [ListGroupMembershipsForMember](#)
- [ListGroups](#)
- [ListUsers](#)
- [UpdateGroup](#)
- [UpdateUser](#)

CloudTrail eventi delle operazioni dell'API OIDC

L'elenco seguente contiene gli CloudTrail eventi emessi dalle operazioni OIDC pubbliche. [Per ulteriori informazioni sulle operazioni pubbliche dell'API OIDC, consulta l'OIDC API Reference.](#)

- [CreateToken](#)(fonte dell'evento) `sso.amazonaws.com`
- [CreateTokenWithIAM](#)(fonte dell'evento) `sso-oauth.amazonaws.com`

CloudTrail eventi relativi alle operazioni dell'API del portale di AWS accesso

L'elenco seguente contiene CloudTrail gli eventi che le operazioni dell'API del portale di AWS accesso emettono con l'origine dell'`sso.amazonaws.com` evento. Le operazioni API rilevate come non disponibili nell'API pubblica supportano le operazioni del portale di AWS accesso. L'utilizzo di AWS CLI può comportare l'emissione di CloudTrail eventi sia delle operazioni dell'API del portale AWS ad accesso pubblico sia di quelli che non sono disponibili nell'API pubblica. Per ulteriori informazioni sulle operazioni dell'API del portale AWS ad accesso pubblico, consulta l'[AWS Access Portal API Reference](#).

- `Authenticate`(Non disponibile nell'API pubblica. Fornisce l'accesso al portale di AWS accesso.)
- `Federate`(Non disponibile nell'API pubblica. Fornisce la federazione nelle applicazioni.)

- [ListAccountRoles](#)
- [ListAccounts](#)
- ListApplications(Non disponibile nell'API pubblica. Fornisce le risorse assegnate agli utenti da visualizzare nel portale di AWS accesso.)
- ListProfilesForApplication(Non disponibile nell'API pubblica. Fornisce i metadati dell'applicazione da visualizzare nel portale di AWS accesso.)
- [GetRoleCredentials](#)
- [Logout](#)

CloudTrail eventi delle operazioni dell'API SCIM

Per informazioni sulle operazioni pubbliche dell'API SCIM, consulta [AWS Access Portal API Reference](#).

Informazioni sull'identità negli eventi di IAM Identity Center CloudTrail

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.
- Se la richiesta è stata effettuata da un utente di IAM Identity Center. In tal caso, i `identityStoreArn` campi `userId` and sono disponibili negli CloudTrail eventi per identificare l'utente IAM Identity Center che ha avviato la richiesta. Per ulteriori informazioni, consulta [Identificazione dell'utente negli eventi avviati dall'utente di IAM Identity Center CloudTrail](#).

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#).

Note

Attualmente, IAM Identity Center non emette CloudTrail eventi per l'accesso degli utenti ad applicazioni Web AWS gestite (ad esempio, Amazon SageMaker AI Studio) con l'API [OIDC](#). Queste applicazioni Web sono un sottoinsieme del set più ampio di [the section called "AWS](#)

[applicazioni gestite](#)", che include anche applicazioni non Web come Amazon Athena SQL e Amazon S3 Access Grants.

Comprensione degli eventi per IAM Identity Center CloudTrail

Un trail è una configurazione che abilita la distribuzione di eventi in un bucket Amazon S3 che specifichi. 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 gli eventi non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico. Scopri il [contenuto di un CloudTrail record](#) nella Guida per l'CloudTrail utente.

Questo esempio dimostra una voce di CloudTrail registro che registra un'DescribePermissionsPoliciesazione eseguita da un utente IAM (samadams) che interagisce con IAM Identity Center:

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJAIENLMexample",
        "arn": "arn:aws:iam::08966example:user/samadams",
        "accountId": "111122223333",
        "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":"111122223333"
    }
]
}

```

Questo esempio dimostra una voce di CloudTrail registro che registra un'ListApplicationsazione eseguita da un utente di IAM Identity Center all'interno del portale di accesso: AWS

```

{
  "Records":[
    {
      "eventVersion":"1.05",
      "userIdentity":{
        "type":"IdentityCenterUser",
        "accountId":"111122223333",
        "onBehalfOf": {
          "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
          "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        },
        "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
      },
      "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":"111122223333"
    }
  ]
}

```

Questo esempio dimostra una voce di CloudTrail registro che registra un'CreateTokenazione eseguita da un utente di IAM Identity Center che si autentica con il servizio OIDC di IAM Identity Center:

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "accountId": "111122223333",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
  },
  "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": "111122223333",
      "type": "IdentityStoreId",
      "ARN": "d-1234567890"
    }
  ]
}
```

```
}  
],  
"eventType": "AwsApiCall",  
"recipientAccountId": "111122223333"  
}
```

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 IAM Identity Center. Le identità di origine di IAM Identity Center e Active Directory (AD Connector e AWS Managed Microsoft AD) includono 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, oltre allo 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
<code>CredentialChallenge</code>	Utilizzato per notificare che IAM Identity Center ha richiesto all'utente di risolvere una specifica richiesta di credenziali e specifica <code>CredentialType</code> quella richiesta (ad esempio, <code>PASSWORD</code> o <code>TOTP</code>).	Utenti nativi di IAM Identity Center, AD Connector e AWS Managed Microsoft AD
<code>CredentialVerification</code>	Utilizzato per notificare che l'utente ha tentato di risolvere una <code>CredentialChallenge</code> e richiesta specifica e specifica se la credenziale è riuscita o meno.	Utenti nativi di IAM Identity Center, AD Connector e AWS Managed Microsoft AD

Nome evento	Scopo dell'evento	Applicabilità della fonte di identità
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 registrazione di alcun <i>UserAuthentication</i> evento.	Tutte le fonti di identità

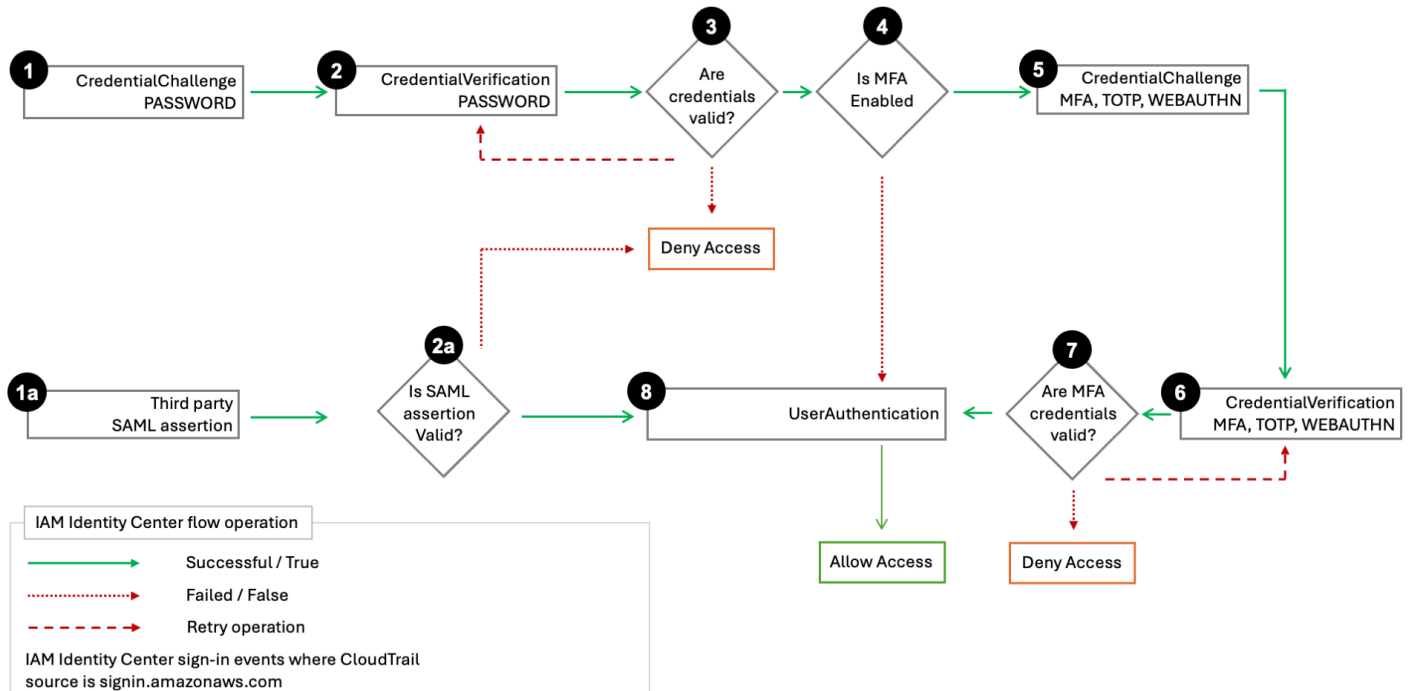
La tabella seguente riporta ulteriori utili campi di dati sugli eventi contenuti all'interno di eventi di accesso CloudTrail specifici.

Campo	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	CredentialChallenge, CredentialVerification	CredentialType: «PASSWORD» o "": CredentialType «PASSWORD, TOTP» (i valori

Campo	Scopo dell'evento	Applicabilità dell'evento di accesso	Valori di esempio
	ntication gli eventi includeranno tutti i CredentialType valori che sono stati verificati con successo nella sequenza di accesso dell'utente.	tion , UserAuthentication	possibili includono : PASSWORD, TOTP, WEBAUTHN, EXTERNAL_IDP, RESYNC_TOTP, EMAIL_OTP)
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/....."

CloudTrail eventi nei flussi di accesso a IAM Identity Center

Il diagramma seguente descrive il flusso di accesso e CloudTrail gli eventi generati da Sign-in.



Il diagramma mostra un flusso di accesso tramite password e un flusso di accesso federato.

Il flusso di accesso tramite password, che comprende i passaggi da 1 a 8, illustra i passaggi da eseguire durante il processo di accesso con nome utente e password. IAM Identity Center è impostato `userIdentity.additionalEventData.CredentialType` su "PASSWORD" e IAM Identity Center esegue il ciclo sfida-risposta delle credenziali, riprovando se necessario.

Il numero di passaggi dipende dal tipo di [accesso e dalla presenza dell'autenticazione a più fattori \(MFA\)](#). Il processo iniziale genera tre o cinque CloudTrail eventi con la `UserAuthentication` fine della sequenza per un'autenticazione corretta. I tentativi di autenticazione con password non riusciti generano CloudTrail eventi aggiuntivi poiché IAM Identity Center esegue nuovamente `CredentialChallenge` l'autenticazione MFA o, se abilitata, l'autenticazione MFA.

Il flusso di accesso tramite password copre anche lo scenario in cui un utente IAM Identity Center appena creato con una chiamata `CreateUser` API accede con una password monouso (OTP). Il tipo di credenziale in questo scenario è «». `EMAIL_OTP`

Il flusso di accesso federato, composto dai passaggi 1a, 2a e 8, illustra le fasi principali del processo di autenticazione federata in cui un'asserzione SAML viene fornita da un provider di identità, convalidata da IAM Identity Center e, in caso di successo, dà luogo. `UserAuthentication` IAM

Identity Center non richiama la sequenza di autenticazione MFA interna nei passaggi da 3 a 7 perché un provider di identità federato esterno è responsabile dell'autenticazione di tutte le credenziali degli utenti.

Nome utente negli eventi di accesso CloudTrail

IAM Identity Center emette il `UserName` campo sotto l'`additionalEventData` elemento una volta per ogni accesso riuscito di un utente IAM Identity Center. L'elenco seguente descrive i due eventi di accesso inclusi nell'ambito e le condizioni in cui si verificano tali eventi. Solo una delle condizioni può essere vera quando un utente effettua l'accesso.

- `CredentialChallenge`
 - Quando `CredentialType` è "PASSWORD": si applica all'autenticazione tramite password con Directory Service o IAM Identity Center directory.
 - Quando `CredentialType` è "EMAIL_OTP": si applica solo al IAM Identity Center directory caso in cui un utente creato con una chiamata `CreateUser` API tenta di accedere per la prima volta e l'utente riceve una password monouso per accedere con quella password una sola volta.
- `UserAuthentication`
 - Quando `CredentialType` è "EXTERNAL_IDP" — si applica all'autenticazione con un IdP esterno.

Il valore `UserName` di una corretta autenticazione è il seguente:

- Quando l'origine dell'identità è un IdP esterno, il valore è uguale al `nameID` valore dell'asserzione SAML in entrata. Questo valore è uguale al campo `in.UserName` IAM Identity Center directory.
- Quando l'origine dell'identità è un IAM Identity Center directory, il valore emesso è uguale al `UserName` campo in questa directory.
- Quando l'origine dell'identità è la Directory Service, il valore emesso è uguale al nome utente che l'utente immette durante l'autenticazione. Ad esempio, un utente che dispone del nome utente `anyuser@company.com` può autenticarsi con `anyuser`, o `anyuser@company.comcompany.com/anyuser`, e in ogni caso il valore inserito viene emesso rispettivamente. CloudTrail

Mascheramento di sicurezza dei tentativi di utilizzo errato del nome utente

Il `UserName` campo contiene la stringa `HIDDEN_DUE_TO_SECURITY_REASONS` quando l'evento registrato è un errore di accesso alla console causato da un errato inserimento del nome utente.

CloudTrail in questo caso non registra il contenuto perché il testo potrebbe contenere informazioni riservate, come descritto negli esempi seguenti:

- Un utente ha immesso accidentalmente una password nel campo del nome utente.
- Un utente immette accidentalmente il nome account di un account e-mail personale, un identificatore di accesso alla banca o a un altro ID privato.

 Tip

Ti consigliamo di utilizzare `userId` e `identityStoreArn` per identificare l'utente responsabile degli CloudTrail eventi di IAM Identity Center. Se è necessario utilizzare il `userName` campo, è possibile utilizzare l'`additionalEventData` elemento `userName` sottostante che viene emesso una volta per ogni accesso riuscito.

Per ulteriori informazioni su come utilizzare il `UserName` campo, consulta. [Correlazione degli eventi utente all'interno della stessa sessione utente](#)

Eventi di esempio per scenari di accesso a IAM Identity Center

Gli esempi seguenti illustrano le sequenze di CloudTrail eventi tipiche generate durante vari AWS scenari di accesso. Questi esempi fungono da modelli di riferimento per aiutarvi a interpretare i log di autenticazione, identificare i problemi di sicurezza e verificare che le politiche di autenticazione funzionino correttamente.

Argomenti

- [Accesso riuscito durante l'autenticazione solo con 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 con password monouso \(TOTP\) basata sul tempo](#)
- [È necessario effettuare correttamente l'accesso durante l'autenticazione con una password e la registrazione MFA forzata](#)
- [Accesso non riuscito a causa di un'autenticazione con password errata](#)

Accesso riuscito durante l'autenticazione solo con password

La seguente sequenza di eventi riporta un esempio di accesso riuscito con sola password.

CredentialChallenge (Password)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    }
  },
  "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
{
  "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",
    "UserName": "bobsmith@example.com",
    "CredentialType": "PASSWORD"
  },
  "requestID": "5be44ffb-6946-4f47-acaf-1adebd4afead",
  "eventID": "27ea7725-c1fd-4355-bdba-d0e628e0e604",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "serviceEventDetails": {
    "CredentialChallenge": "Success"
  }
}
```

Operazione riuscita CredentialVerification (password)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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":"IdentityCenterUser",
  "arn": "",
  "accountId":"111122223333",
  "accessKeyId": "",
  "onBehalfOf": {
    "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
  },
  "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"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
BshlIc50BAA6ftz73M6LsflWDLf0xvi02K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7Tqzi0LiBLBUSx
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": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYSBshIic50BAA6ftz73M6LsfLWD1f0xvi02K3wet9461C30f_iWdilx-zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7Tqzi0LiBLBUSX-east-1",
    "CredentialType": "EXTERNAL_IDP",
    "UserName": "bobsmith@example.com"
  },
  "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 con password monouso (TOTP) basata sul tempo

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":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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",

```

```

    "UserName": "bobsmith@example.com"
  },
  "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": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    }
  },
  "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71",
  "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":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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-7UGIGlYUUVe31Nkzd7ihxKn6DMdnFf00108qc3RF
Sx-pjBXKG_jUcvBk_UILdGytV4o1u97h42B-
TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token
\u003dNMlui44guoVnxRd0qu2tYJIIdyFPX6SDRNTspIScfMM0AgFbho1nnvCaxPTghHbgHCRIXdfffFtzH0sL1ow419Bobn
\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 dimostra una corretta autenticazione tramite password in cui all'utente era richiesto di registrarsi e completare correttamente l'autenticazione a più fattori (MFA) prima di finalizzare il processo di accesso.

CredentialChallenge (Password)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    }
  },
  "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
},
  "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",
      "UserName": "bobsmith@example.com"
    },
    "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": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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": "IdentityCenterUser",
        "arn": "",
        "accountId": "111122223333",
        "accessKeyId": "",
        "onBehalfOf": {
            "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
            "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
        },
        "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
    },
    "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_maUsZ7ABETjeQhyWfvIHyz52rgR28sYAKN1oEk2G07czrwzXvE9HL1N2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY_EgU3fh0L3QWvWiQuYnDPMYPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrggrgbxXat2M646UZGp93krw7WYQdHIgi50YI9QSc
\u003dd-9067230c03\u0026region\u003ddus-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 a causa di un'autenticazione con password errata

La seguente sequenza di eventi mostra un tentativo di autenticazione in cui l'utente ha immesso correttamente il proprio nome utente ma non ha superato la fase di verifica della password, con conseguente errore di accesso.

CredentialChallenge (Password)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"Unknown",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
  },

```

```

"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",
  "UserName":"bobsmith@example.com"
},
"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",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":""
  },
  "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"
  }
}
```

Registrazione delle chiamate API SCIM di IAM Identity Center con AWS CloudTrail

[IAM Identity Center SCIM](#) è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o un. Servizio AWS CloudTrail acquisisce le chiamate API per SCIM come eventi. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare le informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. Per ulteriori informazioni CloudTrail, consulta la [Guida AWS CloudTrail per l'utente](#).

Note

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Tuttavia, potrebbe essere necessario ruotare il token di accesso per visualizzare gli eventi di SCIM, se il token è stato creato prima di settembre 2024.

Per ulteriori informazioni, consulta [Ruota un token di accesso](#).

SCIM supporta la registrazione delle seguenti operazioni come eventi in: CloudTrail

- [CreateGroup](#)
- [CreateUser](#)
- [DeleteGroup](#)

- [DeleteUser](#)
- [GetGroup](#)
- [GetSchema](#)
- [GetUser](#)
- [ListGroups](#)
- [ListResourceTypes](#)
- [ListSchemas](#)
- [ListUsers](#)
- [PatchGroup](#)
- [PatchUser](#)
- [PutUser](#)
- [ServiceProviderConfig](#)

Eventi di esempio CloudTrail

Gli esempi seguenti mostrano i registri CloudTrail degli eventi tipici generati durante le operazioni SCIM con IAM Identity Center. Questi esempi mostrano la struttura e il contenuto degli eventi per operazioni di successo e scenari di errore comuni, aiutandoti a capire come interpretare CloudTrail i log durante la risoluzione dei problemi di provisioning SCIM.

Operazione riuscita **CreateUser**

Questo CloudTrail evento mostra un'CreateUser operazione riuscita eseguita tramite l'API SCIM. L'evento acquisisce sia i parametri della richiesta (con informazioni sensibili mascherate) sia gli elementi di risposta, incluso l'ID dell'utente appena creato. Questo tipo di evento viene generato quando un provider di identità fornisce correttamente un nuovo utente a IAM Identity Center utilizzando il protocollo SCIM.

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "WebIdentityUser",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
```



```

"eventName": "CreateUser",
"awsRegion": "us-east-1",
"sourceIPAddress": "xx.xxx.xxx.xxx",
"userAgent": "Go-http-client/2.0",
"requestParameters": {
  "httpBody": {
    "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "schemas" : [
      "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "name": {
      "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "active": true,
    "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "tenantId": "xxxx"
},
"responseElements": {
  "meta" : {
    "created" : "Oct 10, 2024, 1:23:45 PM",
    "lastModified" : "Oct 10, 2024, 1:23:45 PM",
    "resourceType" : "User"
  },
  "displayName" : "HIDDEN_DUE_TO_SECURITY_REASONS",
  "schemas" : [
    "urn:ietf:params:scim:schemas:core:2.0:User"
  ],
  "name": {
    "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "active": true,
  "id" : "c4488478-a0e1-700e-3d75-96c6bb641596",
  "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
},
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",

```

```
"tlsDetails": {  
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"  
}  
}
```

PatchGroupOperazione non riuscita: attributo di percorso richiesto mancante

Questo CloudTrail evento mostra un'PatchGroupoperazione non riuscita che ha ValidationException provocato un messaggio di errore"Missing path in PATCH request". L'errore si è verificato perché l'PATCHoperazione richiede un attributo path per specificare l'attributo di gruppo da modificare, ma questo attributo non era presente nella richiesta.

```
{  
  "eventVersion": "1.10",  
  "userIdentity": {  
    "type": "Unknown",  
    "accountId": "123456789012",  
    "accessKeyId": "xxxx"  
  },  
  "eventTime": "xxxx",  
  "eventSource": "identitystore-scim.amazonaws.com",  
  "eventName": "PatchGroup",  
  "awsRegion": "us-east-1",  
  "sourceIPAddress": "xxx.xxx.xxx.xxx",  
  "userAgent": "Go-http-client/2.0",  
  "errorCode": "ValidationException",  
  "errorMessage": "Missing path in PATCH request",  
  "requestParameters": {  
    "httpBody": {  
      "operations": [  
        {  
          "op": "REMOVE",  
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"  
        }  
      ],  
      "schemas": [  
        "HIDDEN_DUE_TO_SECURITY_REASONS"  
      ]  
    },  
    "tenantId": "xxxx",  
    "id": "xxxx"  
  },  
  "responseElements": null,
```

```

"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

CreateGroup Operazione non riuscita: il nome del gruppo esiste già

Questo CloudTrail evento mostra un'CreateGroup operazione non riuscita che ha `ConflictException` provocato un messaggio di errore "Duplicate GroupDisplayName". Questo errore si verifica quando si tenta di creare un gruppo con un nome visualizzato già esistente in IAM Identity Center. Il provider di identità deve utilizzare un nome di gruppo univoco o aggiornare il gruppo esistente invece di crearne uno nuovo.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ConflictException",
  "errorMessage": "Duplicate GroupDisplayName",
  "requestParameters": {
    "httpBody": {
      "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "tenantId": "xxxx"
  },
  "responseElements": null,
  "requestID": "xxxx",

```

```

"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

PatchUser Operazione non riuscita: indirizzi e-mail multipli non supportati

Questo CloudTrail evento mostra un PatchUser operazione non riuscita che ha ValidationException provocato un messaggio di errore "List attribute emails exceeds allowed limit of 1". Questo errore si verifica quando si tenta di assegnare più indirizzi e-mail a un utente, poiché IAM Identity Center supporta solo un indirizzo e-mail per utente. Il provider di identità deve configurare la mappatura SCIM per inviare un solo indirizzo e-mail per ogni utente.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "List attribute emails exceeds allowed limit of 1",
  "requestParameters": {
    "httpBody": {
      "operations": [
        {
          "op": "REPLACE",
          "path": "emails",
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      ]
    }
  },

```

```

    "schemas": [
      "HIDDEN_DUE_TO_SECURITY_REASONS"
    ],
    },
    "tenantId": "xxxx",
    "id": "xxxx"
  },
  "responseElements": null,
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}

```

Errori comuni di convalida dell'API SCIM in IAM Identity Center

I seguenti messaggi di errore di convalida compaiono comunemente negli CloudTrail eventi quando si utilizza l'API SCIM con IAM Identity Center. Questi errori di convalida si verificano in genere durante le operazioni di provisioning di utenti e gruppi.

[Per una guida dettagliata sulla risoluzione di questi errori e sulla corretta configurazione del provisioning SCIM, consulta questo articolo.](#) [AWS re:Post](#)

- L'attributo di elenco email supera il limite consentito di 1
- Il limite consentito per gli indirizzi degli attributi di elenco è 1
- Sono stati rilevati 1 errore di convalida: il valore corrispondente a `*name.familyName*` non è riuscito a soddisfare il vincolo: il membro deve soddisfare il modello di espressione regolare: `[\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {P}\\ t\\ n\\ r] +`
- Sono stati rilevati 2 errori di convalida: il valore in `'nome.FamilyName'` non è riuscito a soddisfare il vincolo: il membro deve avere una lunghezza maggiore o uguale a 1; il valore in `'nome.FamilyName'` non è riuscito a soddisfare il vincolo: il membro deve soddisfare il modello di espressione regolare: `[\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {P}\\ t\\ n\\ n\\ r] +`
- 2 errori di convalida rilevati: il valore in `'URN:IETF:params:SCIM:schemas:Extension:enterprise:2.0:user.manager.value'` non è riuscito

a soddisfare il vincolo: il membro deve avere una lunghezza maggiore o uguale a 1; il valore in 'urn:IETF:params:SCIM:schemas:Extension:enterprise:2.0:user.manager.value' non è riuscito a soddisfare il vincolo: Member must soddisfare il modello di espressione regolare: `[\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {P}\\ t\\ n\\ r] +`»,

- JSON non valido da RequestBody
- Formato di filtro non valido

Connect i componenti delle applicazioni con Amazon EventBridge

Puoi integrare IAM Identity Center con [Amazon EventBridge](#) per generare eventi che avviano notifiche amministrative o richiamano flussi di lavoro automatizzati in risposta a specifiche azioni di IAM Identity Center registrate negli eventi. CloudTrail

Ad esempio, potresti configurare [EventBridge regole](#) per rilevare quando un utente elimina un'applicazione o quando IAM Identity Center crea un nuovo gruppo. [A seconda del caso d'uso, puoi indirizzare questi eventi a un argomento di Amazon SNS per avvisare gli amministratori o richiamare un'automazione aggiuntiva utilizzando Step AWS Lambda Functions o altri servizi supportati.](#)
[EventBridge](#)

Registrazione degli errori di sincronizzazione AD configurabili

È possibile abilitare la registrazione sulle configurazioni di sincronizzazione configurabili di Active Directory (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 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 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 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. Seleziona Invia.

Per disabilitare 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. Seleziona Invia.

Campi configurabili del registro degli errori di sincronizzazione AD

Consulta il seguente elenco 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 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 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. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta la [Documentazione AWS sulla sicurezza](#).

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'Health 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 appropriati e di determinare il modello di responsabilità appropriato 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 conformità 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 archiviare, 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 dimostrano 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, consulta [Progettazione 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.

Protezione dei dati in IAM Identity Center

Il [modello di responsabilità AWS condivisa](#) si applica alla protezione dei dati in AWS IAM Identity Center. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutto il AWS cloud. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile delle attività di configurazione e gestione della sicurezza per i AWS servizi che utilizza. Per ulteriori informazioni sulla privacy dei dati, consulta [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post [AWS Modello di responsabilità condivisa](#) e GDPRAWS nel blog sulla sicurezza di .

Ti consigliamo di proteggere i tuoi dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con IAM Identity Center.
- Usa TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta [Lavorare con i CloudTrail percorsi](#) nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS dei servizi.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, come gli indirizzi e-mail dei tuoi clienti, nei tag o nei campi di testo in formato libero come il campo Nome. Ciò include quando lavori con o con AWS IAM Identity Center altri AWS servizi che utilizzano la console, l'API o AWS CLI AWS SDKs Tutti i dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i registri di diagnostica.

Crittografia dei dati in transito

IAM Identity Center protegge i dati in transito, mentre viaggiano da e verso il servizio, crittografando automaticamente tutti i dati tra reti utilizzando il protocollo di crittografia Transport Layer Security (TLS) 1.2 o TLS 1.3. Le richieste HTTPS dirette autenticate con IAM e inviate a IAM Identity Center APIs, Identity Store API o OIDC vengono firmate utilizzando l'algoritmo [AWS Signature](#) Version 4 per stabilire una connessione sicura.

Privacy dei dati

Con IAM Identity Center, mantieni il controllo dei dati della tua organizzazione. Le identità di utenti e gruppi archiviate in IAM Identity Center vengono condivise con altri AWS servizi, come [le applicazioni AWS gestite](#), solo se le abiliti con IAM Identity Center e se necessario con tali servizi.

Per ulteriori informazioni, consulta le [Domande frequenti sulla privacy AWS dei dati](#).

Conservazione dei dati

IAM Identity Center archivia i dati, come le identità di utenti e gruppi e i metadati, finché non li elimini dal servizio. Quando elimini un'istanza di IAM Identity Center, vengono eliminati anche i dati in essa contenuti.

Crittografia dei dati a riposo

IAM Identity Center fornisce la crittografia per proteggere i dati inattivi dei clienti utilizzando i seguenti tipi di chiavi:

- Chiavi di proprietà di AWS (tipo di chiave predefinito): IAM Identity Center utilizza queste chiavi per impostazione predefinita per crittografare automaticamente i dati. Non puoi visualizzarne, gestirne, verificarne l'utilizzo o utilizzare le chiavi AWS di proprietà per altri scopi. IAM Identity Center gestisce interamente la gestione delle chiavi per proteggere i tuoi dati, senza che tu debba intraprendere alcuna azione. Per ulteriori informazioni, consulta la pagina [chiavi di proprietà AWS](#) nella [Guida per gli sviluppatori di AWS Key Management Service](#).
- Chiavi gestite dal cliente: nelle istanze organizzative di IAM Identity Center, puoi scegliere una chiave simmetrica gestita dal cliente per la crittografia del resto dei dati relativi all'identità della forza lavoro, come gli attributi di utenti e gruppi. Sei tu a creare, possedere e gestire queste chiavi di crittografia. Avendo il pieno controllo di questo livello di crittografia, è possibile eseguire operazioni quali:
 - Stabilire e mantenere politiche chiave per limitare l'accesso alla chiave solo ai responsabili IAM che ne hanno bisogno, come IAM Identity Center and [AWS applicazioni gestite](#) in the same AWS Organizations e ai relativi amministratori.
 - Stabilire e mantenere le politiche IAM per l'accesso alla chiave, incluso l'accesso tra più account
 - Abilitare e disabilitare le policy delle chiavi
 - Ruotare i materiali crittografici delle chiavi
 - Verifica dell'accesso ai dati che richiedono l'accesso tramite chiave
 - Aggiungere tag

- Creare alias delle chiavi
- Pianificare l'eliminazione delle chiavi

Per scoprire come implementare una chiave KMS gestita dal cliente in IAM Identity Center, consulta [Implementazione di chiavi KMS gestite dal cliente in AWS IAM Identity Center](#). Per ulteriori informazioni sulle chiavi gestite dal cliente, consulta la [chiave gestita dal cliente](#) nella Guida per gli AWS Key Management Service sviluppatori.

Note

IAM Identity Center abilita automaticamente la crittografia dei dati AWS inattivi utilizzando chiavi KMS di proprietà per proteggere gratuitamente i dati dei clienti. Tuttavia, quando si utilizza una chiave gestita dal cliente, vengono applicati dei costi AWS KMS. Per ulteriori informazioni sui prezzi, consulta [AWS Key Management Service prezzi](#).

Considerazioni sull'implementazione delle chiavi gestite dal cliente:

- Chiavi dedicate: consigliamo di creare una nuova chiave KMS dedicata gestita dal cliente per ogni istanza di IAM Identity Center anziché riutilizzare una chiave esistente. Questo approccio offre una separazione più chiara dei compiti, semplifica la gestione del controllo degli accessi e rende più semplici i controlli di sicurezza. Disporre di una chiave dedicata riduce anche i rischi limitando l'impatto delle modifiche chiave a una singola istanza di IAM Identity Center.
- Utilizzo di IAM Identity Center su più istanze Regioni AWS: se prevedi di replicare la tua istanza IAM Identity Center su altre istanze Regioni AWS, dovrai utilizzare una chiave KMS gestita dal cliente per la crittografia dei dati inattivi. Il tipo di chiave KMS AWS di proprietà predefinita non è supportato in un IAM Identity Center multiregionale. Per ulteriori informazioni, consulta [Utilizzo di IAM Identity Center su più Regioni AWS](#).

Note

IAM Identity Center utilizza la [crittografia a busta](#) per crittografare i dati di identità della forza lavoro. La chiave KMS svolge il ruolo di chiave di avvolgimento che crittografa la chiave dati effettivamente utilizzata per crittografare i dati.

Per ulteriori informazioni su AWS KMS, consulta [Cos'è il servizio di gestione delle chiavi? AWS](#)

Contesto di crittografia IAM Identity Center

Un [contesto di crittografia](#) è un insieme opzionale di coppie chiave-valore non segrete che contengono informazioni contestuali aggiuntive sui dati. AWS KMS utilizza il contesto di crittografia come dati autenticati aggiuntivi per supportare la crittografia autenticata. Quando includi un contesto di crittografia in una richiesta di crittografia dei dati, AWS KMS associa il contesto di crittografia ai dati crittografati. Per decrittografare i dati, nella richiesta deve essere incluso lo stesso contesto di crittografia. Per ulteriori informazioni sul contesto di crittografia, [consulta la AWS KMS Developer Guide](#).

IAM Identity Center utilizza chiavi contestuali di crittografia tra le seguenti: `aws:sso:instance-arn`, `aws:identitystore:identitystore-arn` e `tenant-key-id`. Ad esempio, il AWS KMS seguente contesto di crittografia può apparire nelle operazioni API richiamate dall'API IAM Identity Center.

```
"encryptionContext": {
  "tenant-key-id": "ssoins-1234567890abcdef",
  "aws:sso:instance-arn": "arn:aws:sso::instance/ssoins-1234567890abcdef"
}
```

Il seguente contesto di crittografia può apparire nelle operazioni AWS KMS API richiamate dall'API [Identity Store](#).

```
"encryptionContext": {
  "tenant-key-id": "12345678-1234-1234-1234-123456789012",
  "aws:identitystore:identitystore-arn":
    "arn:aws:identitystore::123456789012:identitystore/d-1234567890"
}
```

Utilizzo del contesto di crittografia per controllare l'accesso alla chiave gestita dal cliente

È possibile utilizzare il contesto di crittografia nelle policy delle chiavi e nelle policy IAM come condizioni per controllare l'accesso alla chiave simmetrica gestita dal cliente. Alcuni dei modelli di policy chiave [Dichiarazioni politiche chiave di Advanced KMS](#) inclusi includono tali condizioni per garantire che la chiave venga utilizzata solo con un'istanza specifica di IAM Identity Center.

Monitoraggio delle chiavi di crittografia per IAM Identity Center

Quando utilizzi una chiave KMS gestita dal cliente con la tua istanza IAM Identity Center, puoi utilizzare [AWS CloudTrail](#) o [Amazon CloudWatch Logs](#) per tenere traccia delle richieste inviate da IAM Identity Center. AWS KMS Le operazioni dell'API KMS in cui sono elencate le chiamate di IAM Identity Center. [Fase 2: Preparare le dichiarazioni politiche chiave del KMS](#) CloudTrail gli eventi per queste operazioni API contengono il contesto di crittografia, che consente di monitorare le operazioni AWS KMS API richiamate dall'istanza di IAM Identity Center per accedere ai dati crittografati dalla chiave gestita dal cliente.

Esempio di contesto di crittografia in un CloudTrail caso di operazione dell' AWS KMS API:

```
{
  "requestParameters": {
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "encryptionContext": {
      "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-xxxxxxxxxxxxxxxxxx",
      "tenant-key-id": "ssoins-xxxxxxxxxxxxxxxxxx"
    }
  }
}
```

AWS archiviazione, crittografia ed eliminazione degli attributi di identità di IAM Identity Center da parte delle applicazioni gestite

Alcune applicazioni AWS gestite con cui esegui la distribuzione AWS IAM Identity Center, come AWS Systems Manager e Amazon CodeCatalyst, memorizzano attributi di utenti e gruppi specifici di IAM Identity Center nel proprio data store. La crittografia inattiva con una chiave KMS gestita dal cliente in IAM Identity Center non si estende agli attributi di utenti e gruppi di IAM Identity Center archiviati nelle applicazioni AWS gestite. AWS le applicazioni gestite supportano diversi metodi di crittografia per i dati che archiviano. Infine, quando elimini gli attributi di utenti e gruppi all'interno di IAM Identity Center, queste applicazioni AWS gestite possono continuare a archiviare queste informazioni anche dopo l'eliminazione in IAM Identity Center. Fai riferimento alla guida per l'utente delle tue applicazioni AWS gestite per la crittografia e la sicurezza dei dati archiviati all'interno delle applicazioni.

Implementazione di chiavi KMS gestite dal cliente in AWS IAM Identity Center

Le chiavi gestite dal cliente sono AWS chiavi del servizio di gestione delle chiavi che puoi creare, possedere e gestire. Per implementare una chiave KMS gestita dal cliente per la crittografia inattiva in AWS IAM Identity Center, segui questi passaggi:

Important

Alcune applicazioni AWS gestite non possono essere utilizzate con AWS IAM Identity Center configurato con una chiave KMS gestita dal cliente. Per informazioni, consulta [AWS applicazioni gestite che è possibile utilizzare con IAM Identity Center](#).

1. [Fase 1: Identifica i casi d'uso per la tua organizzazione](#)- Per definire le autorizzazioni corrette per l'uso della chiave KMS è necessario identificare i casi d'uso pertinenti all'interno dell'organizzazione. Le autorizzazioni chiave KMS consistono in dichiarazioni politiche chiave KMS e politiche basate sull'identità che interagiscono per consentire ai responsabili IAM appropriati di utilizzare la chiave KMS per i loro casi d'uso specifici.
2. [Fase 2: Preparare le dichiarazioni politiche chiave del KMS](#)- Scegliete i modelli di policy chiave KMS pertinenti in base ai casi d'uso identificati nella Fase 1 e inserite gli identificatori richiesti e i nomi principali IAM. Inizia con le dichiarazioni politiche chiave del KMS di base e, se le tue politiche di sicurezza lo richiedono, perfezionale come descritto nelle dichiarazioni chiave di Advanced KMS.
3. [Fase 3: Creare una chiave KMS gestita dal cliente](#)- Crea una chiave KMS in AWS KMS che soddisfi i requisiti di IAM Identity Center e aggiungi le dichiarazioni politiche chiave del KMS preparate nella fase 2 alla politica chiave KMS.
4. [Passaggio 4: configura le politiche IAM per l'uso della chiave KMS su più account](#)- Scegli modelli di policy IAM pertinenti in base ai casi d'uso identificati nella Fase 1 e preparali per l'uso compilando l'ARN chiave. Quindi, consenti ai responsabili IAM per ogni caso d'uso specifico di utilizzare la chiave KMS per tutti gli account aggiungendo le dichiarazioni delle politiche IAM preparate alle politiche IAM dei principali.
5. [Passaggio 5: configura la chiave KMS in IAM Identity Center](#)- Abilita la chiave KMS gestita dal cliente nella tua istanza IAM Identity Center di utilizzarla per la crittografia a riposo.

Fase 1: Identifica i casi d'uso per la tua organizzazione

Prima di creare e configurare la chiave KMS gestita dal cliente, identifica i casi d'uso e prepara le autorizzazioni necessarie per la chiave KMS. Consulta la [AWS KMS Developer Guide](#) per ulteriori informazioni sulla politica delle chiavi KMS.

I presidi IAM che richiamano il servizio APIs IAM Identity Center richiedono autorizzazioni. Ad esempio, un amministratore delegato può essere autorizzato a utilizzarle APIs tramite una politica di set di autorizzazioni. Quando IAM Identity Center è configurato con una chiave gestita dal cliente, i responsabili IAM devono inoltre disporre delle autorizzazioni per utilizzare l'API KMS tramite il servizio IAM Identity Center. API KMS Queste autorizzazioni dell'API KMS vengono definite in due punti: nella policy chiave KMS e nelle politiche IAM associate ai principi IAM.

Le autorizzazioni chiave KMS sono costituite da:

1. Dichiarazioni sulla politica chiave KMS specificate nella chiave KMS durante la sua creazione in [Fase 3: Creare una chiave KMS gestita dal cliente](#)
2. Dichiarazioni sulle politiche IAM per i principi IAM specificate [Passaggio 4: configura le politiche IAM per l'uso della chiave KMS su più account](#) dopo aver creato la chiave KMS.

La tabella seguente specifica i casi d'uso e i principi IAM pertinenti che richiedono le autorizzazioni per utilizzare la chiave KMS.

Caso d'uso	Principi IAM che necessitano di autorizzazioni per utilizzare la chiave KMS	Obbligatorio/facoltativo
Utilizzo di IAM Identity AWS Center	• Amministratori di AWS IAM Identity Center • Servizio IAM Identity Center e servizio Identity Store associato	Richiesto
Utilizzo di applicazioni AWS gestite con IAM Identity Center	• Amministratori di applicazioni AWS gestite • AWS applicazioni gestite • Ruoli di servizio che le applicazioni AWS gestite assumono per	Facoltativo

Caso d'uso	Principi IAM che necessitano di autorizzazioni per utilizzare la chiave KMS	Obbligatorio/facoltativo
	chiamare il servizio IAM Identity Center APIs	
Utilizzo AWS Control Tower sull'istanza AWS IAM Identity Center che ha abilitato	AWS Control Tower amministratori	Facoltativo
Istanze AWS da SSO ad Amazon EC2 con IAM Identity Center	Responsabili IAM autorizzati a eseguire SSO su istanze Amazon EC2	Facoltativo
Qualsiasi altro caso d'uso che effettui chiamate al servizio IAM Identity Center APIs con presidi IAM, ad esempio applicazioni gestite dai clienti, flussi di lavoro per la fornitura di set di autorizzazioni, flussi di lavoro o funzioni AWS Lambda	Principi IAM utilizzati da questi flussi di lavoro per chiamare il servizio IAM Identity Center APIs	Facoltativo

Note

I principali IAM elencati nella tabella richiedono le autorizzazioni dell'API AWS KMS. Tuttavia, per proteggere i dati di utenti e gruppi in IAM Identity Center, solo i servizi IAM Identity Center e Identity Store chiamano direttamente l' AWS API KMS.

Fase 2: Preparare le dichiarazioni politiche chiave del KMS

Dopo aver identificato i casi d'uso pertinenti alla propria organizzazione, è possibile preparare le dichiarazioni politiche chiave del KMS corrispondenti.

1. Scegliete le dichiarazioni politiche chiave del KMS che corrispondono ai casi d'uso per la vostra organizzazione. Inizia con i modelli di policy di base. Se hai bisogno di politiche più specifiche in base ai tuoi requisiti di sicurezza, puoi modificare le dichiarazioni delle politiche utilizzando

gli esempi riportati in [Dichiarazioni politiche chiave di Advanced KMS](#). Per indicazioni su questa decisione, vedere [Considerazioni sulla scelta delle principali dichiarazioni politiche KMS di base rispetto a quelle avanzate](#). Inoltre, ogni sezione di base [Dichiarazioni sulla chiave KMS di base e sulle politiche IAM](#) include considerazioni pertinenti.

2. Copia le politiche pertinenti in un editor e inserisci gli identificatori richiesti e i nomi principali IAM nelle dichiarazioni politiche chiave del KMS. Per informazioni su come trovare i valori degli identificatori di riferimento, consulta. [Dove trovare gli identificatori richiesti](#)

Di seguito sono riportati i modelli di policy di base per ogni caso d'uso. Per utilizzare una chiave KMS è necessario solo il primo set di autorizzazioni per AWS IAM Identity Center. Ti consigliamo di consultare le sottosezioni applicabili per ulteriori informazioni specifiche sui casi d'uso.

- [Dichiarazioni politiche chiave di Baseline KMS per l'uso di IAM Identity Center \(obbligatorio\)](#)
- [Dichiarazioni sulla chiave KMS di base e sulle policy IAM per l'uso delle applicazioni gestite AWS](#)
- [Dichiarazione chiave KMS di base per l'uso di AWS Control Tower](#)
- [Dichiarazioni sulla chiave KMS di base e sulle policy IAM per l'uso di IAM Identity Center per le istanze Amazon EC2](#)
- [Chiave KMS di base e dichiarazioni sulle policy IAM per l'uso di flussi di lavoro personalizzati con IAM Identity Center](#)

Important

Fai attenzione quando modifichi le politiche chiave KMS per le chiavi già utilizzate da IAM Identity Center. Sebbene IAM Identity Center convalidi le autorizzazioni di crittografia e decrittografia quando configuri inizialmente una chiave KMS, non può verificare le successive modifiche alle politiche. La rimozione inavvertitamente delle autorizzazioni necessarie potrebbe interrompere il normale funzionamento dell'IAM Identity Center. Per indicazioni sulla risoluzione degli errori comuni relativi alle chiavi gestite dai clienti in IAM Identity Center, consulta. [Risolvi i problemi relativi alle chiavi gestite dal cliente in AWS IAM Identity Center](#)

Note

IAM Identity Center e l'Identity Store associato richiedono autorizzazioni a livello di servizio per utilizzare la chiave KMS gestita dal cliente. Questo requisito si estende alle applicazioni AWS gestite che richiamano il servizio IAM Identity Center utilizzando le credenziali

di servizio APIs . Per altri casi d'uso in cui il servizio IAM Identity Center APIs viene richiamato con [sessioni di accesso diretto](#), solo il principale IAM iniziante (ad esempio un amministratore) necessita delle autorizzazioni chiave KMS. In particolare, gli utenti finali che utilizzano il portale di AWS accesso e le applicazioni AWS gestite non necessitano di autorizzazioni dirette con chiave KMS, poiché vengono concesse tramite i rispettivi servizi.

Fase 3: Creare una chiave KMS gestita dal cliente

Puoi creare una chiave gestita dal cliente utilizzando la console di AWS gestione o il KMS. AWS APIs Durante la creazione della chiave, aggiungi le dichiarazioni chiave sulla politica KMS che hai preparato nel passaggio 2 alla politica chiave del KMS. Per istruzioni dettagliate, incluse indicazioni sulla politica delle chiavi KMS predefinita, consulta la [AWS Key Management Service Developer Guide](#).

La chiave deve soddisfare i seguenti requisiti:

- La chiave KMS deve trovarsi nella stessa AWS regione dell'istanza IAM Identity Center
- Puoi scegliere una chiave multiregionale o una chiave a regione singola. Tuttavia, se prevedi di utilizzare IAM Identity Center in più di un'area, Regioni AWS devi creare una chiave KMS multiregionale. Non puoi convertire una chiave KMS a regione singola in una chiave KMS multiregionale, quindi ti consigliamo di iniziare con una chiave KMS multiregionale a meno che tu non abbia l'esigenza specifica di utilizzare una chiave KMS per regione singola.
- La chiave KMS deve essere una chiave simmetrica configurata per l'utilizzo di «crittografia e decrittografia»
- La chiave KMS deve trovarsi nello stesso account di AWS Organizations gestione dell'istanza organizzativa di IAM Identity Center

Note

Se intendi replicare questa chiave KMS nelle regioni in cui desideri replicare il tuo IAM Identity Center, ti consigliamo di completare prima la configurazione in questa sezione e poi di seguire le indicazioni riportate in [the section called “Replica IAM Identity Center in un'altra regione”](#)

Passaggio 4: configura le politiche IAM per l'uso della chiave KMS su più account

Qualsiasi responsabile IAM che utilizzi il servizio IAM Identity Center APIs da un altro AWS account, ad esempio gli amministratori delegati di IAM Identity Center, necessita inoltre di una dichiarazione di policy IAM che consenta l'uso della chiave KMS attraverso questi account. APIs

Per ogni caso d'uso identificato nella fase 1:

1. Individua i modelli di policy IAM pertinenti in Baseline KMS key e IAM policy statements.
2. Copia i modelli in un editor e inserisci la chiave ARN, che è ora disponibile dopo la creazione della chiave KMS nel passaggio 3. Per informazioni su come trovare il valore ARN chiave, vedere. [Dove trovare gli identificatori richiesti](#)
3. Nella Console di gestione AWS, individua la policy IAM del principale IAM associata allo use case. La posizione di questa policy varia a seconda del caso d'uso e del modo in cui viene concesso l'accesso.
 - Per l'accesso concesso direttamente in IAM, puoi individuare i principali IAM, come i ruoli IAM, nella console IAM.
 - Per l'accesso concesso tramite IAM Identity Center, puoi individuare il set di autorizzazioni pertinente nella console IAM Identity Center.
4. Aggiungi le istruzioni di policy IAM specifiche del caso d'uso al ruolo IAM e salva la modifica.

Note

Le politiche IAM descritte qui sono politiche basate sull'identità. Sebbene tali policy possano essere associate a utenti, gruppi e ruoli IAM, consigliamo l'uso di ruoli IAM quando possibile. Consulta la guida per l'utente IAM per ulteriori informazioni sui ruoli IAM rispetto agli utenti IAM.

Configurazione aggiuntiva in alcune applicazioni AWS gestite

Alcune applicazioni AWS gestite richiedono la configurazione di un ruolo di servizio per consentire alle applicazioni di utilizzare il servizio IAM Identity Center APIs. Se la tua organizzazione utilizza applicazioni AWS gestite con IAM Identity Center, completa i seguenti passaggi per ciascuna applicazione distribuita:

1. Consulta la guida per l'utente dell'applicazione per confermare se le autorizzazioni sono state aggiornate per includere le autorizzazioni relative alla chiave KMS per l'uso dell'applicazione con IAM Identity Center.
2. In tal caso, aggiorna le autorizzazioni come indicato nella guida per l'utente dell'applicazione per evitare interruzioni delle operazioni dell'applicazione.

Note

Se non sei sicuro che un'applicazione AWS gestita utilizzi queste autorizzazioni, ti consigliamo di consultare i manuali utente di tutte le applicazioni gestite distribuite. AWS È necessario eseguire questa configurazione solo una volta per ogni applicazione che richiede la configurazione.

Passaggio 5: configura la chiave KMS in IAM Identity Center

Important

Prima di procedere con questo passaggio:

- Verifica che le tue applicazioni AWS gestite siano compatibili con le chiavi KMS gestite dal cliente. Per un elenco di applicazioni compatibili, consulta [Applicazioni AWS gestite che puoi utilizzare con IAM Identity Center](#). Se hai applicazioni incompatibili, non procedere.
- Configura le autorizzazioni necessarie per l'uso della chiave KMS. Senza le autorizzazioni appropriate, questo passaggio potrebbe fallire o interrompere l'amministrazione di IAM Identity Center, l'uso di applicazioni AWS gestite e altri casi d'uso che richiedono le autorizzazioni delle chiavi KMS. Per ulteriori informazioni, consulta [Fase 1: Identifica i casi d'uso per la tua organizzazione](#).
- Assicurati che le autorizzazioni per le applicazioni AWS gestite e le applicazioni gestite dai clienti che richiamano il servizio IAM Identity Center APIs con ruoli IAM consentano anche l'uso della chiave KMS tramite il servizio IAM Identity Center. APIs Alcune applicazioni AWS gestite richiedono la configurazione delle autorizzazioni, ad esempio un ruolo di servizio, per il loro utilizzo. APIs Consulta la Guida per l'utente di ciascuna applicazione AWS gestita distribuita per confermare se è necessario aggiungere autorizzazioni specifiche per le chiavi KMS.

Specificate una chiave KMS quando abilitate una nuova istanza organizzativa di IAM Identity Center

Quando abiliti una nuova istanza organizzativa di IAM Identity Center, puoi specificare una chiave KMS gestita dal cliente durante la configurazione. Ciò garantisce che l'istanza utilizzi la tua chiave per la crittografia inattiva sin dall'inizio. Prima di iniziare, consulta [Considerazioni sulle chiavi KMS gestite dal cliente e sulle politiche chiave KMS avanzate](#).

1. Nella pagina Abilita IAM Identity Center, espandi la sezione Encryption at rest.
2. Scegli Manage Encryption (Gestisci crittografia).
3. Scegli la chiave gestita dal cliente.
4. Per la chiave KMS, esegui una delle seguenti operazioni:
 - a. Scegli Seleziona dalle tue chiavi KMS e seleziona la chiave che hai creato dall'elenco a discesa.
 - b. Scegli Inserisci l'ARN della chiave KMS e inserisci l'ARN completo della tua chiave.
5. Scegli Save (Salva).
6. Scegli Abilita per completare la configurazione.

Per ulteriori informazioni, consulta [Enable IAM Identity Center](#).

Modifica la configurazione chiave per un'istanza organizzativa esistente di IAM Identity Center

Puoi cambiare la chiave KMS gestita dal cliente con un'altra chiave o passare a una chiave AWS di proprietà in qualsiasi momento.

Console

Per modificare la configurazione della chiave KMS

1. Apri la console IAM Identity Center all'indirizzo <https://console.aws.amazon.com/singlesignon/>.
2. Nel pannello di navigazione scegli Impostazioni.
3. Vai alla scheda Impostazioni aggiuntive.
4. Scegli Gestisci la crittografia.
5. Seleziona una delle seguenti opzioni:
 - a. Chiave gestita dal cliente: seleziona una chiave gestita dal cliente diversa dal menu a discesa o inserisci una nuova chiave ARN.

- b. AWS chiave proprietaria: passa all'opzione di crittografia predefinita.
6. Scegli Save (Salva).

AWS CLI

Per modificare un'istanza organizzativa esistente di IAM Identity Center per utilizzare la chiave gestita dal cliente KMS

```
aws sso-admin update-instance \
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
  --encryption-configuration \
    KeyType=CUSTOMER_MANAGED_KEY,KmsKeyArn=arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Per modificare un'istanza organizzativa esistente di IAM Identity Center per utilizzare una chiave AWS proprietaria

```
aws sso-admin update-instance \
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
  --encryption-configuration KeyType=AWS_OWNED_KMS_KEY
```

Considerazioni chiave gestite dal cliente

- L'aggiornamento della configurazione delle chiavi KMS per il funzionamento di IAM Identity Center non ha alcun effetto sulle sessioni utente attive nel tuo IAM Identity Center. Puoi continuare a utilizzare il portale di AWS accesso, la console IAM Identity Center e il servizio IAM Identity Center APIs durante questo processo.
- Quando si passa a una nuova chiave KMS, IAM Identity Center verifica di poter utilizzare correttamente la chiave per la crittografia e la decrittografia. Se hai commesso un errore durante la configurazione della policy chiave o della policy IAM, la console mostrerà un messaggio di errore esplicativo e la chiave KMS precedente rimarrà in uso.
- La rotazione annuale predefinita delle chiavi KMS avverrà automaticamente. Puoi fare riferimento alla [Guida per gli AWS KMS sviluppatori](#) per informazioni su argomenti come la [rotazione delle chiavi](#), il [monitoraggio delle AWS KMS chiavi](#) e il [controllo dell'accesso all'eliminazione delle chiavi](#).

Important

Se la chiave KMS gestita dal cliente utilizzata dall'istanza di IAM Identity Center viene eliminata, disabilitata o inaccessibile a causa di una politica di chiave KMS errata, gli utenti della forza lavoro e gli amministratori di IAM Identity Center non saranno in grado di utilizzare IAM Identity Center. La perdita di accesso può essere temporanea (una policy chiave può essere corretta) o permanente (una chiave eliminata non può essere ripristinata) a seconda delle circostanze. Ti consigliamo di [limitare l'accesso](#) a operazioni critiche, come l'eliminazione o la disabilitazione della chiave KMS. Inoltre, consigliamo alla tua organizzazione di impostare [procedure di accesso AWS ininterrotte per garantire che gli utenti privilegiati possano accedere](#) nel caso AWS in cui IAM Identity Center sia inaccessibile.

Dove trovare gli identificatori richiesti

Quando configuri le autorizzazioni per la tua chiave KMS gestita dal cliente, avrai bisogno di identificatori di AWS risorsa specifici per completare i modelli di policy chiave e di dichiarazione delle policy IAM. Inserisci gli identificatori richiesti (ad esempio, l'ID dell'organizzazione) e i nomi principali IAM nelle dichiarazioni politiche chiave del KMS.

Di seguito è riportata una guida per individuare questi identificatori nella console di gestione. AWS

IAM Identity Center Amazon Resource Name (ARN) e Identity Store ARN

Un'istanza di IAM Identity Center è una AWS risorsa con un proprio ARN univoco come `arn:aws:sso: :instance/ssoins-1234567890abcdef`. L'ARN segue lo schema documentato nella sezione dei tipi di risorse di IAM Identity Center del Service Authorization Reference.

A ogni istanza di IAM Identity Center è associato un Identity Store che memorizza le identità degli utenti e dei gruppi. Un Identity Store ha un identificatore univoco chiamato Identity Store ID (ad esempio, `d-123456789a`). L'ARN segue lo schema documentato nella sezione dei tipi di risorse Identity Store del [Service](#) Authorization Reference.

Puoi trovare i valori ARN e Identity Store ID nella pagina Impostazioni del tuo IAM Identity Center. L'ID Identity Store si trova nella scheda Identity source.

AWS Organizations ID

Se desideri specificare un ID dell'organizzazione (ad esempio, `o-example.org1`) nella tua policy chiave, puoi trovarne il valore nella pagina Impostazioni delle console IAM Identity Center and

Organizations. L'ARN segue lo schema documentato nella sezione Organizations resource types del Service Authorization Reference.

Chiave KMS ARN

Puoi trovare l'ARN di una chiave KMS nella console. AWS KMS Scegli Chiavi gestite dal cliente a sinistra, fai clic sulla chiave di cui desideri cercare l'ARN e la vedrai nella sezione Configurazione generale. L'ARN segue lo schema documentato nella sezione sui tipi di AWS KMS risorse del Service Authorization Reference.

Consulta la Guida per gli AWS Key Management Service sviluppatori per ulteriori informazioni sulle politiche chiave AWS KMS e sulla risoluzione dei problemi relativi AWS KMS alle autorizzazioni. Per ulteriori informazioni sulle policy IAM e sulla loro rappresentazione in JSON, consulta la IAM User Guide.

Dichiarazioni sulla chiave KMS di base e sulle politiche IAM

La chiave KMS di base e le politiche basate sull'identità fornite qui fungono da base per requisiti comuni. Ti consigliamo inoltre di verificare [Dichiarazioni politiche chiave di Advanced KMS](#) che forniscano controlli di accesso più granulari, ad esempio garantendo che la chiave KMS sia accessibile solo a una specifica istanza o applicazione gestita di IAM Identity Center. AWS Prima di utilizzare le dichiarazioni politiche chiave avanzate di KMS, consulta il [Considerazioni sulla scelta delle principali dichiarazioni politiche KMS di base rispetto a quelle avanzate](#)

Le seguenti sezioni forniscono le dichiarazioni politiche di base per ogni caso d'uso. Espandi le sezioni che corrispondono ai tuoi casi d'uso e copia le dichiarazioni politiche chiave del KMS. Quindi, torna a [Fase 2: Preparare le dichiarazioni politiche chiave del KMS](#)

Dichiarazioni politiche chiave di Baseline KMS per l'uso di IAM Identity Center (obbligatorio)

Utilizza il seguente modello di dichiarazione di policy chiave KMS [Fase 2: Preparare le dichiarazioni politiche chiave del KMS](#) per consentire agli amministratori di IAM Identity Center, dell'Identity Store associato e dell'IAM Identity Center di utilizzare la chiave KMS.

- Nell'elemento Principal for administrator policy statement, specifica i principali AWS account degli account di amministrazione di IAM Identity Center, che sono l'account di gestione dell' AWS organizzazione e l'account di amministrazione delegata, utilizzando il formato «arn:aws:iam: :111122223333:root».
- Nell' PrincipalArn elemento, sostituisci l'esempio con i ruoli IAM degli amministratori di IAM Identity Center. ARNs

Puoi specificare uno dei seguenti elementi:

- Ruolo IAM specifico ARN:

```
"arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/ap-southeast-2/AWSReservedSSO_permsetname_12345678"
```

- Pattern Wildcard (consigliato):

```
"arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/ap-southeast-2/AWSReservedSSO_permsetname_*"
```

L'uso del wildcard (*) previene la perdita di accesso se il set di autorizzazioni viene eliminato e ricreato, poiché Identity Center genera nuovi identificatori univoci per i set di autorizzazioni ricreati. Per un esempio di implementazione, vedere. [Esempio di politica di fiducia personalizzata](#)

- Nell' SourceAccount elemento, specifica l'ID dell'account IAM Identity Center.
- Identity Store dispone di un proprio service `principalidentitystore.amazonaws.com`, al quale deve essere consentito di utilizzare la chiave KMS.
- Queste dichiarazioni politiche consentono alle istanze IAM Identity Center in un AWS account specifico di utilizzare la chiave KMS. Per limitare l'accesso a una specifica istanza di IAM Identity Center, consulta. [Dichiarazioni politiche chiave di Advanced KMS](#) Puoi avere solo un'istanza IAM Identity Center per ogni AWS account.

Dichiarazioni politiche chiave di KMS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root"
        ]
      },
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",

```

```

    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
        "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
      ]
    }
  },
  "StringLike": {
    "kms:ViaService": "sso.*.amazonaws.com",
    "kms:EncryptionContext:aws:sso:instance-arn": "*"
  }
},
{
  "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityStore",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:root",
      "arn:aws:iam::444455556666:root"
    ]
  },
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
        "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
      ]
    }
  },
  "StringLike": {
    "kms:ViaService": "identitystore.*.amazonaws.com",

```

```

        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
    }
}
},
{
    "Sid": "AllowIAMIdentityCenterAdminToDescribeTheKMSKey",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root"
        ]
    },
    "Action": "kms:DescribeKey",
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_Admin_*",
                "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_DelegatedAdmin_*"
            ]
        }
    }
},
{
    "Sid": "AllowIAMIdentityCenterToUseTheKMSKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "sso.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "kms:EncryptionContext:aws:sso:instance-arn": "*"
        },
        "StringEquals": {

```

```
        "aws:SourceAccount": "111122223333"
    }
}
},
{
    "Sid": "AllowIdentityStoreToUseTheKMSKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "identitystore.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        },
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        }
    }
},
{
    "Sid": "AllowIAMIdentityCenterAndIdentityStoreToDescribeKMSKey",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "identitystore.amazonaws.com",
            "sso.amazonaws.com"
        ]
    },
    "Action": "kms:DescribeKey",
    "Resource": "*"
}
]
```


Utilizza il seguente modello di dichiarazione delle politiche IAM [the section called “Fase 4: Configurazione delle politiche IAM”](#) per consentire agli amministratori di IAM Identity Center di utilizzare la chiave KMS.

- Sostituisci la chiave di esempio ARN nell'`Resource` elemento con la tua chiave KMS ARN effettiva. Per informazioni su come trovare i valori degli identificatori di riferimento, consulta. [Dove trovare gli identificatori richiesti](#)
- Queste dichiarazioni politiche IAM concedono l'accesso tramite chiave KMS al principale IAM, ma non limitano il AWS servizio che può effettuare la richiesta. La policy chiave KMS prevede in genere queste restrizioni di servizio. Tuttavia, puoi aggiungere un contesto di crittografia a questa policy IAM per limitare l'utilizzo a una specifica istanza di Identity Center. Fare riferimento a [Dichiarazioni politiche chiave di Advanced KMS](#) per ulteriori dettagli.

Dichiarazioni di policy IAM richieste per gli amministratori delegati di IAM Identity Center

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "IAMPolicyToAllowIAMIdentityCenterAdminToUseKMSkey",
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:GenerateDataKeyWithoutPlaintext",
      "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  {
    "Sid": "IAMPolicyToAllowIAMIdentityCenterAdminToListKeyAliases",
    "Effect": "Allow",
    "Action": "kms:ListAliases",
    "Resource": "*"
  }
]
```

Dichiarazioni sulla chiave KMS di base e sulle policy IAM per l'uso delle applicazioni gestite AWS

Note

Alcune applicazioni AWS gestite non possono essere utilizzate con IAM Identity Center configurato con una chiave KMS gestita dal cliente. Per ulteriori informazioni, consulta [Applicazioni AWS gestite che funzionano con IAM Identity Center](#).

Utilizza il seguente modello di dichiarazione di policy chiave KMS [Fase 2: Preparare le dichiarazioni politiche chiave del KMS](#) per consentire sia alle applicazioni AWS gestite che ai relativi amministratori di utilizzare la chiave KMS.

- Inserisci il tuo AWS Organizations ID nell'ID e nelle condizioni PrincipalOrg. SourceOrgId Per informazioni su come trovare i valori degli identificatori di riferimento, consulta. [Dove trovare gli identificatori richiesti](#)
- Queste dichiarazioni politiche consentono a tutte le applicazioni AWS gestite e a tutti i responsabili IAM (amministratori delle applicazioni) dell' AWS organizzazione di utilizzare kms: Decrypt utilizzando IAM Identity Center e Identity Store. Per limitare queste dichiarazioni politiche a specifiche applicazioni AWS gestite, account o istanze IAM Identity Center, consulta. [Dichiarazioni politiche chiave di Advanced KMS](#)

Puoi limitare l'accesso a specifici amministratori di applicazioni sostituendoli * con principi IAM specifici. Per proteggerti dalle modifiche ai nomi dei ruoli IAM quando vengono ricreati i set di autorizzazioni, utilizza l'approccio descritto in. [Esempio di politica di fiducia personalizzata](#) Per ulteriori informazioni, consulta [Considerazioni sulla scelta delle principali dichiarazioni politiche KMS di base rispetto a quelle avanzate](#).

Dichiarazioni politiche chiave di KMS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
      "Resource": "*",
    }
  ]
}
```

```

    "Condition": {
      "StringEquals": {
        "aws:PrincipalOrgID": "o-a1b2c3d4e5"
      },
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:PrincipalOrgID": "o-a1b2c3d4e5"
      },
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      },
      "StringEquals": {
        "aws:SourceOrgID": "o-a1b2c3d4e5"
      }
    }
  }
}

```

```

    },
    {
      "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        },
        "StringEquals": {
          "aws:SourceOrgID": "o-a1b2c3d4e5"
        }
      }
    }
  ]
}

```

Utilizza il seguente modello di dichiarazione delle politiche IAM [Passaggio 4: configura le politiche IAM per l'uso della chiave KMS su più account](#) per consentire agli amministratori delle applicazioni AWS gestite di utilizzare la chiave KMS di un account membro.

- Sostituisci l'ARN di esempio nell'elemento Resource con la tua chiave KMS ARN effettiva. Per informazioni su come trovare i valori degli identificatori di riferimento, vedere. [Dove trovare gli identificatori richiesti](#)
- Alcune applicazioni AWS gestite richiedono la configurazione delle autorizzazioni per il servizio IAM Identity Center. APIs Prima di configurare una chiave gestita dal cliente in IAM Identity Center, verifica che queste autorizzazioni consentano anche l'uso della chiave KMS. Per requisiti specifici di autorizzazione delle chiavi KMS, consulta la documentazione per ogni applicazione AWS gestita che hai distribuito.

Dichiarazioni politiche IAM richieste per gli amministratori delle AWS applicazioni gestite:

```

{
  "Version": "2012-10-17",
  "Statement": [{

```

```

    "Sid":
    "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
        "StringLike": {
            "kms:ViaService": [
                "sso.*.amazonaws.com",
                "identitystore.*.amazonaws.com"
            ]
        }
    }
}

```

Dichiarazione chiave KMS di base per l'uso di AWS Control Tower

Utilizza i seguenti modelli di istruzioni chiave KMS [Fase 2: Preparare le dichiarazioni politiche chiave del KMS](#) per consentire agli amministratori di AWS Control Tower di utilizzare la chiave KMS.

- Nell'elemento Principal, specifica i principi IAM utilizzati per l'accesso al servizio IAM Identity Center. APIs Per ulteriori informazioni sui principi IAM, consulta [Specifying a principal](#) nella IAM User Guide.
- Queste dichiarazioni politiche consentono agli amministratori di AWS Control Tower di utilizzare la chiave KMS tramite qualsiasi istanza di IAM Identity Center. Tuttavia, AWS Control Tower limita l'accesso all'istanza organizzativa di IAM Identity Center nella stessa AWS organizzazione. A causa di questa restrizione, non vi è alcun vantaggio pratico nel limitare ulteriormente la chiave KMS a un'istanza specifica di IAM Identity Center, come descritto in. [Dichiarazioni politiche chiave di Advanced KMS](#)
- Per proteggerti dalle modifiche ai nomi dei ruoli IAM quando vengono ricreati i set di autorizzazioni, utilizza l'approccio descritto in. [Esempio di politica di fiducia personalizzata](#)

Dichiarazione della policy della chiave KMS:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```

    "Sid": "AllowControlTowerAdminRoleToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/AWSControlTowerAdmin"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowControlTowerAdminRoleToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/AWSControlTowerAdmin"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  }
]
}

```

AWS Control Tower non supporta l'amministrazione delegata e, pertanto, non è necessario configurare una policy IAM per i suoi amministratori.

Important

La precedente dichiarazione sulla politica riguarda le operazioni AWS Control Tower gestite dai servizi, come la registrazione automatica degli account, dove assume il ruolo. AWS Control Tower `AWSControlTowerAdmin`. Tuttavia, per le operazioni avviate dal cliente, come il provisioning degli account tramite Account Factory o le chiamate AWS Control Tower APIs dirette, AWS Control Tower utilizza [sessioni di accesso inoltrato \(FAS\)](#) e opera secondo

il ruolo IAM del cliente. Ciò significa che il ruolo IAM utilizzato per avviare queste operazioni necessita anche delle `kms:Decrypt` autorizzazioni sulla chiave KMS gestita dal cliente. Aggiungi le seguenti dichiarazioni politiche chiave di KMS insieme alle dichiarazioni precedenti. `AWSControlTowerAdmin` Sostituisci *MyControlTowerRole* con l'ARN del ruolo IAM con cui utilizzi per interagire AWS Control Tower, ad esempio un ruolo del set di autorizzazioni IAM Identity Center (ad esempio, `AWSReservedSSO_PermissionSetName_*`), un ruolo IAM personalizzato per l'automazione o qualsiasi altro ruolo utilizzato per chiamare AWS Control Tower o. AWS Service Catalog APIs

Dichiarazione politica chiave di KMS per le operazioni avviate dal cliente AWS Control Tower :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCustomerRoleToUseTheKMSKeyViaIdentityCenterForControlTower",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyControlTowerRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
      }
    },
    {
      "Sid": "AllowCustomerRoleToUseTheKMSKeyViaIdentityStoreForControlTower",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyControlTowerRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
```

```

        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
    }
}
]
}

```

Dichiarazioni sulla chiave KMS di base e sulle policy IAM per l'uso di IAM Identity Center per le istanze Amazon EC2

Utilizza il seguente modello di dichiarazione sulla politica delle chiavi KMS [Fase 2: Preparare le dichiarazioni politiche chiave del KMS](#) per consentire agli utenti di Single Sign-On (SSO) per le istanze Amazon EC2 di utilizzare la chiave KMS tra gli account.

- Specificare i principali IAM utilizzati per l'accesso a IAM Identity Center nel campo Principal. Per ulteriori informazioni sui principi IAM, consulta [Specifying a principal](#) nella IAM User Guide.
- Questa dichiarazione politica consente a qualsiasi istanza IAM Identity Center di utilizzare la chiave KMS. Per limitare l'accesso a una specifica istanza di IAM Identity Center, consulta [Dichiarazioni politiche chiave di Advanced KMS](#)
- Per proteggerti dalle modifiche ai nomi dei ruoli IAM quando vengono ricreati i set di autorizzazioni, utilizza l'approccio descritto nell'esempio della politica di fiducia personalizzata.

Dichiarazione della policy della chiave KMS

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIAMIdentityCenterPermissionSetRoleToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_MyPermissionSet_1a2b3c4d5e6f7g8h"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",

```



```

        "kms:EncryptionContext:aws:sso:instance-arn": "*"
    }
},
{
    "Sid": "AllowIAMIdentityCenterPermissionSetRoleToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_MyPermissionSet_1a2b3c4d5e6f7g8h"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "kms:ViaService": "identitystore.*.amazonaws.com",
            "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        }
    }
}
]
}

```

Utilizza il seguente modello di dichiarazione di policy IAM [Passaggio 4: configura le politiche IAM per l'uso della chiave KMS su più account](#) per consentire alle istanze da SSO a EC2 di utilizzare la chiave KMS.

Allega la dichiarazione della policy IAM al set di autorizzazioni esistente in IAM Identity Center che stai utilizzando per consentire l'accesso SSO alle istanze Amazon EC2. Per esempi di policy IAM, consulta le [connessioni Remote Desktop Protocol](#) nella AWS Systems Manager User Guide.

- Sostituisci l'ARN di esempio nell'elemento Resource con la tua chiave KMS ARN effettiva. Per informazioni su come trovare i valori degli identificatori di riferimento, vedere. [Dove trovare gli identificatori richiesti](#)

Policy IAM relativa al set di autorizzazioni:

```

{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "IAMPolicyToAllowKMSKeyUseViaIdentityCenterAndIdentityStore",

```

```

    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
        ]
      }
    }
  }
}

```

Chiave KMS di base e dichiarazioni sulle policy IAM per l'uso di flussi di lavoro personalizzati con IAM Identity Center

Utilizza i seguenti modelli di dichiarazioni politiche chiave KMS [Fase 2: Preparare le dichiarazioni politiche chiave del KMS](#) per consentire ai flussi di lavoro personalizzati, come le applicazioni gestite dai clienti, nell'account di AWS Organizations gestione o nell'account di amministrazione delegata di utilizzare la chiave KMS. Tieni presente che la federazione SAML nelle applicazioni gestite dai clienti non richiede le autorizzazioni relative alle chiavi KMS.

- Nell'elemento Principal, specifica i principi IAM utilizzati per accedere al servizio IAM Identity Center. APIs Per ulteriori informazioni sui principi IAM, consulta [Specifying a principal](#) nella IAM User Guide.
- Queste dichiarazioni politiche consentono al flusso di lavoro di utilizzare la chiave KMS tramite qualsiasi istanza di IAM Identity Center. Per limitare l'accesso a una specifica istanza di IAM Identity Center, consulta. [Dichiarazioni politiche chiave di Advanced KMS](#)
- Per proteggerti dalle modifiche ai nomi dei ruoli IAM quando vengono ricreati i set di autorizzazioni, utilizza l'approccio descritto in. [Esempio di politica di fiducia personalizzata](#)

Dichiarazione della policy della chiave KMS:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityCenter",

```

```

    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/MyCustomWorkflowRole"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/MyCustomWorkflowRole"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  }
]
}

```

Utilizza il seguente modello di dichiarazione delle politiche IAM [Passaggio 4: configura le politiche IAM per l'uso della chiave KMS su più account](#) per consentire al principale IAM associato al flusso di lavoro personalizzato di utilizzare la chiave KMS tra gli account. Aggiungi la dichiarazione di policy IAM all'IAM principal.

- Sostituisci l'ARN di esempio nell'elemento Resource con la tua chiave KMS ARN effettiva. Per informazioni su come trovare i valori degli identificatori di riferimento, vedere. [Dove trovare gli identificatori richiesti](#)

Dichiarazione sulla politica IAM (richiesta solo per l'utilizzo su più account):

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
        ]
      }
    }
  }]
}
```

Esempi di dichiarazioni politiche chiave di KMS per casi d'uso comuni

IAM Identity Center con amministratori delegati e applicazioni gestite AWS

Questa sezione contiene esempi di dichiarazioni politiche chiave KMS che è possibile utilizzare per un'istanza di IAM Identity Center con amministratori delegati e applicazioni gestite. AWS

Important

Le dichiarazioni politiche chiave del KMS presuppongono che l'istanza di IAM Identity Center non venga utilizzata in altri casi d'uso che richiedono le autorizzazioni della chiave KMS. [Per confermare, puoi esaminare tutti i casi d'uso.](#) Inoltre, per confermare se le applicazioni AWS gestite richiedono una configurazione aggiuntiva, consulta [the section called “Configurazione aggiuntiva in alcune applicazioni AWS gestite”](#)

Copia le dichiarazioni chiave sulla politica KMS sotto la tabella e aggiungile alla politica chiave del KMS. Questo esempio utilizza i seguenti valori di esempio:

- 111122223333- ID account dell'istanza IAM Identity Center
- 444455556666- ID dell'account di amministrazione delegato

- o-a1b2c3d4e5- ID AWS dell'organizzazione
- `arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_Admin_*`- Un pattern jolly del ruolo IAM di un amministratore di IAM Identity Center fornito dal set di autorizzazioni. *Admin* Tale ruolo contiene il codice regionale della regione principale (us-east-1 in questo esempio).
- `arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_DelegatedAdmin_*`- Un pattern jolly del ruolo IAM di un amministratore delegato di IAM Identity Center fornito dal set di autorizzazioni. *DelegatedAdmin* Tale ruolo contiene il codice regionale della regione principale (us-east-1 in questo esempio).

Se il ruolo IAM non è stato generato da un set di autorizzazioni, il ruolo IAM avrà l'aspetto di un ruolo normale, ad esempio. `arn:aws:iam::111122223333:role/idcadmin`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root"
        ]
      },
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_Admin_*",
            "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_DelegatedAdmin_*"
          ]
        }
      }
    }
  ],
}
```

```

    "StringLike": {
      "kms:ViaService": "sso.*.amazonaws.com",
      "kms:EncryptionContext:aws:sso:instance-arn": "*"
    }
  },
  {
    "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::111122223333:root",
        "arn:aws:iam::444455556666:root"
      ]
    },
    "Action": [
      "kms:Decrypt",
      "kms:Encrypt",
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
      "ArnLike": {
        "aws:PrincipalArn": [
          "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_Admin_*",
          "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_DelegatedAdmin_*"
        ]
      }
    },
    "StringLike": {
      "kms:ViaService": "identitystore.*.amazonaws.com",
      "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
    }
  }
],
{
  "Sid": "AllowIAMIdentityCenterAdminToDescribeTheKMSKey",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:root",
      "arn:aws:iam::444455556666:root"
    ]
  }
}

```

```

    },
    "Action": "kms:DescribeKey",
    "Resource": "*",
    "Condition": {
      "ArnLike": {
        "aws:PrincipalArn": [
          "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
          "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
        ]
      }
    }
  },
  {
    "Sid": "AllowIAMIdentityCenterToUseTheKMSKey",
    "Effect": "Allow",
    "Principal": {
      "Service": "sso.amazonaws.com"
    },
    "Action": [
      "kms:Decrypt",
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom",
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      },
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      }
    }
  },
  {
    "Sid": "AllowIdentityStoreToUseTheKMSKey",
    "Effect": "Allow",
    "Principal": {
      "Service": "identitystore.amazonaws.com"
    },
    "Action": [
      "kms:Decrypt",

```

```

        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        },
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        }
    }
},
{
    "Sid": "AllowIAMIdentityCenterAndIdentityStoreToDescribeKMSKey",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "identitystore.amazonaws.com",
            "sso.amazonaws.com"
        ]
    },
    "Action": "kms:DescribeKey",
    "Resource": "*"
},

{
    "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "o-a1b2c3d4e5"
        },
        "StringLike": {
            "kms:ViaService": "sso.*.amazonaws.com",
            "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
    }
},
{

```



```

    "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:PrincipalOrgID": "o-a1b2c3d4e5"
      },
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      },
      "StringEquals": {
        "aws:SourceOrgID": "o-a1b2c3d4e5"
      }
    }
  },
  {
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  }
}

```

```

    },
    "Bool": {
      "aws:PrincipalIsAWSService": "true"
    },
    "StringEquals": {
      "aws:SourceOrgID": "o-a1b2c3d4e5"
    }
  }
}
]
}

```

Dichiarazioni politiche chiave di Advanced KMS

Utilizza le dichiarazioni politiche chiave avanzate per implementare controlli di accesso più granulari per la chiave KMS gestita dal cliente. Queste politiche si basano sull'aggiunta di condizioni [Dichiarazioni sulla chiave KMS di base e sulle politiche IAM](#) di contesto di crittografia e restrizioni specifiche del servizio. Prima di decidere se utilizzare le dichiarazioni chiave avanzate sulle politiche KMS, assicurati di esaminare le considerazioni pertinenti.

Utilizzo del contesto di crittografia per limitare l'accesso

Puoi limitare l'utilizzo della chiave KMS a una specifica istanza di IAM Identity Center specificando una condizione del contesto di crittografia nelle istruzioni chiave delle policy. Le dichiarazioni politiche chiave di base includono già questo contesto con un valore generico. Sostituisci il carattere jolly «*» con l'ARN e l'ARN di Identity Store di un'istanza di Identity Center specifici per assicurarti che la chiave funzioni solo con l'istanza desiderata. Puoi anche aggiungere le stesse condizioni di contesto di crittografia alla policy IAM configurata per l'uso della chiave KMS su più account.

Centro identità

```

"StringEquals": {
  "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
}

```

Archivio identità

```

"StringEquals": {

```

```
"kms:EncryptionContext:aws:identitystore:identitystore-arn":  
  "arn:aws:identitystore::111122223333:identitystore/d-1234567890"  
}
```

Se hai bisogno di aiuto per trovare questi identificatori, consulta. [Dove trovare gli identificatori richiesti](#)

Note

Puoi utilizzare una chiave KMS gestita dal cliente solo con un'istanza organizzativa di IAM Identity Center. La chiave gestita dal cliente deve trovarsi nell'account di gestione dell' AWS organizzazione, il che aiuta a garantire che venga utilizzata con una singola istanza di IAM Identity Center. Tuttavia, il meccanismo del contesto di crittografia fornisce una protezione tecnica indipendente per l'utilizzo di una singola istanza. È inoltre possibile utilizzare la chiave di `aws:SourceArn` condizione nelle dichiarazioni politiche chiave del KMS destinate ai principali servizi Identity Center e Identity Store.

Considerazioni sull'implementazione delle condizioni del contesto di crittografia

Prima di implementare le condizioni del contesto di crittografia, esamina questi requisiti:

- **DescribeKey azione.** Il contesto di crittografia non può essere applicato all'azione «kms:DescribeKey», che può essere utilizzata dagli amministratori di IAM Identity Center. Quando configuri la policy delle chiavi KMS, escludi il contesto di crittografia per questa azione specifica per garantire il corretto funzionamento dell'istanza di IAM Identity Center.
- **Configurazione di una nuova istanza.** Se stai abilitando una nuova istanza IAM Identity Center con una chiave KMS gestita dal cliente, vedi [Considerazioni sulle chiavi KMS gestite dal cliente e sulle politiche chiave KMS avanzate](#).
- **Modifiche alla fonte dell'identità.** Quando si modifica l'origine dell'identità da o verso Active Directory, il contesto di crittografia richiede un'attenzione speciale. Per informazioni, consulta [Considerazioni sulla modifica dell'origine dell'identità](#).

Modelli di policy

Scegli tra questi modelli di policy avanzati in base ai tuoi requisiti di sicurezza. Bilancia i controlli granulari degli accessi con il sovraccarico amministrativo che introducono.

Argomenti trattati qui:

- [Dichiarazioni sulle policy KMS per l'uso in sola lettura di un'istanza specifica di IAM Identity Center](#). Questa sezione illustra l'uso del contesto di crittografia per l'accesso in sola lettura a IAM Identity Center.
- [Dichiarazioni politiche chiave raffinate di KMS per l'uso delle applicazioni gestite AWS](#). Questa sezione illustra come perfezionare le politiche delle chiavi KMS per le applicazioni AWS gestite utilizzando il contesto di crittografia e le informazioni sull'applicazione, come il principale del servizio dell'applicazione, l'ARN dell'applicazione e l'ID dell'account. AWS

Dichiarazioni sulle policy KMS per l'uso in sola lettura di un'istanza specifica di IAM Identity Center

Questa policy consente [ai revisori di sicurezza](#) e ad altro personale che necessita solo dell'accesso in lettura a IAM Identity Center di utilizzare la chiave KMS.

Per utilizzare questa politica:

1. Sostituisci l'esempio di amministratore IAM principals di sola lettura con i tuoi amministratori IAM principals effettivi
2. Sostituisci l'ARN dell'istanza IAM Identity Center di esempio con l'ARN dell'istanza attuale
3. Sostituisci l'esempio di Identity Store ARN con l'attuale ARN di Identity Store
4. Se si utilizza l'amministrazione [delegata, vedere](#) [Passaggio 4: configura le politiche IAM per l'uso della chiave KMS su più account](#)

Se hai bisogno di aiuto per trovare i valori di questi identificatori, consulta. [Dove trovare gli identificatori richiesti](#)

Dopo aver aggiornato il modello con i tuoi valori, torna [Fase 2: Preparare le dichiarazioni politiche chiave del KMS](#) a preparare le dichiarazioni politiche chiave del KMS aggiuntive, se necessario.

L'azione kms: Decrypt da sola non limita l'accesso alle operazioni di sola lettura. La policy IAM deve imporre l'accesso in sola lettura al servizio IAM Identity Center. APIs

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadOnlyAccessToIdentityCenterAPI",
      "Effect": "Allow",
```

```

    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
      }
    }
  },
  {
    "Sid": "AllowReadOnlyAccessToIdentityStoreAPI",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
      }
    }
  }
]
}

```

Dichiarazioni politiche chiave raffinate di KMS per l'uso delle applicazioni gestite AWS

Questi modelli di policy forniscono un controllo più granulare su quali applicazioni AWS gestite possono utilizzare la chiave KMS.

Note

Alcune applicazioni AWS gestite non possono essere utilizzate con IAM Identity Center configurato con una chiave KMS gestita dal cliente. Scopri [le applicazioni AWS gestite che puoi utilizzare con IAM Identity Center](#).

[Dichiarazioni sulla chiave KMS di base e sulle policy IAM per l'uso delle applicazioni gestite](#)

[AWS](#) Consenti AWS a qualsiasi applicazione gestita di qualsiasi account della stessa AWS organizzazione di utilizzare la chiave KMS. Utilizza queste politiche raffinate per limitare l'accesso in base a:

- Responsabile del servizio applicativo
- Istanza dell'applicazione ARNs
- AWS account IDs
- Contesto di crittografia per istanze IAM Identity Center specifiche

Note

Un service principal è un identificatore univoco per un AWS servizio, in genere formattato come `servicename.amazonaws.com` (ad esempio, `elasticmapreduce.amazonaws.com` per Amazon EMR).

Limita per account

Questo modello di dichiarazione delle politiche chiave KMS consente AWS a un'applicazione gestita in AWS account specifici di utilizzare la chiave KMS utilizzando un'istanza specifica di IAM Identity Center.

Per utilizzare questa politica:

1. Sostituisci il service principal di esempio con il service principal effettivo dell'applicazione
2. Sostituisci l'account di esempio IDs con l'account effettivo IDs in cui vengono AWS distribuite le applicazioni gestite
3. Sostituisci l'esempio di Identity Store ARN con l'attuale ARN di Identity Store
4. Sostituisci l'ARN dell'istanza IAM Identity Center di esempio con l'ARN dell'istanza attuale

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
```

```

    "Principal": {
      "Service": "myapp.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": [
          "111122223333",
          "444455556666"
        ]
      },
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      }
    },
  },
  {
    "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "Service": "myapp.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": [
          "111122223333",
          "444455556666"
        ]
      },
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore:::111122223333:identitystore/d-1234567890"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      }
    }
  }
}

```

```

    }
  }
}
]
}

```

Limita per istanza dell'applicazione

Questo modello di dichiarazione di policy chiave KMS consente a una specifica istanza di applicazione AWS gestita di utilizzare la chiave KMS utilizzando un'istanza specifica di IAM Identity Center.

Per utilizzare questa policy:

1. Sostituisci il service principal di esempio con il service principal effettivo dell'applicazione
2. Sostituisci l'ARN dell'applicazione di esempio con l'ARN dell'istanza dell'applicazione effettiva
3. Sostituisci l'esempio di Identity Store ARN con l'attuale ARN di Identity Store
4. Sostituisci l'ARN dell'istanza IAM Identity Center di esempio con l'ARN dell'istanza attuale

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-application"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-1234567890abcdef"
        },
        "Bool": {

```



```

        "aws:PrincipalIsAWSService": "true"
    }
}
},
{
    "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
        "Service": "myapp.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-
application"
        },
        "StringLike": {
            "kms:ViaService": "identitystore.*.amazonaws.com",
            "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        },
        "Bool": {
            "aws:PrincipalIsAWSService": "true"
        }
    }
}
]
}

```

Considerazioni sulle chiavi KMS gestite dal cliente e sulle politiche chiave KMS avanzate

Quando implementi chiavi KMS gestite dal cliente con IAM Identity Center, considera questi fattori che influiscono sulla configurazione, sulla sicurezza e sulla manutenzione continua della configurazione di crittografia.

Considerazioni sulla scelta delle principali dichiarazioni politiche KMS di base rispetto a quelle avanzate

Quando decidi se rendere più specifico l'utilizzo delle autorizzazioni chiave KMS [Dichiarazioni politiche chiave di Advanced KMS](#), considera il sovraccarico di gestione e le esigenze di sicurezza

della tua organizzazione. Dichiarazioni politiche più specifiche forniscono un controllo più preciso su chi può utilizzare la chiave e per quali scopi; tuttavia, richiedono una manutenzione continua man mano che la configurazione di IAM Identity Center si evolve. Ad esempio, se limiti l'uso della chiave KMS a specifiche implementazioni di applicazioni AWS gestite, dovrai aggiornare la policy chiave ogni volta che l'organizzazione desidera distribuire o annullare la distribuzione di un'applicazione. Policy meno restrittive riducono l'onere amministrativo, ma possono concedere autorizzazioni più ampie di quelle necessarie per i requisiti di sicurezza.

Considerazioni sull'abilitazione di una nuova istanza IAM Identity Center con una chiave KMS gestita dal cliente

Le considerazioni riportate qui si applicano se si utilizza il contesto di crittografia descritto in [Dichiarazioni politiche chiave di Advanced KMS](#) per limitare l'uso della chiave KMS a una specifica istanza di IAM Identity Center.

Quando si abilita una nuova istanza IAM Identity Center con una chiave KMS gestita dal cliente, IAM Identity Center e Identity Store ARNs sono disponibili solo dopo la configurazione. Sono disponibili le seguenti opzioni:

- Utilizzate temporaneamente modelli ARN generici, quindi sostituiteli con completi ARNs dopo l'attivazione dell'istanza. Ricordatevi di passare da un StringLike operatore StringEquals all'altro secondo necessità.
 - Per IAM Identity Center SPN: «arn: \$ {Partition} :sso: ::instance/*».
 - Per Identity Store SPN: «arn: \$ {Partition} :identitystore: :\$ {Account} :identitystore/*».
- Usa temporaneamente «Purpose:key_configuration» nell'ARN. Funziona solo per l'abilitazione delle istanze e deve essere sostituita con l'ARN effettivo affinché l'istanza IAM Identity Center funzioni normalmente. Il vantaggio di questo approccio è che non puoi dimenticare di sostituirlo dopo aver abilitato l'istanza.
 - Per IAM Identity Center SPN, usa: «arn: \$ {Partition} :sso: :instance/purpose:key_configuration»
 - Per Identity Store SPN, usa: «arn: \$ {Partition} :identitystore: :\$ {Account} :identitystore/purpose:key_configuration»

 Important

Non applicare questa configurazione a una chiave KMS già in uso in un'istanza IAM Identity Center esistente, poiché potrebbe interromperne le normali operazioni.

- Ometti la condizione del contesto di crittografia dalla politica della chiave KMS fino a quando l'istanza non è abilitata.

Taggare le risorse AWS IAM Identity Center

Un tag è un'etichetta di attributo personalizzata che aggiungi a una AWS risorsa per semplificare l'identificazione, l'organizzazione e la ricerca di 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 è possibile impostare il valore di un tag su null. Non specificare il valore del tag equivale a utilizzare una stringa vuota.

I tag ti aiutano a identificare e organizzare AWS le tue risorse. Molti AWS servizi supportano l'etichettatura, quindi puoi assegnare lo stesso tag a risorse di servizi diversi per indicare che le risorse 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 AWS Guida 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.

Puoi applicare i tag solo ai set di autorizzazioni. Non è possibile applicare tag ai ruoli corrispondenti in cui IAM Identity Center crea Account AWS. Puoi utilizzare la console IAM Identity Center AWS CLI o IAM Identity Center APIs per aggiungere, modificare o eliminare i tag per un set di autorizzazioni.

Le seguenti sezioni forniscono ulteriori informazioni sui tag per IAM Identity Center.

Argomenti

- [Limitazioni applicate ai tag](#)
- [Gestisci i tag utilizzando la console IAM Identity Center](#)
- [AWS CLI esempi](#)
- [Gestisci i tag utilizzando l'API 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 `@`
- Le chiavi e i valori fanno distinzione tra maiuscole e minuscole.
- Non utilizzare `aws:` come prefisso per le chiavi; è riservato all'uso 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 Centro identità IAM](#).
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 nessun tag è assegnato 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 Centro identità IAM](#).

2. Seleziona Impostazioni.
3. Selezionare la scheda Tag.
4. Per ogni tag, digita i valori nei campi Chiave e Valore (facoltativi). Quando hai finito, scegli il pulsante Aggiungi nuovo tag.

Per rimuovere un tag, scegli il pulsante Rimuovi accanto al tag che desideri rimuovere.

AWS CLI esempi

AWS CLI Fornisce comandi che è possibile utilizzare per gestire i tag assegnati al 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,Environment=Prod
```

```
> --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 \  
> --tags Stage=Test, CostCenter=80432, Owner=SysEng
```

```
> --name permission=set-name \  
> --tags Stage=Test, CostCenter=80432, Owner=SysEng
```

Gestisci i tag utilizzando l'API 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 della AWS CLI con IAM Identity Center

AWS L'integrazione della Command Line Interface (CLI) versione 2 con IAM Identity Center semplifica il processo di accesso. Gli sviluppatori possono accedere direttamente a IAM AWS CLI utilizzando le stesse credenziali di Active Directory o IAM Identity Center che utilizzano 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 AWS CLI direttamente utilizzando le proprie credenziali Active Directory.

AWS L'integrazione della 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 collegando IAM Identity Center a Active Directory utilizzando Directory Service
- Gli sviluppatori possono accedere dalla CLI per un accesso più rapido.
- Gli sviluppatori possono elencare e passare da un account e un ruolo all'altro a cui hanno assegnato l'accesso.
- Gli sviluppatori possono generare e salvare automaticamente profili di ruolo denominati nella loro configurazione CLI e farvi riferimento 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 lunga durata.

Come integrare la AWS CLI con IAM Identity Center

Per utilizzare l'integrazione AWS CLI con IAM Identity Center, scarica, installa e configura la AWS Command Line Interface versione 2. Per i passaggi dettagliati su come scaricarlo e integrarlo AWS CLI con IAM Identity Center, consulta [Configurazione della AWS CLI per l'uso di IAM Identity Center nella Guida per AWS Command Line Interface](#) l'utente.

Considerazioni per l'accesso Console di gestione AWS privato

Se la tua organizzazione utilizza la funzionalità di accesso Console di gestione AWS privato, dovresti considerare in che modo gli utenti accederanno a IAM Identity Center.

Una policy sugli endpoint VPC limita l'accesso alla console di gestione, il che impedisce agli utenti di accedere a siti a cui Account AWS non sono autorizzati. Per ulteriori informazioni, consulta [Console di gestione AWS Private Access nella Guida introduttiva](#) Console di gestione AWS .

Gli endpoint VPC bloccano l'accesso allo IAM Identity Center

È importante notare che l'utilizzo degli endpoint VPC bloccherà l'accesso all'IAM Identity Center. Ciò accade quando un utente ha già effettuato l'accesso alla console di gestione tramite l'endpoint VPC. Per garantire che gli utenti possano continuare ad accedere a IAM Identity Center, devono utilizzare l'endpoint pubblico per AWS l'accesso, anziché l'endpoint VPC.

Quote e limiti in IAM Identity Center

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 di APIs amministrare IAM Identity Center se hai più di 50.000 utenti, 10.000 gruppi o 500 set di autorizzazioni. Per ulteriori informazioni sulla CLI, vedere. [Integrazione della AWS CLI con IAM Identity Center](#) Per ulteriori informazioni APIs, 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 applicazioni	25	No

Account AWS quote

Risorsa	Quota predefinita	Può essere aumentata
Numero dei set di autorizzazioni consentiti in IAM Identity Center	3500	Sì
Numero di set di autorizzazioni predisposti consentiti per Account AWS	500	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	25 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 contemporaneamente Account AWS	1	No

¹AWS 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

[Gestisci Account AWS con set di autorizzazioni](#) vengono forniti Account AWS come ruoli IAM o utilizzano ruoli IAM esistenti in e quindi seguono le Account AWS quote 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 degli archivi di identità di IAM Identity Center

Risorsa	Quota predefinita	Può essere aumentata
Numero di utenti supportati in IAM Identity Center	200000	Sì
Numero di gruppi supportati in IAM Identità Center	100000	Sì
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
IAM Identity Center APIs	IAM Identity Center APIs ha un limite di accelerazione collettivo di 20 transazioni al secondo (TPS). In fase di lettura APIs, puoi aprire una richiesta di assistenza per richiedere un aumento del limite. L'API di CreateAccountAssignment scrittura ha un limite di 15 chiamate asincrone in sospeso. Questo limite non può essere aumentato.
Identity Store APIs	Identity Store APIs ha un limite di velocità di 20 transazioni al secondo (TPS) per API. Questo limite si applica per ogni istanza di Identity Store. Puoi aprire una richiesta di assistenza per richiedere un aumento del limite.
SCIM APIs	SCIM APIs ha limiti di accelerazione di 25 transazioni al secondo (TPS) per la scrittura APIs e 40 TPS per la lettura. APIs Questi limiti si applicano per ogni istanza di Identity Store. Puoi aprire una richiesta di assistenza per richiedere un aumento del limite.

Se la tua istanza IAM Identity Center è abilitata in modalità multipla Regioni AWS, i limiti di accelerazione si applicano allo stesso modo a ciascuna regione abilitata. Ad esempio, avresti il limite di 20 TPS sull'Identity Store APIs in ogni regione abilitata. [Per ulteriori informazioni su quali operazioni API sono disponibili in altre regioni, consulta la tabella corrispondente.](#)

Quote di richieste di servizio OIDC

Risorsa	Valore predefinito (richieste al secondo)	Può essere aumentata
Richiedi la tariffa da un indirizzo remoto per registrare un client pubblico OAuth Si applica a: RegisterClient	20	Sì
Richiedi la tariffa a un cliente pubblico registrato con il servizio OIDC Si applica a: CreateToken StartDeviceAuthorization	80	Sì
Frequenza di richiesta da tutti i client pubblici registrati con la stessa istanza di IAM Identity Center Si applica a: CreateToken	250	Sì
Frequenza di richiesta da un'applicazione IAM Identity Center registrata con l'istanza IAM Identity Center Si applica a: CreateTokenWithIAM	80	Sì
Velocità di generazione di token da tutte le applicazioni IAM Identity Center registrate con la stessa istanza IAM Identity Center con concessione JWT Bearer	10	Contatta l' AWS assistenza

Risorsa	Valore predefinito (richieste al secondo)	Può essere aumentata
Si applica a: IAM CreateTokenWith		

Se la tua istanza IAM Identity Center è abilitata in più Regioni AWS, le tariffe di richiesta sopra riportate si applicano allo stesso modo a ciascuna regione abilitata. Ad esempio, se la frequenza di richieste consentita per registrare un OAuth client pubblico da un indirizzo remoto è di 20 richieste al secondo, questo throughput è disponibile in ogni regione abilitata. Per ulteriori informazioni su quali operazioni API sono disponibili in altre regioni, consulta la [tabella corrispondente](#).

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
Numero totale di gruppi che possono essere assegnati a un set di autorizzazioni per Account AWS o a un'applicazione	100	No
Numero totale di utenti Regioni AWS abilitati per una	3	Sì

Risorsa	Quota predefinita	Può essere aumentata
singola istanza di IAM Identity Center		

* Ad esempio, potresti configurare 2750 account e 250 applicazioni, per un totale di 3000 account e applicazioni.

** L'operazione [ProvisionPermissionSet](#) API può fornire un set di autorizzazioni utilizzando l'opzione ALL_PROVISIONED_ACCOUNTS fino a un massimo di Account AWS 3500. Se è necessario fornire un set di autorizzazioni superiore a 3500 Account AWS, è possibile utilizzare l'operazione ProvisionPermissionSet API con l'AWS_ACCOUNT opzione, che fornisce il set di autorizzazioni in un'unica soluzione. Account AWS È possibile effettuare fino a tre chiamate simultanee a ProvisionPermissionSet

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 altri IAM Identity Center APIs. Aggiorna la tua policy per risolvere questo errore.

L'`ListApplications` autorizzazione autorizza più APIs:

- L'`ListApplicationsAPI`.

- Un'API interna simile all'`ListApplicationProvidersAPI` 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'`ListApplicationsAPI` pubblica ma negare l'API interna, la policy deve includere una dichiarazione che neghi l'azione: `ListApplicationProviders`

```
"Statement": [  
  {  
    "Effect": "Deny",  
    "Action": "sso:ListApplicationProviders",  
    "Resource": "*"  
  },  
  {  
    "Effect": "Allow",  
    "Action": "sso:ListApplications",  
    "Resource": "<instanceArn>" // (or "*" for all instances)  
  }  
]
```

Per consentire l'API interna ma negare l'`ListApplications`, la policy deve solo consentire `ListApplicationProviders`. L'`ListApplicationsAPI` viene negata se non è esplicitamente consentita.

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": "sso:ListApplicationProviders",  
    "Resource": "*"  
  }  
]
```

Una volta aggiornate le politiche, contattateci Supporto 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 di browser e 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 il tuo Identity Provider (IdP) è configurato per fornire gli utenti in IAM Identity Center utilizzando la sincronizzazione SCIM, potresti riscontrare errori di sincronizzazione durante il processo di provisioning degli utenti. Ciò potrebbe indicare che la configurazione utente nel tuo IdP non è compatibile con i requisiti di IAM Identity Center. Quando ciò accade, IAM Identity Center SCIM APIs restituirà messaggi di errore che forniscono informazioni sulla causa principale del problema. Puoi individuare questi messaggi di errore nei log o nell'interfaccia utente del tuo IdP. [In alternativa, puoi trovare informazioni più dettagliate sugli errori di provisioning nei log AWS CloudTrail](#)

Per ulteriori informazioni sulle implementazioni SCIM di IAM Identity Center, comprese le specifiche dei parametri e delle operazioni obbligatori, opzionali e non supportati per gli oggetti utente, consulta la Guida per gli sviluppatori di [IAM Identity Center SCIM nella SCIM Developer Guide](#)

Di seguito sono riportate alcune delle cause più comuni di questo errore:

1. L'oggetto utente nell'IdP manca di un nome (dato), un cognome (di famiglia) e and/or un nome visualizzato.

Messaggio di errore: «Sono stati rilevati 2 errori di convalida: Valore *'name.givenName'* non riuscito a soddisfare il vincolo: il membro deve soddisfare il modello di espressione regolare: `[\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {P}\\ t\\ n\\ r] +`; Valore *'name.givenName'* non riuscito a soddisfare il vincolo: il membro deve avere una lunghezza maggiore o uguale a 1"

- Soluzione: aggiungere 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.

Messaggio di errore: «L'attributo List *emails* supera il limite consentito di 1"

- 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.

Errore duplicato di utenti o gruppi durante il provisioning di utenti o gruppi con un provider di identità esterno

Se riscontri problemi di sincronizzazione di IAM Identity Center durante il provisioning di utenti o gruppi in un provider di identità (IdP) esterno, ciò potrebbe essere dovuto al fatto che gli utenti o i gruppi IdP esterni non dispongono di valori di attributo univoci. Potresti ricevere i seguenti messaggi di errore nel tuo IdP esterno:

Rifiutato di creare una nuova risorsa duplicata

Questo problema può verificarsi nei seguenti scenari:

- Scenario 1
 - Stai utilizzando attributi personalizzati non univoci nel tuo IdP esterno per attributi che devono essere unici in IAM Identity Center. Gli utenti o i gruppi IAM Identity Center esistenti non riescono a sincronizzarsi con il tuo IdP.
- Scenario 2
 - Tenti di creare utenti con attributi duplicati per attributi che devono essere unici in IAM Identity Center.
 - Ad esempio, crei o disponi di un utente IAM Identity Center esistente con i seguenti attributi:
 - Nome utente: Jane Doe
 - Indirizzo email principale: jane_doe@example.com
 - Quindi tenti di creare un altro utente nel tuo IdP esterno con i seguenti attributi:
 - Nome utente: Richard Doe
 - Indirizzo email principale: jane_doe@example.com
 - L'IdP esterno tenta di sincronizzare e creare l'utente in IAM Identity Center. Tuttavia, queste azioni falliscono poiché entrambi gli utenti hanno valori duplicati per un indirizzo email principale che deve essere univoco.

Il nome utente, l'indirizzo e-mail principale e ExternalID devono essere univoci per consentire agli utenti IdP esterni di sincronizzarsi correttamente con IAM Identity Center. Allo stesso modo, il nome del gruppo deve essere univoco per consentire la corretta sincronizzazione dei gruppi IdP esterni con IAM Identity Center.

La soluzione consiste nel rivedere gli attributi della fonte di identità e assicurarsi che siano unici.

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 [MFA per gli utenti della directory 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 esami i ruoli IAM in un account, potresti notare che i nomi dei ruoli iniziano con 'SSO_'. AWSReserved 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 predefinita in materia di password, come descritto in [Requisiti relativi alle password per la gestione delle identità in IAM Identity Center](#)

Se un utente inserisce una password che aderisce 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 Login. ExternalId PDirectory

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, consulta [FIDO2: Web Authentication \(WebAuthn\)](#) per ulteriori informazioni sul browser/platform supporto. Per ulteriori informazioni su WebAuthn IAM Identity Center, consulta [FIDO2 autenticatori](#).

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 si 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 o Microsoft 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.](#) local/regional

Quando tento di accedere a IAM Identity Center ricevo il messaggio di errore «Non sei tu, siamo noi»

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 accedere ai set di autorizzazioni forniti nell'account di gestione

Questo messaggio indica che la [Amministrare delegata](#) funzionalità è stata abilitata e che l'operazione tentata in precedenza può essere eseguita correttamente solo da qualcuno che dispone delle autorizzazioni dell'account di gestione in AWS Organizations. Per risolvere il problema, accedi come utente con queste autorizzazioni e prova a eseguire nuovamente l'attività o assegna 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 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.

I membri del gruppo provenienti da domini affidabili non si sincronizzano con IAM Identity Center

Se un gruppo di sicurezza si sincronizza correttamente con IAM Identity Center, ma i suoi membri provenienti da un dominio locale affidabile non vengono visualizzati in IAM Identity Center, ciò può essere causato dal fatto che il gruppo risiede in AWS Managed Microsoft AD e contiene Foreign Security Principal (FSPs) che rappresenta gli utenti di un dominio affidabile.

Per risolvere i problemi, prova a eseguire i seguenti passaggi:

- Sincronizza i gruppi direttamente dal dominio affidabile: invece di sincronizzare un gruppo AWS Managed Microsoft AD che contiene membri tra domini diversi, crea e sincronizza il gruppo direttamente dal dominio locale affidabile. Questo approccio funziona perché IAM Identity Center può accedere agli oggetti utente effettivi nel dominio di origine.
- Verifica le autorizzazioni dell'account di servizio: assicurati che l'account del servizio IAM Identity Center disponga delle autorizzazioni richieste sugli oggetti utente nel dominio affidabile: `ReadProperties` e `ListContents` dell'autorizzazione.

Risolvi i problemi relativi alle chiavi gestite dal cliente in AWS IAM Identity Center

Questo argomento descrive gli errori più comuni relativi alle chiavi gestite dai clienti che potresti riscontrare durante l'utilizzo AWS IAM Identity Center e fornisce le procedure di risoluzione dei problemi per risolverli.

Accesso negato: problema di autorizzazione KMS Decrypt

Errore: «L'utente xxxxxxxx non è autorizzato a eseguire: kms: decrittografia sulla risorsa associata a questo testo cifrato perché nessuna politica basata sull'identità consente l'azione di decrittografia»
kms:

L'utente o il responsabile IAM non dispone dell'autorizzazione richiesta kms:Decrypt nella politica IAM o nella politica delle chiavi KMS.

Risoluzione dei problemi con AWS CloudTrail:

1. Cerca kms.amazonaws.com eventi in CloudTrail
2. Cerca il nome dell'evento Decrypt
3. Controlla i errorMessage campi errorCode e
4. Controlla userIdentity per confermare quale preside ha tentato l'operazione

Per risolvere questo problema, concedi all'utente o al principale IAM le autorizzazioni di kms:Decrypt accesso nella policy IAM e nella policy delle chiavi KMS. Per ulteriori informazioni, consulta [Implementazione di chiavi KMS gestite dal cliente in AWS IAM Identity Center](#).

AWS ha gestito gli errori di accesso alle applicazioni con una chiave KMS gestita dal cliente abilitata in IAM Identity Center

Se nessun utente di Identity Center può accedere alle applicazioni AWS gestite e nell'istanza di IAM Identity Center è abilitata una chiave KMS gestita dal cliente, verifica che la policy delle chiavi KMS conceda alle applicazioni AWS gestite le autorizzazioni per utilizzare la chiave KMS gestita dal cliente. Per ulteriori informazioni, consulta [Dichiarazioni sulla chiave KMS di base e sulle politiche IAM](#).

AWS errori di assegnazione and/or degli utenti nell'installazione di applicazioni gestite con una chiave KMS gestita dal cliente abilitata in IAM Identity Center

Errore: «L'utente xxxxxxxx non è autorizzato a eseguire: kms: decrittografia sulla risorsa associata a questo testo cifrato perché nessuna politica basata sull'identità consente l'azione di decrittografia»
kms:

L'utente o il responsabile IAM non dispone dell'autorizzazione richiesta kms:Decrypt nella politica IAM o nella politica delle chiavi KMS.

Risoluzione dei problemi con CloudTrail:

1. Cerca il nome dell'evento Decrypt
2. Controlla i errorMessage campi errorCode e
3. Controlla userIdentity per confermare quale preside ha tentato l'operazione

Per risolvere questo problema, concedi all'utente o al principale IAM le autorizzazioni di kms:Decrypt accesso nella policy IAM e nella policy delle chiavi KMS. Per ulteriori informazioni, consulta [Implementazione di chiavi KMS gestite dal cliente in AWS IAM Identity Center](#).

Problema relativo alle autorizzazioni KMS: configurazione della chiave gestita dal cliente con AWS IAM Identity Center

L'utente o il responsabile IAM non dispongono di una o più autorizzazioni KMS richieste (kms:Decrypt,, kms:Encryptkms:GenerateDataKey,kms:DescribeKey) quando abilita la chiave gestita dal cliente.

Risoluzione dei problemi con: CloudTrail

1. CercaDecrypt, EncryptGenerateDataKey, o DescribeKey eventi
2. Controlla i errorMessage campi errorCode e
3. Controlla userIdentity per confermare quale preside ha tentato l'operazione

Per risolvere questo problema, concedi tutte le autorizzazioni KMS richieste all'utente o al responsabile IAM nella politica basata sull'identità o nella politica delle chiavi KMS. Per ulteriori informazioni, consulta [Implementazione di chiavi KMS gestite dal cliente in AWS IAM Identity Center](#).

AWS accedere agli errori di accesso al portale con una chiave KMS gestita dal cliente abilitata in IAM Identity Center

Errore: «Codice ERRORE: 0001 - l'accesso al IdentityCenter servizio è bloccato. Contatta il tuo IdentityCenter amministratore per ulteriori passaggi».

Se gli utenti non riescono ad AWS accedere al portale di accesso e nella tua istanza di IAM Identity Center è abilitata una chiave KMS gestita dal cliente, verifica che la policy delle chiavi KMS conceda le autorizzazioni necessarie a Identity Center e Identity Store. Per ulteriori informazioni, consulta [Dichiarazioni sulla chiave KMS di base e sulle politiche IAM](#).

Risolvi i problemi di configurazione multiregionale in AWS IAM Identity Center

Questo argomento descrive gli errori più comuni relativi alla configurazione multiregionale che potrebbero verificarsi durante l'utilizzo AWS IAM Identity Center e fornisce le procedure di risoluzione dei problemi per risolverli.

La regione in cui voglio replicare la mia istanza IAM Identity Center non è disponibile nella console IAM Identity Center

È innanzitutto necessario creare una chiave di replica per la chiave KMS gestita dal cliente nella regione in cui si desidera replicare l'istanza IAM Identity Center. Una volta creata la chiave di replica, vedrai la regione nell'elenco delle regioni disponibili per le repliche. Per ulteriori informazioni, consulta [the section called “Fase 1: Creare una chiave di replica”](#).

AWS errori di accesso alle applicazioni gestiti in una regione aggiuntiva

Se nessun utente di IAM Identity Center può accedere alle applicazioni AWS gestite in una regione aggiuntiva dopo aver aggiunto la regione in IAM Identity Center, conferma di aver configurato l'URL Assertion Consumer Service (ACS) della regione aggiuntiva nel provider di identità esterno come descritto in [the section called “Fase 3: Aggiornare la configurazione dell'IdP esterno”](#). Inoltre, verifica che gli utenti dispongano della connettività alla regione.

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: 21 ottobre 2025

Modifica	Descrizione	Data
Supporto multiregionale	È stato aggiunto il supporto multiregionale, inclusa la replica in regioni aggiuntive, Account AWS l'accesso e l'uso di applicazioni AWS gestite in regioni aggiuntive.	2 febbraio 2026
Politica AWS gestita aggiornata	È stata aggiornata la politica <code>AWSIdentityCenterExternalManagementPolicy</code> AWS gestita per modificare l'ARN per il provisioning del tenant.	5 dicembre 2025
Nuovo argomento relativo alla politica AWS gestita	Sono stati aggiunti dettagli per la politica <code>AWSIdentityCenterExternalManagementPolicy</code> AWS gestita.	21 novembre 2025
Guida alla verifica e alla riconciliazione del provisioning automatico	Sono state aggiunte linee guida per il controllo e la riconciliazione di utenti, gruppi e appartenenze ai gruppi con provisioning automatico SCIM tramite Identity Store e comandi. APIs AWS CLI	17 ottobre 2025

[Quote per le richieste di assistenza OIDC](#)

Sono state aggiunte le quote di richieste di servizio OIDC, inclusi i limiti di velocità per la registrazione dei OAuth clienti, la creazione di token e altre operazioni OIDC.

13 ottobre 2025

[Aggiornamenti per la politica AWS gestita](#)

IAM Identity Center ha aggiornato le policy `AWSSSOMasterAccountAdministrator` gestite e `AWSSSODirectoryReadOnly` ha incluso le AWS KMS autorizzazioni richieste per le istanze IAM Identity Center che utilizzano chiavi gestite dal cliente per la crittografia. `AWSSSOMemberAccountAdministrator` `AWSSSODirectoryAdministrator`

17 settembre 2025

[Chiavi gestite dal cliente per la crittografia a riposo](#)

È stato aggiunto il supporto per le chiavi KMS gestite dal cliente per crittografare i dati sull'identità della forza lavoro inattivi.

17 settembre 2025

[Esempio di politica basata sulle risorse per consentire la creazione di token](#)

È stato aggiunto un esempio di politica basata sulle risorse che consente la creazione di token per applicazioni client autorizzate.

16 settembre 2025

Support per sessioni utente in background	Aggiunti contenuti per le sessioni in background degli utenti.	11 agosto 2025
Sessioni console con identità migliorata	Terminologia aggiornata per le sessioni di console con riconoscimento dell'identità (precedentemente note come sessioni con riconoscimento dell'identità).	12 maggio 2025
Guida introduttiva alla riorganizzazione	Contenuti introduttivi riorganizzati per una maggiore chiarezza ed esperienza utente.	6 maggio 2025
IAM Identity Center AD Sync è obsoleto	Non è più possibile fornire agli utenti di Active Directory IAM Identity Center AD Sync. Puoi invece utilizzare AD Sync configurabile con IAM Identity Center.	17 aprile 2025
Contenuto aggiornato per la sessione autenticata	Aggiorna la durata delle sessioni di IAM Identity Center quando la sessione utente viene eliminata.	2 aprile 2025
Aggiornamenti per le policy AWS gestite	Autorizzazioni aggiornate per la politica AWSSSOServiceRolePolicy AWS gestita.	11 febbraio 2025
Il flusso di lavoro di abilitazione di IAM Identity Center è migliorato	Flusso di lavoro aggiornato per abilitare le istanze dell'organizzazione e le istanze degli account di IAM Identity Center.	11 febbraio 2025

Aggiornamenti per l'abilitazione di IAM Identity Center	Contenuti e procedure aggiornati per abilitare le istanze dell'organizzazione e le istanze degli account di IAM Identity Center.	10 ottobre 2024
Aggiornamenti per AWS le policy gestite	Autorizzazioni aggiornate per la politica AWSIAMIdentityCenterAllowListForIdentityContext AWS gestita.	2 ottobre 2024
Aggiornamenti per la politica AWS gestita	Autorizzazioni aggiornate per la politica AWSSSOMasterAccountAdministrator AWS gestita.	26 settembre 2024
Aggiornamenti per la politica AWS gestita	Autorizzazioni aggiornate per la politica AWSIAMIdentityCenterAllowListForIdentityContext AWS gestita.	4 settembre 2024
Aggiornamenti a «Cos'è IAM Identity Center?» argomento	È stato aggiornato il contenuto che descrive i vantaggi e le funzionalità di IAM Identity Center.	19 agosto 2024
Aggiornamenti per le policy AWS gestite	Autorizzazioni aggiornate per la politica AWSIAMIdentityCenterAllowListForIdentityContext AWS gestita.	12 luglio 2024

[Aggiornamenti per la politica AWS gestita](#)

Autorizzazioni aggiornate per la politica AWSIAMIdentityCenterAllowListForIdentityContext AWS gestita.

27 giugno 2024

[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 AWSSS0ReadOnly AWS gestita.

26 aprile 2024

[Aggiornamenti per la politica AWS gestita](#)

Autorizzazioni aggiornate per la politica AWSIAMIdentityCenterAllowListForIdentityContext AWS gestita.

26 aprile 2024

Aggiornamenti per la politica AWS gestita	Autorizzazioni aggiornate per la politica AWSIAMIdentityCenterAllowListForIdentityContext AWS gestita.	24 aprile 2024
Aggiornamenti per la politica AWS gestita	Autorizzazioni aggiornate per la politica AWSIAMIdentityCenterAllowListForIdentityContext AWS gestita.	19 aprile 2024
Aggiornamenti per la politica AWS gestita	Autorizzazioni aggiornate per la politica AWSIAMIdentityCenterAllowListForIdentityContext AWS gestita.	11 aprile 2024
Aggiornamenti per la politica AWS gestita	Autorizzazioni aggiornate per la politica AWSIAMIdentityCenterAllowListForIdentityContext AWS gestita.	26 novembre 2023
Nuovo argomento relativo alla politica AWS gestita	Sono stati aggiunti dettagli per la politica AWSIAMIdentityCenterAllowListForIdentityContext 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 alla nuova guida Create, Update and Delete APIs nella Identity Center API Reference Guide.	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 le politiche AWSSS0ReadOnly AWS gestite. AWSSS0MasterAccountAdministrator AWSSS0MemberAccountAdministrator	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 AWSSS0MasterAccountAdministrator 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 sulle 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 e 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

<u>Nuova opzione per utilizzare la directory Identity Center</u>	Contenuto aggiunto per la scelta della directory Identity Center o per la connessione a una directory esistente in Active Directory.	17 ottobre 2018
<u>Support per lo stato di inoltro e la durata della sessione sulle applicazioni</u>	Aggiunti contenuti sullo stato di inoltro e sulla durata della sessione per le applicazioni.	10 ottobre 2018
<u>Supporto aggiuntivo per nuove applicazioni</u>	Aggiunto 4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvalnSync, 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
<u>Support per l'accesso multiaccount agli account di gestione</u>	Sono stati aggiunti contenuti su come delegare l'accesso a più account agli utenti in un account di gestione.	9 luglio 2018
<u>Support per nuove applicazioni</u>	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

AWS Glossario

Per la AWS terminologia più recente, consultate il [AWS glossario](#) nella sezione Reference. 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.